Francesc de Borja Moll
Centre Integrat de Formació Professional

www.cifpfbmoll.eu
C/ Caracas, 6 - 07007 – PALMA
Tel. 971278150
cifpfrancescdeborjamoll@educaib.eu

FORMACIÓ PROFESSIONAL FP
ILLES BALEARS

DIGITALIZACIÓN APLICADA A LOS SECTORES PRODUCTIVOS:

EL CAMINO A LA EMPRESA INTELIGENTE

Julio Isaac Navarro Navarrete

CIFP Francesc Borja Moll

Administración de sistemas informáticos en redes I

Profesor Bartomeu Segura Duran

2026

INDICE

1 Introducción

La transformación digital se ha convertido en un factor clave para la competitividad de las empresas, especialmente en sectores como el almacenamiento, la distribución y la logística, donde la rapidez operativa, la trazabilidad de los pedidos, la seguridad de la información y la capacidad de adaptación tecnológica influyen directamente en la calidad del servicio. En este contexto, muchas organizaciones de reciente creación todavía dependen de procesos manuales, herramientas poco integradas y una infraestructura tecnológica limitada, lo que genera ineficiencias, errores operativos y dificultades para escalar su actividad. La transformación digital en logística se entiende como la integración de tecnologías digitales en todas las áreas de la cadena de suministro para mejorar eficiencia, trazabilidad y capacidad de análisis de datos (Mecalux, 2019; Marco, 2026).

El presente trabajo desarrolla una propuesta integral de digitalización para PacketRoute S.L., una empresa ficticia pero realista del sector logístico, ubicada en el Polígono Industrial de Marratxí, dedicada al almacenaje, preparación y distribución local de productos de comercio electrónico. La empresa, fundada en 2023, se encuentra en una fase de consolidación y presenta una operativa basada en procesos parcialmente manuales, gestión dispersa de la información y escasa automatización, lo que hace necesario plantear una evolución tecnológica ordenada, segura y escalable.

A partir de esta situación, el objetivo del proyecto es diseñar una solución global que permita modernizar la organización mediante la implantación de Odoo Enterprise como núcleo de gestión empresarial, junto con mejoras en la infraestructura tecnológica, una red corporativa segmentada, mecanismos de ciberseguridad, gestión estructurada de datos, automatización de procesos y una estrategia realista de implantación. Este planteamiento se ajusta al propósito del proyecto académico, que exige abordar de forma conjunta la infraestructura, la arquitectura de red, la seguridad informática, la gestión de datos, la automatización, el trabajo colaborativo y la planificación de la implantación.

Para ello, el documento parte del análisis de la empresa y de su diagnóstico tecnológico actual, con el fin de identificar debilidades, riesgos e ineficiencias, y a partir de ahí definir un plan estratégico de digitalización adaptado a sus necesidades presentes y futuras. Posteriormente, se desarrolla una propuesta técnica que articula la implantación de Odoo

Enterprise como plataforma central de gestión con la infraestructura, la red, la seguridad, la continuidad de servicio, la gestión documental y las herramientas orientadas a mejorar la eficiencia operativa y la toma de decisiones.

Diversos estudios señalan que la digitalización en logística no es un fin en sí mismo, sino un medio para incrementar la productividad y responder a las exigencias de clientes y competencia (Mecalux, 2019). En este sentido, el presente trabajo plantea una aproximación integral a la digitalización empresarial, entendida como un proceso estructurado en el que las soluciones tecnológicas propuestas se articulan de manera coherente con las necesidades operativas, organizativas y estratégicas de la empresa. De este modo, la propuesta no se concibe como una simple incorporación aislada de herramientas, sino como un modelo de transformación orientado a mejorar la eficiencia de los procesos, reforzar la seguridad de la información, aumentar la trazabilidad operativa y favorecer la capacidad de crecimiento y adaptación futura de la organización. La transformación digital se ha convertido en un factor clave para la competitividad de las empresas, especialmente en sectores como el almacenamiento, la distribución y la logística, donde la rapidez operativa, la trazabilidad de los pedidos, la seguridad de la información y la capacidad de adaptación tecnológica influyen directamente en la calidad del servicio. En este contexto, muchas organizaciones de reciente creación todavía dependen de procesos manuales, herramientas poco integradas y una infraestructura tecnológica limitada, lo que genera ineficiencias, errores operativos y dificultades para escalar su actividad. La transformación digital en logística puede definirse como la integración de tecnologías digitales en todas las áreas de la cadena de suministro con el propósito de mejorar la eficiencia, la trazabilidad y la capacidad de análisis de datos (Mecalux, 2019; Marco, 2026).

2 Objetivos

2.1 Objetivo general

El presente trabajo tiene como objetivo general diseñar una propuesta integral de digitalización para PacketRoute S.L., concebida como un proceso de transformación tecnológica orientado a modernizar su funcionamiento interno, optimizar sus procesos operativos y administrativos, mejorar la seguridad de la información y fortalecer su capacidad de crecimiento en un entorno empresarial cada vez más dependiente de la integración entre datos, comunicaciones y sistemas. Para ello, se plantea una solución global basada en la implantación de Odoo Enterprise como núcleo ERP/CRM, complementada con una infraestructura organizada, una arquitectura de red segura, mecanismos de automatización, estrategias de gestión de datos y medidas de continuidad operativa, todo ello adaptado a las necesidades reales de una empresa logística de reciente creación y con perspectivas de consolidación y escalabilidad.

2.2 Objetivos específicos

En primer lugar, se pretende analizar de forma detallada la realidad empresarial de PacketRoute S.L., atendiendo a su actividad económica, su estructura organizativa, la distribución de sus departamentos, sus procesos de negocio y sus necesidades tecnológicas, con el fin de construir una base sólida sobre la que desarrollar el resto de la propuesta. Este análisis permitirá comprender de qué manera se relacionan las distintas áreas de la empresa y cuáles son los puntos críticos que condicionan su funcionamiento actual.

En segundo lugar, se busca realizar un diagnóstico de la situación tecnológica presente en la organización, considerando los recursos hardware disponibles, el software utilizado, el estado de la conectividad, los métodos de almacenamiento de la información y las medidas de seguridad actualmente existentes. A partir de este diagnóstico, será posible identificar las principales debilidades, riesgos e ineficiencias que justifican la necesidad de una digitalización estructurada y progresiva.

Asimismo, el trabajo persigue diseñar un plan estratégico de digitalización que permita sustituir procedimientos manuales, dispersos o poco eficientes por soluciones tecnológicas integradas, especialmente en ámbitos como la gestión de pedidos, el control de inventario, la

atención al cliente, la facturación, la trazabilidad logística y la coordinación del reparto. De esta manera, se aspira a mejorar la eficiencia operativa de la empresa y a reducir los errores derivados de la falta de automatización y de la escasa integración entre áreas.

Del mismo modo, se plantea la definición de un modelo de sistemas de información empresariales que facilite la centralización y circulación ordenada de la información mediante la implantación de Odoo Enterprise como plataforma principal de gestión, complementada con herramientas colaborativas, soluciones de gestión documental y servicios cloud. Esta integración debe contribuir a mejorar la coordinación interna, la disponibilidad de los datos y la capacidad de respuesta ante las necesidades operativas y administrativas de la organización.

Otro de los objetivos fundamentales consiste en diseñar una infraestructura tecnológica coherente con las dimensiones y necesidades de PacketRoute S.L., incluyendo servidores, almacenamiento, virtualización, estaciones de trabajo y dispositivos móviles destinados tanto al entorno de oficina como al entorno logístico. Esta infraestructura deberá responder no solo a las necesidades actuales de la empresa, sino también a sus previsiones de crecimiento y a sus futuros requerimientos de escalabilidad.

Igualmente, se pretende definir una arquitectura de red corporativa que permita garantizar comunicaciones seguras, segmentadas y estables, incorporando elementos como VLAN, WiFi empresarial, acceso remoto, VPN, firewall y mecanismos de redundancia que reduzcan la dependencia de puntos únicos de fallo. Esta arquitectura deberá ajustarse a las exigencias operativas de una empresa logística en la que la conectividad y la disponibilidad de los sistemas resultan esenciales para el desarrollo diario de la actividad.

Por otra parte, el proyecto tiene como finalidad establecer una estrategia de virtualización y cloud híbrido que combine adecuadamente los recursos locales con los servicios en la nube, favoreciendo la flexibilidad tecnológica, la continuidad operativa, la redundancia de la información y la capacidad de adaptación de la empresa ante escenarios de crecimiento o incidencia técnica.

También se persigue incorporar mecanismos de automatización aplicables tanto a la administración de sistemas como a los procesos de negocio, incluyendo la monitorización del entorno tecnológico, la automatización de copias de seguridad, el despliegue controlado de software y la digitalización progresiva del ciclo completo del pedido. Con ello, se busca reducir

la carga operativa manual, mejorar la fiabilidad de los procesos y aumentar la capacidad de control sobre el funcionamiento de la empresa.

De igual forma, el trabajo aspira a diseñar un modelo completo de seguridad informática que contemple el control de accesos, la gestión de identidades, la autenticación reforzada, la segmentación de red, la protección frente a amenazas, la definición de políticas internas de seguridad y la planificación de copias de seguridad y recuperación ante desastres. Esta dimensión resulta especialmente relevante en una organización que gestiona datos personales de clientes, información laboral de empleados y procesos críticos vinculados a la operativa diaria.

Finalmente, se pretende definir un sistema de gestión de datos que contemple bases de datos, almacenamiento, replicación, análisis de información y aprovechamiento estratégico de los datos generados por la actividad de la empresa, así como evaluar el impacto global de la digitalización sobre la productividad, la eficiencia, la seguridad, la toma de decisiones y la competitividad. Todo ello deberá concretarse en una propuesta técnica realista, acompañada de un plan de implantación por fases y de una estimación económica que permita valorar su viabilidad dentro del contexto empresarial definido.

3 Marco teórico

3.1 Transformación digital en empresas logísticas

La transformación digital puede entenderse como un proceso de cambio organizativo y tecnológico mediante el cual una empresa revisa sus procesos, herramientas, flujos de información y formas de decisión para adaptarse a un entorno cada vez más interconectado y dependiente de los datos. En el ámbito logístico, este proceso implica la adopción de tecnologías como sistemas de gestión de almacenes, automatización, internet de las cosas o análisis avanzado de datos para optimizar las operaciones y reducir los tiempos de respuesta (Marco, 2026; Mecalux, 2019). Desde esta perspectiva, digitalizar una empresa no significa únicamente incorporar nuevas aplicaciones o dispositivos, sino redefinir su funcionamiento para mejorar la eficiencia, reducir errores y facilitar la escalabilidad de la actividad.

La literatura especializada subraya que las iniciativas de transformación digital tienen mayor probabilidad de éxito cuando responden a una visión estratégica definida y se articulan de manera coherente con los procesos y las personas de la organización, en lugar de limitarse a la adopción tecnológica descoordinada (Mecalux, 2019). Esta perspectiva resulta especialmente relevante en empresas pequeñas del sector logístico, donde los recursos disponibles son limitados y cada decisión tecnológica debe justificarse desde su impacto operativo real.

3.2 Sistemas de información empresariales

Dentro del proceso de modernización, los sistemas de información empresariales constituyen uno de los elementos más importantes, ya que permiten estructurar y centralizar la información generada por la organización. Un sistema ERP (Enterprise Resource Planning) puede definirse como una solución de gestión empresarial que centraliza datos y procesos en una única base de datos para automatizar y optimizar áreas como compras, inventario, contabilidad o facturación (Wolters Kluwer, 2026). Esta integración de datos en un único repositorio permite eliminar las duplicidades habituales en organizaciones que trabajan con herramientas dispersas y no conectadas entre sí.

Los sistemas CRM (Customer Relationship Management) complementan la visión ERP al centrarse en la gestión estructurada de las relaciones con los clientes. Guerola Navarro define los sistemas CRM como herramientas tecnológicas destinadas a gestionar de forma centralizada

las relaciones con los clientes y a apoyar las decisiones de marketing, ventas y servicio (Guerola Navarro, 2021). La literatura reciente subraya que el CRM se ha consolidado como un pilar de la gestión de información centrada en el cliente, especialmente en entornos digitales donde el volumen de interacciones es elevado y la personalización del servicio constituye un factor diferenciador.

La implantación combinada de ERP y CRM permite unificar la información operativa y mejorar la capacidad de planificación de recursos (Wolters Kluwer, 2026). En consecuencia, la integración de sistemas de información debe entenderse como una condición básica para automatizar procesos, mejorar la coordinación interna y disponer de una visión global del funcionamiento empresarial que habilite la toma de decisiones basada en datos.

3.3 Infraestructura tecnológica, virtualización y cloud

La digitalización empresarial requiere una infraestructura tecnológica capaz de sostener de forma estable los servicios, aplicaciones y datos que intervienen en la actividad diaria de la organización. Dicha infraestructura comprende servidores, almacenamiento, estaciones de trabajo, dispositivos móviles, conectividad y mecanismos de disponibilidad, y su diseño debe responder tanto a las necesidades actuales de la empresa como a sus previsiones de crecimiento.

En este contexto, la virtualización permite ejecutar múltiples máquinas virtuales sobre un mismo servidor físico, optimizando el uso del hardware, simplificando el mantenimiento y mejorando la capacidad de recuperación ante fallos. El cloud computing, por su parte, proporciona recursos de computación bajo demanda a través de internet, combinando modelos de servicio como IaaS, PaaS o SaaS, que se diferencian en el grado de control y responsabilidad que retiene el usuario final (VMware, 2024; Microsoft Azure, 2024). El modelo de cloud híbrido combina recursos locales con servicios en la nube para ganar flexibilidad, escalabilidad y redundancia en el entorno empresarial, lo que lo convierte en la opción más adecuada para pequeñas y medianas empresas que necesitan equilibrar coste, control y disponibilidad.

3.4 Arquitectura de red y continuidad operativa

La arquitectura de red representa otro de los pilares fundamentales de cualquier propuesta de digitalización, ya que sobre ella se apoyan las comunicaciones entre usuarios, dispositivos, aplicaciones y servicios corporativos. El diseño de una red empresarial debe

contemplar aspectos como la topología, la segmentación lógica mediante VLAN, la disponibilidad de redes WiFi seguras, el acceso remoto mediante VPN y la protección perimetral a través de firewall. La segmentación permite separar el tráfico según funciones o áreas de trabajo, mejorar el rendimiento y limitar la exposición entre entornos con distintos niveles de criticidad.

La continuidad de servicio exige, a su vez, reducir los puntos únicos de fallo mediante medidas de redundancia de conectividad y de infraestructura. En organizaciones cuya operativa depende de la disponibilidad de los sistemas durante la preparación y expedición de pedidos, la estabilidad de la red constituye un requisito esencial para garantizar el funcionamiento diario. Los marcos de referencia de ciberseguridad recomiendan diseñar infraestructuras de red que minimicen los puntos únicos de fallo y contemplen medidas de detección, respuesta y recuperación ante incidentes (NIST, 2024).

3.5 Seguridad informática y gestión de identidades

La incorporación de soluciones tecnológicas en una empresa debe ir acompañada de un modelo de seguridad que proteja tanto los sistemas como la información gestionada por la organización. La gestión de identidades, el control de accesos, la autenticación robusta y la segmentación de privilegios se consideran elementos básicos de cualquier estrategia de ciberseguridad (NIST, 2024). En entornos corporativos, los servicios centralizados de identidad permiten organizar usuarios, equipos y permisos de manera estructurada, mientras que los mecanismos de control sobre carpetas y recursos compartidos contribuyen a aplicar el principio de mínimo privilegio.

A este conjunto de medidas preventivas deben añadirse la protección frente a malware, las copias de seguridad periódicas y la planificación de recuperación ante desastres, ya que la seguridad no depende únicamente de la prevención, sino también de la capacidad de restaurar la operatividad frente a incidencias técnicas. La introducción de mecanismos de autenticación multifactor se ha consolidado como una recomendación prácticamente universal para reducir las brechas de autenticación en entornos corporativos (Microsoft, 2024). El marco de ciberseguridad del NIST articula estas funciones en cinco categorías —identificar, proteger, detectar, responder y recuperar— que ofrecen un modelo de referencia aplicable a organizaciones de cualquier tamaño (NIST, 2024).

En el ámbito normativo español y europeo, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), desarrolla y complementa el Reglamento General de Protección de Datos (RGPD) adaptando sus exigencias al ordenamiento jurídico español (Jefatura del Estado, 2018). Para entidades del sector privado que gestionan datos de clientes y empleados, como PacketRoute S.L., la LOPDGDD establece obligaciones concretas en materia de consentimiento, derechos de los interesados y medidas de seguridad que deben integrarse desde el diseño de los sistemas.

3.6 Gestión de datos, trazabilidad y protección de datos

La gestión de datos constituye una dimensión transversal de la digitalización, dado que la mayor parte de los procesos empresariales dependen de la captura, almacenamiento, consulta y explotación de información estructurada. Las bases de datos relacionales constituyen el núcleo de muchos sistemas de información empresariales, permitiendo organizar y explotar la información relativa a clientes, operaciones e inventario de forma coherente y escalable (Forés Julián et al., 2015a). El diseño riguroso del modelo de datos, siguiendo principios de normalización y consistencia, garantiza que la información pueda crecer junto con la empresa sin generar incoherencias ni redundancias.

En el sector logístico, esta capacidad se relaciona directamente con la trazabilidad, definida como la capacidad de rastrear y documentar la historia, ubicación y recorrido de un producto a lo largo de la cadena de suministro (Triangle, 2025). En el contexto europeo, el tratamiento de datos personales se encuentra regulado por el Reglamento (UE) 2016/679 (RGPD), que establece principios y obligaciones para las organizaciones que tratan información personal, incluyendo el deber de garantizar la confidencialidad, integridad y disponibilidad de los datos mediante medidas técnicas y organizativas apropiadas (Parlamento Europeo y Consejo, 2016). La empresa debe además considerar el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, como marco de referencia para la gestión de la seguridad de los sistemas de información en organizaciones que prestan servicios a la Administración o gestionan información sensible (Ministerio de la Presidencia, 2022).

4 Metodología

El presente trabajo se ha desarrollado mediante una metodología de carácter aplicado, descriptivo y proyectual, orientada al diseño de una propuesta integral de digitalización para una empresa ficticia pero verosímil del sector logístico. Este enfoque resulta adecuado porque el objetivo del proyecto no consiste en realizar una investigación experimental, sino en analizar una situación empresarial concreta, identificar sus necesidades tecnológicas y formular una solución técnica estructurada, coherente y viable dentro del contexto definido.

En una primera fase, se llevó a cabo la definición del caso de estudio, concretando la identidad de la empresa PacketRoute S.L., su actividad económica, su ubicación, su dimensión organizativa, su volumen de actividad y sus principales procesos de negocio. A partir de esta caracterización inicial, se delimitó el alcance del proyecto y se identificaron los elementos clave que debían ser abordados en la propuesta, especialmente en relación con la logística de pedidos, la gestión del inventario, la administración interna, la atención al cliente, el reparto y la infraestructura tecnológica asociada.

En una segunda fase, se realizó un análisis funcional de la empresa con el fin de comprender la relación entre sus áreas organizativas, sus flujos de trabajo y sus necesidades operativas. Este análisis permitió estudiar cómo circula la información entre departamentos, qué tareas se ejecutan de forma manual, qué dependencias existen entre procesos y qué limitaciones pueden afectar al rendimiento, a la seguridad o a la trazabilidad de la actividad empresarial. Sobre esta base, fue posible establecer una visión global del funcionamiento de la organización y detectar los puntos más susceptibles de mejora.

Posteriormente, se efectuó un diagnóstico de la situación tecnológica actual, atendiendo a aspectos como el hardware existente, el software utilizado, la conectividad, el almacenamiento de la información y las medidas de seguridad disponibles. Esta fase tuvo como finalidad identificar debilidades, riesgos e ineficiencias, en coherencia con lo exigido por el enunciado, y responder de forma fundamentada a la necesidad de digitalización de la empresa.

Una vez definido el escenario de partida, se procedió al diseño de la propuesta técnica de digitalización. Esta etapa se desarrolló siguiendo una lógica modular, abordando de manera coordinada los distintos ámbitos que conforman la arquitectura tecnológica empresarial: digitalización de procesos, implantación de sistemas de información, infraestructura tecnológica, arquitectura de red, virtualización, cloud, automatización, seguridad informática,

protección de datos y gestión de datos. De esta forma, cada decisión adoptada se vinculó tanto a una necesidad operativa detectada como a uno o varios criterios de mejora tecnológica y organizativa.

La propuesta elaborada se apoyó asimismo en una revisión conceptual previa, recogida en el marco teórico, con el propósito de fundamentar las decisiones técnicas desde una base terminológica y funcional coherente. De este modo, conceptos como ERP, CRM, cloud híbrido, segmentación de red, control de accesos, trazabilidad, copias de seguridad o gestión de identidades no se incorporan como elementos aislados, sino como componentes integrados en un modelo global de transformación digital ajustado a las características de la empresa.

Finalmente, la metodología del trabajo incorpora una perspectiva de viabilidad, al incluir no solo el diseño técnico de la solución, sino también la valoración de su impacto, una planificación de implantación por fases y una estimación económica aproximada. Este planteamiento permite que la propuesta no se limite a una descripción idealizada de herramientas o tecnologías, sino que se presente como un proyecto estructurado, progresivo y alineado con las necesidades presentes y futuras de la organización. Para el soporte documental de la investigación, se consultaron fuentes académicas, publicaciones técnicas de fabricantes y marcos normativos oficiales, garantizando en todo momento que las referencias bibliográficas incluidas en el documento correspondieran a fuentes verificables y directamente relacionadas con el contenido citado.

5 Análisis de la empresa

El presente capítulo tiene por finalidad describir la realidad actual de PacketRoute S.L. desde una perspectiva organizativa, funcional y tecnológica, con el objetivo de establecer una base sólida para el posterior diagnóstico técnico y para la propuesta de digitalización desarrollada en los capítulos siguientes. El análisis toma como referencia el marco de estudio de caso definido en la metodología y se estructura en torno a la actividad económica, la organización interna, los procesos de negocio y las necesidades tecnológicas identificadas.

5.1 Actividad económica

PacketRoute S.L. es una empresa del sector logístico dedicada al almacenaje, preparación y distribución local de productos comercializados a través de canales de comercio electrónico. Su actividad principal consiste en recepcionar mercancía importada, almacenarla en una única sede, gestionar los pedidos procedentes de clientes particulares y distribuirlos dentro del ámbito local de Mallorca mediante medios de reparto propios.

La empresa fue fundada en 2023 y se encuentra todavía en una fase de asentamiento y consolidación. Esta circunstancia resulta determinante para comprender su situación actual: muchas de sus dinámicas de trabajo conservan rasgos propios de una organización joven, con estructura interna poco especializada, procedimientos operativos parcialmente manuales, estandarización documental limitada y una fuerte dependencia de la coordinación interpersonal frente a la integración de sistemas.

PacketRoute S.L. opera desde una única sede ubicada en el Polígono Industrial de Marratxí. En ella se concentran tanto las actividades logísticas como las tareas administrativas, comerciales y de soporte tecnológico. El edificio puede entenderse funcionalmente dividido en dos niveles: una planta baja destinada al trabajo operativo de almacén, recepción de mercancía, preparación de pedidos y salida de vehículos; y una planta superior orientada a funciones administrativas, de gestión, atención al cliente y soporte interno.

El catálogo de productos manejado por la empresa está compuesto principalmente por artículos de pequeño y mediano tamaño, con un perfil típico de ecommerce generalista: accesorios, pequeños artículos de hogar, productos de bazar, complementos tecnológicos y otros bienes de consumo habitual de volumen y peso moderados. Esta característica condiciona directamente la organización del almacén, el tipo de reparto empleado y el modelo logístico

general, ya que no requiere flota especializada para grandes cargas ni instalaciones de almacenamiento de alta complejidad técnica.

En cuanto al volumen de actividad, la empresa gestiona aproximadamente setenta pedidos diarios. Esta cifra permite clasificarla como una pequeña empresa con actividad estable, pero todavía alejada de estructuras logísticas masivas o altamente automatizadas. Aun así, el volumen resulta suficientemente significativo como para que las carencias en trazabilidad, control de stock e integración de sistemas produzcan impactos visibles en la operativa, en la atención al cliente y en la calidad del servicio. Su ámbito geográfico de actuación es, por el momento, exclusivamente local, con cobertura centrada en Palma y municipios próximos, aunque la empresa mantiene una aspiración de crecimiento a medio plazo hacia otras zonas de la isla.

5.2 Estructura organizativa

Desde el punto de vista organizativo, PacketRoute S.L. presenta una estructura funcional básica, característica de una empresa pequeña que ha crecido en un período relativamente corto y que todavía no ha desarrollado una segmentación interna plenamente especializada. La estructura permite operar de manera continua, pero muestra una concentración de responsabilidades en determinadas áreas y una delimitación incompleta entre algunas funciones administrativas, comerciales y logísticas. *(véase Figura 1, Apéndice A)*

La dirección ocupa el nivel superior de la organización y ejerce una función central en la supervisión global del negocio, la coordinación entre áreas, la toma de decisiones y el seguimiento de los resultados. Dado el tamaño reducido de la empresa, la dirección no se apoya aún en una capa intermedia sólida de mandos especializados, sino que mantiene una relación directa con las áreas funcionales, participando activamente en la resolución de incidencias y en la validación de decisiones operativas.

Por debajo de la dirección, la empresa se articula alrededor de ámbitos de trabajo claramente reconocibles: administración, contabilidad y compras, comercial y atención al cliente, logística y almacén, reparto y distribución, y soporte IT. Sin embargo, varios de estos ámbitos mantienen zonas de solapamiento funcional, especialmente entre administración y contabilidad, y entre comercial y logística. Determinadas tareas son asumidas de manera compartida o informal por el personal disponible, situación que se agrava en episodios de alta

carga operativa o incidencias. La estructura funcional descrita se representa en la Figura 1 mediante el organigrama de la empresa.

Esta configuración resulta comprensible y coherente con una empresa en fase de asentamiento, pero revela limitaciones desde el punto de vista de la madurez organizativa: la ausencia de una delimitación más precisa entre funciones dificulta el control de responsabilidades, incrementa la dependencia del conocimiento informal de determinadas personas e impide una trazabilidad rigurosa de ciertos procesos clave, especialmente los relacionados con inventario, documentación e incidencias.

5.3 Departamentos y funciones actuales

En la fecha de elaboración de este proyecto, PacketRoute S.L. cuenta con una plantilla aproximada de treinta y cinco trabajadores distribuidos entre los distintos departamentos funcionales. La organización actual resulta operativa y suficiente para el sostenimiento de la actividad diaria, aunque presenta un nivel de especialización interna moderado. Varias funciones críticas se encuentran integradas dentro de áreas amplias y no completamente diferenciadas, lo que incrementa la dependencia de procedimientos manuales y dificulta el control riguroso de determinados procesos.

5.3.1 Dirección general

La dirección general constituye el núcleo de coordinación y supervisión de la organización. Desde esta posición se controlan los aspectos más relevantes del negocio: planificación general, toma de decisiones estratégicas y operativas, supervisión de la actividad diaria, relación con proveedores estratégicos y seguimiento de los resultados empresariales. Dado el tamaño de la empresa, la dirección mantiene una relación cercana con todas las áreas y participa de forma directa en la resolución de incidencias relevantes y en la validación de decisiones con impacto transversal.

5.3.2 Administración

El área de administración agrupa actualmente un conjunto diverso de tareas vinculadas a la gestión interna: archivo documental, gestión administrativa general, soporte a la facturación, seguimiento básico de documentación interna y coordinación general. En la práctica, esta área

absorbe también funciones que en organizaciones más desarrolladas estarían diferenciadas, como parte de la gestión de personal, el control documental y determinadas responsabilidades relacionadas con calidad administrativa. Esta concentración de funciones permite operar con plantilla reducida, pero genera sobrecarga y dependencia de procedimientos escasamente estandarizados.

5.3.3 Contabilidad y compras

El área de contabilidad y compras se encarga del registro económico básico, del control de pagos y cobros, de la relación administrativa con proveedores y del apoyo a la facturación. En la situación actual no siempre existe una separación completamente nítida entre las funciones de administración y las de contabilidad, de modo que ambas áreas mantienen una relación de trabajo muy estrecha y comparten información de forma continua. Esta proximidad funcional es habitual en pequeñas empresas, aunque puede generar duplicidades, errores en el tratamiento manual de datos o falta de uniformidad en los registros.

5.3.4 Comercial y atención al cliente

El área comercial y de atención al cliente representa un punto crítico dentro de la cadena operativa de la empresa. En el modelo actual, buena parte de los pedidos se recibe a través de redes sociales y canales digitales no integrados, lo que obliga al personal de esta área a dedicar una parte significativa de su tiempo a la recepción, revisión y tramitación manual de solicitudes. Además de captar y registrar pedidos, esta unidad atiende consultas, confirma datos de clientes, comunica estados de pedido y gestiona parte de las incidencias posventa. La acumulación de estas tareas comerciales y de soporte introduce una carga operativa considerable y reduce la capacidad de especialización del servicio.

5.3.5 Logística y almacén

El área de logística y almacén representa el núcleo operativo de PacketRoute S.L. y concentra las tareas relacionadas con la recepción de mercancía, el conteo inicial, la clasificación, el almacenamiento, la localización de productos, la preparación de pedidos y la expedición. Dentro de esta área, muchas funciones se desarrollan todavía sin una separación formal entre recepción, inventario, picking, empaquetado y salida. El departamento sostiene la

actividad diaria, pero depende en gran medida de la experiencia práctica del personal y de rutinas que no se encuentran suficientemente documentadas ni respaldadas por sistemas digitales de trazabilidad.

5.3.6 Reparto y distribución

El área de reparto y distribución se encarga de la entrega final de los pedidos al cliente. La empresa dispone de repartidores propios y de una zona exterior destinada al estacionamiento de motos y vehículos ligeros utilizados para el servicio. En la operativa actual, la asignación de pedidos se realiza de forma predominantemente manual, en función de la carga diaria y de criterios organizativos informales, y no sobre la base de un sistema automatizado de rutas. Esta carencia puede producir ineficiencias en la organización del reparto, retrasos en la actualización del estado del pedido y dificultades para proporcionar al cliente una previsión precisa del momento de entrega.

5.3.7 IT y soporte tecnológico

El área de soporte IT existe en la empresa con una dimensión reducida. Su función principal consiste en mantener operativos los equipos informáticos, prestar apoyo básico a los usuarios y colaborar en la resolución de incidencias tecnológicas. Sin embargo, al tratarse de una organización con un nivel de madurez digital todavía medio-bajo, el área tecnológica no actúa aún como un departamento plenamente estructurado de transformación digital, sino como una unidad de soporte y mantenimiento reactivo. Esta situación limita la capacidad de planificación tecnológica a medio y largo plazo.

5.3.8 Procesos de negocio actuales

La actividad de PacketRoute S.L. se articula alrededor de un conjunto de procesos que presentan una elevada interdependencia entre áreas, de modo que las incidencias o retrasos en una fase del flujo repercuten con facilidad en el resto de la operativa.

Aprovisionamiento y recepción de mercancía. La empresa adquiere productos a proveedores externos para su posterior comercialización en el canal ecommerce. Al llegar la mercancía a la sede, el personal de logística procede a su descarga, revisión básica y conteo inicial. En esta fase se verifica que el material recibido coincida con la documentación

disponible y con la previsión de entrada. A continuación, la mercancía se clasifica y ubica en el almacén para quedar disponible para su preparación.

Recepción y gestión del pedido. Una parte significativa de los pedidos llega actualmente a través de redes sociales y otros canales digitales no automatizados, lo que implica que el personal del área comercial y de atención al cliente deba revisar manualmente cada solicitud, confirmar la información del cliente y trasladar el pedido al circuito interno de preparación. Este modelo introduce una dependencia considerable del trabajo manual y del tratamiento individual de cada solicitud.

Preparación logística del pedido. Una vez validado el pedido, el área de almacén localiza los productos correspondientes, los extrae del stock disponible y los prepara para la expedición. Esta fase comprende la selección del artículo, la verificación de la coincidencia con la solicitud, la agrupación del pedido y el empaquetado. Dado que la empresa no dispone aún de un sistema avanzado de trazabilidad interna, parte del control depende del criterio del operario y de los registros manuales disponibles.

Expedición y reparto. Una vez preparado el pedido, este pasa al área de distribución, donde se asigna a un repartidor. La asignación diaria se realiza según disponibilidad, volumen de pedidos y organización interna, sin que exista automatización completa de rutas, prioridades o tiempos estimados de entrega.

Cierre administrativo y gestión de incidencias. Tras la entrega, la empresa debe confirmar el resultado de la operación, registrar la situación final del envío y atender posibles errores o reclamaciones. En este punto se ponen de manifiesto algunas de las limitaciones más evidentes del modelo actual: la ausencia de integración entre áreas y la dependencia de registros manuales dificultan la trazabilidad completa del pedido, la actualización rápida de su estado y la gestión ágil de incidencias relacionadas con stock, facturación o entrega.

5.4 Necesidades tecnológicas actuales

El estudio de la estructura y de los procesos de PacketRoute S.L. permite identificar cinco necesidades tecnológicas de carácter prioritario.

La primera es la centralización de la información. En la situación actual, parte de los datos de pedidos, stock, facturación e incidencias se gestionan mediante procedimientos poco integrados, lo que dificulta la coherencia entre áreas y aumenta la probabilidad de error.

La segunda necesidad es la mejora de la trazabilidad operativa. El trabajo con registros manuales o con escasa automatización provoca discrepancias entre el stock real y el registrado, dificulta el seguimiento detallado del pedido y complica la localización del origen de una incidencia. Esta carencia afecta de forma transversal a logística, atención al cliente, administración y reparto.

La tercera necesidad es la automatización de tareas administrativas y comerciales. La recepción manual de pedidos, la facturación poco integrada y la actualización no sincronizada de la información generan carga de trabajo innecesaria y reducen la capacidad de respuesta de la empresa, con impacto directo en la productividad y en la fiabilidad de los datos disponibles para la toma de decisiones.

La cuarta necesidad es disponer de una infraestructura tecnológica más ordenada y escalable, con sistemas capaces de sostener la actividad diaria sin depender de soluciones improvisadas, una red interna estructurada, mecanismos adecuados de respaldo y continuidad, y una organización clara del acceso a la información según perfiles y responsabilidades.

La quinta necesidad es avanzar en madurez digital como organización. Esto implica no solo incorporar nuevas herramientas, sino mejorar la formación del personal, normalizar los procesos, definir responsabilidades tecnológicas y reducir la dependencia del conocimiento informal acumulado por determinadas personas. Las necesidades tecnológicas de PacketRoute S.L. no se limitan, por tanto, a la adquisición de equipamiento o software, sino que afectan al modelo de funcionamiento global de la organización.

5.5 Diagrama de actividades del proceso operativo actual

El diagrama de actividades representado en la *Figura 2, Apéndice B* ilustra el flujo operativo principal de PacketRoute S.L. en su estado actual. Se ha optado por un diagrama de actividades con swimlanes para reflejar con claridad qué área asume la responsabilidad de cada tarea a lo largo del proceso, desde la recepción del pedido hasta su cierre administrativo.

El flujo se inicia en el área de Comercial y Atención al Cliente, donde el pedido es recibido a través de canales no integrados —redes sociales, teléfono o mensajes directos— y sometido a una única validación formal: comprobar si la información del pedido está completa y puede ser aceptada. Esta es la única bifurcación explícita contemplada actualmente en el proceso. En caso negativo, el personal gestiona la incidencia de forma manual y solicita la

información faltante antes de reintentar el registro. Cuando el pedido resulta aceptado, se registra también de forma manual.

A continuación, el flujo pasa al área de Logística y Almacén, donde se genera la orden de preparación, se ejecuta el picking y empaquetado y se realiza un control básico del stock disponible. Seguidamente, Reparto y Distribución asigna el repartidor y la ruta correspondiente y ejecuta la entrega. Finalmente, Administración y Contabilidad gestiona la documentación asociada y procede al cierre administrativo y la facturación. De manera transversal a todo el proceso, el área de IT y Soporte interviene de forma puntual para mantener operativos los equipos y las aplicaciones básicas, aunque sin un rol formalizado dentro del flujo.

La escasa presencia de bifurcaciones en el diagrama no constituye una simplificación, sino un reflejo fiel de la realidad operativa: los procesos carecen en su mayor parte de mecanismos formales de control, validación o gestión de excepciones. La única decisión explícita contemplada es la validación inicial del pedido; situaciones como errores de stock, incidencias en el reparto, devoluciones o fallos en la facturación se gestionan de forma improvisada, sin procedimientos estandarizados. Esta limitación constituye una de las principales ineficiencias identificadas en el análisis y será abordada en el plan de digitalización mediante la incorporación de nuevos puntos de control, automatizaciones y flujos de gestión de errores a lo largo de todo el proceso operativo.

5.6 Síntesis del análisis y principales ineficiencias

El análisis de PacketRoute S.L. muestra una organización operativamente funcional, pero con limitaciones claras en integración de información, trazabilidad y soporte tecnológico que condicionan su capacidad de crecimiento. La literatura sobre transformación digital en logística subraya que los procesos basados en registros manuales y herramientas poco integradas tienden a generar errores, retrasos e ineficiencias a medida que aumenta el volumen de actividad (Mecalux, 2019; Marco, 2026). Esta situación se corresponde directamente con la realidad de la empresa, que todavía depende del registro manual de pedidos, de la gestión documental dispersa y de un control de stock poco automatizado, especialmente sensible cuando se procesan decenas de pedidos diarios.

La ausencia de un sistema integrado de gestión se traduce en que los datos de pedidos, clientes, inventario y facturación se reparten entre hojas de cálculo y aplicaciones básicas sin

conexión entre sí. Según Wolters Kluwer (2026), un ERP actúa como núcleo centralizado que unifica información y procesos en áreas como compras, almacén y contabilidad, reduciendo la fragmentación y mejorando la coherencia de los datos. Del mismo modo, Guerola Navarro (2021) destaca que los sistemas CRM permiten estructurar la relación con los clientes y las incidencias en un repositorio único, facilitando el seguimiento y la respuesta. En PacketRoute, la ausencia de estas herramientas dificulta tanto la coordinación interna como la trazabilidad administrativa de cada pedido.

La trazabilidad operativa también resulta limitada. Estudios sobre logística señalan que, sin una visión clara del recorrido del producto desde la recepción hasta la entrega, resulta complejo responder ante incidencias o identificar cuellos de botella en la cadena de suministro (Triangle, 2025; Marco, 2026). En el caso de PacketRoute, el seguimiento interno del pedido depende en gran medida de comunicaciones informales entre Comercial, Logística y Reparto, y no siempre es posible conocer de forma inmediata en qué fase exacta del proceso se encuentra un pedido.

En materia de infraestructura, la empresa dispone de una red básica sin segmentación ni mecanismos formales de redundancia o seguridad avanzada. Los marcos de referencia de ciberseguridad, como el Marco de Ciberseguridad del NIST, recomiendan estructurar la infraestructura y las redes de forma que se reduzcan los puntos únicos de fallo, se controlen los accesos y se planifiquen las capacidades de protección, detección y recuperación ante incidentes (NIST, 2018). La situación actual de PacketRoute se encuentra aún alejada de estas recomendaciones, lo que incrementa su exposición ante fallos técnicos o incidentes de seguridad.

Por último, la gestión de datos se apoya en archivos dispersos y en estructuras poco sistemáticas. Forés Julián et al. (2015) señalan que una gestión eficaz de la información empresarial requiere bases de datos bien diseñadas que permitan organizar, consultar y explotar los datos de forma coherente. A ello se añade que el Reglamento General de Protección de Datos establece obligaciones específicas en cuanto al tratamiento, la confidencialidad y la disponibilidad de los datos personales, que exigen un nivel mínimo de control sobre cómo se almacenan y quién accede a ellos (Parlamento Europeo y Consejo, 2016). La dispersión de la información dificulta tanto el aprovechamiento analítico de los datos como el cumplimiento riguroso de estas exigencias normativas.

En conjunto, estas observaciones permiten concluir que la empresa necesita un diagnóstico tecnológico específico y un plan de digitalización que actúen de manera prioritaria sobre la integración de sistemas de información, la mejora de la infraestructura, el refuerzo de la seguridad y la estructuración de la gestión de datos, aspectos que se desarrollan en los capítulos siguientes.

6 Diagnóstico tecnológico actual

6.1 Situación general del entorno tecnológico

El entorno tecnológico actual de PacketRoute S.L. se caracteriza por un nivel de madurez medio-bajo, coherente con una empresa de reciente creación que ha priorizado la puesta en marcha de la operativa frente a la consolidación de una infraestructura planificada. La organización dispone de equipos informáticos básicos para tareas administrativas, comerciales y de gestión diaria, así como de dispositivos imprescindibles para la actividad logística y de reparto. Sin embargo, el análisis previo ha evidenciado que la configuración de este entorno no responde a una planificación estructurada, sino a una acumulación progresiva de recursos en función de necesidades inmediatas, lo que genera heterogeneidad, falta de estandarización y una dependencia excesiva del conocimiento práctico individual.

Desde una perspectiva de transformación digital, esta situación coloca a la empresa en un punto de partida razonable, pero pone de manifiesto que la infraestructura y los sistemas actuales resultan insuficientes para sostener un crecimiento ordenado, garantizar trazabilidad completa de los procesos y aprovechar el potencial analítico de los datos generados por la actividad. Diversos estudios sobre logística señalan que, sin una base tecnológica sólida, la digitalización corre el riesgo de limitarse a iniciativas aisladas sin impacto real en la eficiencia global de la organización (Mecalux, 2019; Marco, 2026).

6.2 Hardware y dispositivos

En el ámbito del hardware, PacketRoute S.L. cuenta con un conjunto de ordenadores de sobremesa y portátiles destinados a administración, contabilidad y atención al cliente, así como con algunos dispositivos móviles utilizados de manera informal para comunicación y soporte operativo. La empresa dispone de una red local sencilla basada en un switch principal y un router proporcionado por el proveedor de acceso a internet, que permite la conexión básica de los equipos, pero sin segmentación ni jerarquía claramente definidas.

No existe un servidor central dedicado a funciones corporativas críticas, como el almacenamiento estructurado de datos, la autenticación de usuarios o la ejecución de aplicaciones de negocio. Tampoco se han implementado soluciones de virtualización que permitan consolidar servicios en máquinas virtuales gestionadas de forma coordinada, ni se

observa una estrategia deliberada de renovación y homogeneización del parque de equipos. Esta situación contrasta con las recomendaciones que plantean aprovechar la virtualización para optimizar el uso del hardware, facilitar el mantenimiento y mejorar la capacidad de recuperación ante fallos (VMware, 2024; Microsoft Azure, 2024).

La siguiente tabla resume el inventario tecnológico actual:

Elemento	Descripción	Observaciones
Ordenadores de sobremesa	10 unidades, uso administrativo y comercial	Heterogéneos, sin gestión centralizada
Portátiles	5 unidades, uso mixto	Sin política de cifrado ni actualización
Dispositivos móviles	8 unidades, repartidores y logística	Uso personal, sin MDM corporativo
Switch de red	1 switch no gestionable	Sin soporte para VLAN
Router/Firewall	Router del ISP	Sin segmentación ni reglas avanzadas
Impresoras	2-3 unidades, uso compartido	Compartidas en red local plana
Servidor	Inexistente	Funciones críticas distribuidas en PCs

6.3 Software y sistemas de información

En cuanto al software, la empresa utiliza principalmente herramientas ofimáticas y hojas de cálculo para la gestión de pedidos, el seguimiento de inventario, la facturación y el archivo documental. Parte de la comunicación con los clientes se canaliza a través de redes sociales, mensajería y correo electrónico, lo que obliga al personal a trasladar manualmente la información relevante a los registros internos.

No se ha implantado aún un sistema ERP que centralice los procesos de compras, almacén, facturación y contabilidad, ni un sistema CRM que estructure la relación con clientes e incidencias. Según Wolters Kluwer (2026), los sistemas ERP permiten unificar procesos empresariales clave en una base de datos única, reduciendo la fragmentación y facilitando la toma de decisiones. De manera complementaria, Guerola Navarro (2021) señala que los sistemas CRM se han consolidado como herramientas esenciales para gestionar y analizar las

relaciones con los clientes, especialmente en entornos digitales donde el volumen de interacciones es elevado. La ausencia de estas plataformas en PacketRoute se traduce en duplicidades de información, dificultades para mantener una visión completa del cliente y limitaciones para explotar los datos de forma estratégica.

La siguiente tabla recoge el software actualmente utilizado en los distintos ámbitos de gestión:

Ámbito	Herramienta actual	Limitaciones identificadas
Gestión de pedidos	Hojas de cálculo (Excel/Google Sheets)	Sin trazabilidad, propensa a errores manuales
Control de inventario	Hojas de cálculo	Desconectado de pedidos y compras
Facturación	Software básico o manual	Sin integración con contabilidad ni ERP
Atención al cliente	Redes sociales, WhatsApp, email	Canales no integrados, sin histórico centralizado
Comunicación interna	Email y mensajería informal	Sin plataforma colaborativa corporativa
Gestión documental	Carpetas locales, correo	Sin versión única ni control de accesos
Seguridad	Antivirus básico en equipos	Sin gestión centralizada ni políticas formales

6.4 Red, conectividad y acceso remoto

La red corporativa se ha configurado con un enfoque funcional orientado a garantizar la conectividad básica de los equipos y el acceso a internet, pero sin una arquitectura diseñada en términos de topología, segmentación o servicios avanzados. Todos los dispositivos comparten el mismo dominio de broadcast, la red WiFi no distingue entre tráfico de visitantes y tráfico interno, y el control de acceso a la red se basa exclusivamente en la clave del punto de acceso.

Los marcos de referencia de ciberseguridad insisten en la necesidad de segmentar las redes en función de los tipos de dispositivos, los niveles de criticidad y las funciones asociadas, de manera que un incidente en un segmento no comprometa al resto de la infraestructura (NIST, 2018). En la situación actual de PacketRoute, esta segmentación no existe, por lo que un problema en un equipo concreto podría, en el peor de los casos, afectar a otras áreas sin que la

red disponga de barreras lógicas que lo contengan. Asimismo, no se han establecido soluciones formales de acceso remoto seguro, como VPN corporativas, que permitan trabajo remoto o soporte externo de forma controlada.

6.5 Almacenamiento de la información y copias de seguridad

El almacenamiento de la información se realiza de forma distribuida en los propios equipos de usuario y en algunas carpetas compartidas sencillas, sin que exista un sistema centralizado y estructurado de gestión documental o de bases de datos. Esto implica que los documentos relevantes pueden encontrarse duplicados en varios dispositivos, que la versión vigente de un archivo no siempre está claramente identificada y que la recuperación de información ante un fallo de hardware puede depender de copias locales informales.

No se ha definido un plan formal de copias de seguridad que especifique qué datos se respaldan, con qué frecuencia, dónde se almacenan las copias y cómo se verifica su integridad. La ausencia de este tipo de planificación contrasta con las prácticas recomendadas, que señalan la necesidad de contar con copias periódicas almacenadas en ubicaciones seguras y probadas regularmente como parte de una estrategia de continuidad de negocio (NIST, 2018). Además, la dispersión de la información dificulta la explotación analítica de los datos y reduce la capacidad de la empresa para generar indicadores fiables a partir de su actividad diaria.

6.6 Seguridad informática y protección de datos

En materia de seguridad informática, la empresa dispone de medidas básicas como soluciones antivirus en los equipos y un firewall asociado al router del proveedor de acceso, pero no existe un modelo de seguridad definido de forma global. No hay un servicio centralizado de gestión de identidades, las contraseñas y los permisos se gestionan principalmente a nivel de aplicación o de dispositivo, y no se han establecido políticas formales sobre el uso de los recursos tecnológicos, el acceso a la información o la gestión de incidentes.

El NIST plantea que un enfoque maduro de ciberseguridad debe contemplar, al menos, cinco funciones articuladas: identificar, proteger, detectar, responder y recuperar, integradas a través de políticas, procesos y controles técnicos coherentes (NIST, 2018). Estas funciones se redefinen y amplían en el NIST CSF 2.0, que añade la función de gobernanza como elemento estructurador de todo el marco (NIST, 2024). En el caso de PacketRoute, estas funciones existen

de forma parcial y dispersa, sin que estén integradas en un marco común, lo que dificulta evaluar el nivel real de protección y reaccionar de manera ordenada ante un incidente.

Esta situación se relaciona directamente con las obligaciones derivadas del Reglamento General de Protección de Datos (RGPD), que exige identificar los tratamientos realizados, limitar los accesos y garantizar la confidencialidad, integridad y disponibilidad de la información personal (Parlamento Europeo y Consejo, 2016). En el territorio español, estas obligaciones se complementan con lo establecido en la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que adapta el RGPD al ordenamiento jurídico nacional e incorpora disposiciones específicas para el entorno laboral y el tratamiento de datos en el ámbito de las relaciones de trabajo (Jefatura del Estado, 2018). La falta de una política de seguridad y una gestión estructurada de datos hace que el cumplimiento de estas obligaciones dependa, en la práctica, del criterio individual de cada persona más que de un diseño organizativo consciente.

6.7 Conclusión del diagnóstico

El diagnóstico tecnológico actual de PacketRoute S.L. muestra un entorno que ha permitido iniciar y sostener la actividad, pero que presenta debilidades significativas en hardware, software, red, almacenamiento y seguridad. Estas debilidades se concretan en una fuerte dependencia de procesos manuales, en la ausencia de sistemas integrados de gestión, en una red no segmentada y en una protección limitada de la información, tanto desde el punto de vista técnico como normativo. La siguiente tabla sintetiza los principales hallazgos del diagnóstico:

Dimensión	Estado actual	Nivel de riesgo
Hardware	Heterogéneo, sin servidor central	Medio
Software	Hojas de cálculo, sin ERP ni CRM	Alto
Red y conectividad	Red plana, sin VLAN ni VPN	Alto
Almacenamiento	Distribuido en equipos de usuario	Alto
Copias de seguridad	Sin plan formal definido	Muy alto
Seguridad informática	Antivirus básico, sin políticas	Muy alto
Gestión de identidades	Sin directorio centralizado	Alto

Cumplimiento RGPD/LOPDGDD	Incompleto, dependiente de hábitos individuales	Alto

Este escenario confirma la necesidad de un plan de digitalización que actúe de forma prioritaria sobre la integración de sistemas de información, la modernización de la infraestructura, la implantación de medidas de seguridad coherentes con los marcos de referencia y la estructuración de la gestión de datos, aspectos desarrollados en los capítulos posteriores.

7 Análisis DAFO

Antes de definir el plan estratégico de digitalización, resulta conveniente sintetizar los factores internos y externos que condicionan el proceso de transformación de PacketRoute S.L. mediante un análisis DAFO. Este instrumento permite contrastar las capacidades actuales de la organización con las oportunidades y amenazas del entorno, ofreciendo una visión estructurada que facilita la priorización de actuaciones (Guerola Navarro, 2021; Mecalux, 2019).

7.1 Factores internos

7.1.1 Debilidades

a) Ausencia de un sistema ERP o CRM que centralice la gestión de pedidos, inventario y clientes
b) Procesos clave dependientes de registros manuales y hojas de cálculo, con riesgo elevado de error
c) Red corporativa plana, sin segmentación, sin VPN y con controles de acceso insuficientes
d) Falta de un plan formal de copias de seguridad y continuidad de servicio
e) Sin gestión centralizada de identidades ni políticas de acceso diferenciadas por perfil
f) Ausencia de métricas e indicadores operativos formalizados (KPIs)
g) Dependencia del conocimiento informal de determinadas personas para el funcionamiento de procesos críticos
h) Cumplimiento parcial e informal de las obligaciones del RGPD y la LOPDGDD

7.1.2 Fortalezas

a) Empresa de reciente creación con estructura organizativa flexible y adaptable
b) Plantilla reducida que facilita la implantación de cambios y la formación del personal
c) Volumen de actividad estable (~70 pedidos diarios) que justifica la inversión en digitalización
d) Sede única que simplifica el diseño y la gestión de la infraestructura tecnológica
e) Actividad centrada en ecommerce, sector en plena expansión digital
f) Dirección cercana a la operativa, lo que facilita la toma de decisiones ágil

7.2 Factores externos

7.2.1 Oportunidades

a) Crecimiento sostenido del comercio electrónico en España, que aumenta la demanda de servicios de logística local (Mecalux, 2019)
b) Disponibilidad de soluciones ERP/CRM en modo SaaS con costes accesibles para pymes, como Odoo Enterprise
c) Madurez tecnológica del cloud híbrido y la virtualización como opciones viables para empresas pequeñas (Microsoft Azure, 2024)
d) Marco normativo estable (RGPD, LOPDGDD, ENS) que impulsa la profesionalización de la gestión de datos y la seguridad
e) Posibilidad de diferenciación competitiva a través de la trazabilidad y la calidad del servicio al cliente
f) Apoyos públicos e incentivos fiscales para la digitalización de pymes en España (Plan de Digitalización de Pymes 2021-2025)

7.2.2 Amenazas

a) Competencia creciente de operadores logísticos de mayor tamaño y mayor madurez digital
b) Incremento de los ataques de ciberseguridad dirigidos a pymes con infraestructuras poco protegidas
c) Escasez de perfiles técnicos especializados en el mercado local de Mallorca
d) Posibles sanciones por incumplimiento del RGPD y la LOPDGDD en ausencia de medidas técnicas y organizativas adecuadas (AEPD, 2024)
e) Dependencia de proveedores de servicios cloud con posibles cambios en tarifas o condiciones de servicio

7.3 Síntesis estratégica del DAFO

El cruce entre los factores internos y externos permite identificar las líneas estratégicas prioritarias que guiarán el plan de digitalización. La combinación de las fortalezas con las oportunidades señala que PacketRoute S.L. está en condiciones de aprovechar el crecimiento

del ecommerce implantando sistemas integrados que le permitan escalar su operativa de forma controlada. El cruce entre debilidades y oportunidades indica que la adopción de soluciones cloud y ERP/CRM accesibles puede corregir las carencias actuales sin necesidad de inversiones desorbitadas. La combinación entre fortalezas y amenazas pone de manifiesto que la flexibilidad organizativa y la dimensión reducida de la empresa son ventajas que pueden aprovecharse para implantar medidas de seguridad de forma ágil antes de que las amenazas se materialicen. Finalmente, el cruce entre debilidades y amenazas refuerza la urgencia de abordar la gestión de identidades, la segmentación de red y el cumplimiento normativo, ya que estas carencias representan los puntos de mayor riesgo frente al entorno competitivo y regulatorio actual.

8 Plan estratégico de digitalización

8.1 Enfoque general y criterios del plan

El plan estratégico de digitalización de PacketRoute S.L. se concibe como una hoja de ruta progresiva para transformar una operativa basada en procesos manuales y sistemas dispersos en un modelo apoyado en plataformas integradas, infraestructura estructurada y gestión controlada de datos. La literatura sobre transformación digital en logística insiste en que las iniciativas tecnológicas deben responder a objetivos operativos concretos y estar alineadas con la estrategia de la empresa, evitando la acumulación de herramientas sin coordinación (Mecalux, 2019; Marco, 2026). En este sentido, el plan parte de los problemas detectados en el análisis y en el diagnóstico tecnológico, y prioriza las actuaciones que permiten reducir errores, mejorar la trazabilidad y reforzar la seguridad de la información.

La propuesta se apoya en cuatro criterios generales:

a) Integración: sustituir los procedimientos fragmentados por flujos digitales continuos que conecten recepción de pedidos, almacén, reparto y administración en un único sistema coherente.
b) Escalabilidad: garantizar que la solución pueda absorber incrementos de volumen de pedidos y crecimiento de la plantilla sin requerir reestructuraciones profundas de la arquitectura tecnológica.
c) Seguridad: contemplar la dimensión de seguridad de forma transversal, en línea con las recomendaciones del NIST CSF 2.0 y con las obligaciones establecidas por el RGPD, la LOPDGDD y el Esquema Nacional de Seguridad (ENS) (NIST, 2024; Parlamento Europeo y Consejo, 2016; Jefatura del Estado, 2018; CCN-CERT, 2022).
d) Aprovechamiento de datos: posibilitar que la información generada por la actividad diaria pueda utilizarse para la toma de decisiones y para el cumplimiento adecuado de las obligaciones normativas sobre protección de datos.

8.2 Digitalización de procesos clave

La primera línea de actuación se centra en digitalizar los procesos que hoy dependen en mayor medida de tareas manuales: recepción y registro de pedidos, gestión documental, control de stock, preparación de pedidos, reparto y cierre administrativo. La experiencia del sector muestra que la digitalización de estos flujos tiene un impacto directo en la reducción de errores

y en la mejora de los tiempos de respuesta cuando se aborda de manera ordenada (Mecalux, 2019; Triangle, 2025).

Para PacketRoute, se propone sustituir el registro manual de pedidos por un sistema estructurado que permita introducir y consultar pedidos desde un entorno único, eliminando la necesidad de transcribir información desde redes sociales o comunicaciones informales. De manera complementaria, la gestión documental asociada a cada pedido —albaranes, facturas, justificantes de entrega— se integrará en un repositorio digital vinculado al propio registro del pedido, de forma que la documentación sea accesible desde un único punto y quede sujeta a control de versiones y de acceso.

En almacén, el objetivo es que las operaciones de preparación y control de stock se apoyen en procesos digitales que permitan registrar entradas y salidas con mayor precisión y relacionar físicamente los movimientos de mercancía con el estado del pedido en el sistema. En reparto, se propone que la asignación de rutas y la confirmación de entregas dejen de depender de comunicaciones verbales o anotaciones manuales, de modo que la información de entrega se registre directamente en el sistema y pueda reflejarse en tiempo casi real en la situación del pedido.

Un aspecto añadido en este plan, no presente en la operativa actual, es la integración con plataformas de ecommerce. La empresa recibe pedidos principalmente a través de canales digitales no automatizados; la digitalización debe contemplar, en una fase posterior de madurez, la integración de Odoo Enterprise con las plataformas de venta (por ejemplo, WooCommerce, Shopify o marketplaces como Amazon) mediante conectores o API, de modo que los pedidos fluyan directamente al sistema de gestión sin intervención manual. Esta integración eliminará el cuello de botella actual en el área comercial y sentará las bases para escalar el volumen de operaciones sin incremento proporcional de la plantilla.

8.3 Implantación de sistemas de información

La segunda línea del plan consiste en introducir sistemas de información empresariales que actúen como soporte de la digitalización de procesos. Según Wolters Kluwer (2026), los sistemas ERP se han consolidado como herramientas clave para integrar procesos de compras, inventario, ventas y contabilidad en una única plataforma, reduciendo la duplicidad de datos y facilitando la coordinación entre áreas. De manera análoga, Guerola Navarro (2021) destaca el

papel de los sistemas CRM para centralizar la información sobre clientes, contactos, incidencias y oportunidades comerciales.

En coherencia con estas recomendaciones, el plan propone la implantación de Odoo Enterprise como plataforma central para la gestión de pedidos, almacén, facturación, contabilidad y relación con clientes. Esta solución integrará, al menos, los módulos de ventas, inventario, compras, facturación, contabilidad básica y CRM, permitiendo que las operaciones realizadas en almacén o reparto tengan reflejo directo en las áreas administrativas y que la empresa disponga de una visión unificada de toda su actividad.

Paralelamente, se plantea la utilización del módulo CRM de Odoo Enterprise para gestionar la información de clientes, el historial de pedidos y las incidencias asociadas, unificando la información de contacto y proporcionando una visión más clara de la calidad del servicio prestado. La combinación de módulos ERP y CRM dentro de una misma plataforma, complementada con herramientas colaborativas y gestión documental en la nube, constituye el núcleo del modelo de sistemas de información que PacketRoute necesita para evolucionar desde una gestión manual a una gestión integrada.

8.4 Infraestructura, virtualización y cloud como soporte del plan

La digitalización de procesos y la implantación de sistemas de información exige una infraestructura capaz de sostener de forma estable los servicios y datos corporativos. Los enfoques actuales señalan que la combinación de servidores físicos con entornos virtualizados y servicios en la nube permite equilibrar control local, flexibilidad y coste, especialmente en pequeñas y medianas empresas (Microsoft Azure, 2024; VMware, 2024).

En este plan, se propone estructurar la infraestructura de PacketRoute sobre tres pilares: un servidor físico principal que hospede máquinas virtuales para los servicios críticos locales; un sistema de almacenamiento en red que centralice la documentación corporativa; y una adopción gradual de servicios cloud para correo, colaboración y, potencialmente, para el propio ERP y CRM si se opta por soluciones en modo servicio. Este enfoque de cloud híbrido permitirá mantener bajo control determinados recursos sensibles, al tiempo que se aprovechan las ventajas de la nube en términos de disponibilidad, actualizaciones automáticas y escalabilidad.

La red deberá adaptarse a esta nueva arquitectura, incorporando una segmentación básica que separe al menos la red de usuarios internos, la red de dispositivos logísticos y una

red de invitados, en línea con las recomendaciones del NIST CSF 2.0 (NIST, 2024). Esta adaptación se desarrolla en detalle en el capítulo 9 del presente proyecto.

8.5 Datos, seguridad y cumplimiento normativo

El plan estratégico incorpora de forma explícita las dimensiones de datos y seguridad como ejes transversales de toda la propuesta. Forés Julián et al. (2015) subrayan que una gestión eficaz de la información empresarial se basa en bases de datos bien diseñadas que soporten los procesos clave del negocio. En PacketRoute, la implantación de ERP y CRM implicará el diseño de un esquema relacional que permita organizar la información de clientes, pedidos, inventario y facturación de forma coherente y normalizada, tal como se desarrolla en el capítulo 13.

Desde el punto de vista normativo, el RGPD requiere que las organizaciones definan con claridad qué datos personales tratan, con qué fines, durante cuánto tiempo y quién puede acceder a ellos, además de garantizar medidas adecuadas de seguridad y de respuesta ante incidentes (Parlamento Europeo y Consejo, 2016). A estas obligaciones se añaden las de la LOPDGDD en el ámbito nacional (Jefatura del Estado, 2018) y, en la medida en que la empresa utilice sistemas que procesen información de las Administraciones Públicas o sus proveedores, las disposiciones del Esquema Nacional de Seguridad como referencia de buenas prácticas (CCN-CERT, 2022). El plan de digitalización prevé que la implantación de nuevos sistemas vaya acompañada de la definición de políticas de acceso, perfiles de usuario y procedimientos básicos de gestión de incidentes de seguridad, de manera que la modernización tecnológica contribuya también a reforzar el cumplimiento legal y no solo la eficiencia operativa.

8.6 Gestión del cambio

Ninguna iniciativa de digitalización puede tener éxito si se aborda exclusivamente desde una perspectiva técnica. La transformación digital implica cambios profundos en los procesos de trabajo, en los hábitos del personal y en la cultura organizativa de la empresa. Por este motivo, el plan estratégico incorpora una dimensión explícita de gestión del cambio como condición necesaria para que las soluciones propuestas sean adoptadas de forma efectiva y sostenida.

En primer lugar, se propone involucrar a los responsables de cada área en las decisiones de diseño del sistema desde las fases tempranas de la implantación. Esta participación activa reduce la resistencia al cambio y aumenta la probabilidad de que las soluciones propuestas

respondan a las necesidades reales de cada departamento. En segundo lugar, se prevé un plan de formación escalonado para el personal, adaptado al perfil de cada área: formación básica en el uso del ERP para todo el personal que interactúa con el sistema, formación avanzada para los responsables de administración, logística y IT, y sesiones específicas sobre seguridad y protección de datos para el conjunto de la plantilla. En tercer lugar, se recomienda designar a un referente interno de digitalización —preferiblemente dentro del área IT— que actúe como interlocutor con los proveedores, supervise la evolución de la implantación y gestione las incidencias durante el proceso de transición. Este rol resulta especialmente relevante en una empresa de tamaño reducido, donde la dependencia de un único proveedor externo para la gestión del cambio puede generar vulnerabilidades organizativas.

8.7 KPIs y métricas de éxito

La efectividad del plan de digitalización debe poder medirse y evaluarse de forma objetiva. Para ello, se definen a continuación los indicadores clave de rendimiento (KPIs) que permitirán verificar el grado de consecución de los objetivos del proyecto, tanto durante la implantación como en el período de explotación posterior:

KPI	Descripción	Valor objetivo
Tasa de digitalización de pedidos	% de pedidos registrados directamente en el ERP sin intervención manual	>95% en los primeros 3 meses
Precisión de inventario	Diferencia entre stock físico y stock registrado en sistema	<1% de discrepancia
Tiempo de procesamiento del pedido	Tiempo medio desde la recepción hasta la expedición	Reducción del 30% respecto al baseline
Tasa de incidencias en reparto	% de pedidos con incidencia registrada sobre el total	<3%
Disponibilidad de sistemas críticos	Tiempo de actividad del servidor y ERP	>99,5% mensual
Tiempo de recuperación ante incidente (RTO)	Tiempo máximo para restaurar el servicio tras un fallo	<4 horas

Cobertura de backups	% de datos críticos incluidos en el plan de copias de seguridad	100%
Cumplimiento de políticas de acceso	% de usuarios con permisos asignados por rol documentado	100%

El seguimiento de estos indicadores se realizará mediante los dashboards de Metabase conectados al modelo de datos corporativo y mediante los informes nativos del ERP, garantizando que la dirección disponga de una visión actualizada del estado de la transformación digital en todo momento.

9 Propuesta de infraestructura tecnológica

9.1 Principios de diseño de la infraestructura

La infraestructura tecnológica propuesta para PacketRoute S.L. se concibe como la base estable sobre la que deben ejecutarse los servicios críticos, los sistemas de información y los mecanismos de seguridad. El objetivo fundamental es superar el entorno disperso y escasamente planificado descrito en el diagnóstico y reemplazarlo por una arquitectura coherente, capaz de sostener el volumen actual de trabajo y de acompañar el crecimiento previsto, reduciendo al mismo tiempo los puntos únicos de fallo. Los enfoques actuales de diseño de infraestructuras recomiendan aprovechar la combinación de servidores físicos, virtualización y servicios en la nube para equilibrar control, flexibilidad y coste, especialmente en pequeñas y medianas empresas (VMware, 2024; Microsoft Azure, 2024).

En coherencia con este planteamiento, la infraestructura propuesta se apoya en tres pilares principales: un servidor físico central para los servicios internos críticos, un sistema de almacenamiento corporativo accesible de forma controlada y una adopción gradual de servicios cloud para correo, colaboración y, en su caso, para parte de los sistemas de información. De este modo, la empresa mantiene capacidad de decisión sobre los activos más sensibles, al tiempo que externaliza servicios que resultan más eficientes cuando se consumen como servicio gestionado. Esta combinación responde directamente a las necesidades identificadas en el diagnóstico: centralización de datos, trazabilidad operativa, disponibilidad de servicios y cumplimiento de las obligaciones del RGPD y la LOPDGDD en materia de protección de datos personales (Parlamento Europeo y Consejo, 2016; Jefatura del Estado, 2018).

9.2 Seguridad física del CPD

Un aspecto que no puede omitirse en el diseño de infraestructura es la protección física del espacio donde residirá el servidor central y los equipos de red. Aunque PacketRoute S.L. no dispone ni requiere de un centro de proceso de datos de gran escala, sí debe habilitar un espacio cerrado y controlado —un armario rack o sala técnica cerrada con llave— donde alojar el servidor, el switch gestionable, el firewall perimetral y el sistema NAS. Las buenas prácticas de seguridad física para entornos empresariales establecen que el acceso físico a los equipos críticos debe estar limitado al personal autorizado de IT, protegido frente a acceso no autorizado,

y complementado con medidas ambientales básicas como ventilación adecuada, protección frente a humedad y un SAI (Sistema de Alimentación Ininterrumpida) que garantice continuidad ante cortes de suministro eléctrico (NIST, 2024; CCN-CERT, 2022).

En el caso de PacketRoute, se propone habilitar en la planta superior de la sede un armario rack cerrado de 12U, convenientemente ventilado, con acceso restringido a llaves en poder del responsable de IT y de dirección. Este armario alojará el servidor de virtualización, el switch de capa 3 gestionable, el firewall perimetral, el patch panel de red y el NAS corporativo. El SAI se dimensionará para garantizar al menos 20 minutos de autonomía en caso de corte eléctrico, tiempo suficiente para ejecutar un apagado controlado de los sistemas o para que el generador de emergencia entre en funcionamiento, si se incorporara en etapas futuras. Esta medida, aunque sencilla, elimina uno de los riesgos más comunes en pequeñas empresas: la exposición de los equipos críticos a entornos físicamente accesibles para el conjunto del personal

9.3 Servidor central y virtualización

Se propone la implantación de un servidor físico dedicado en la sede de PacketRoute, dimensionado para ejecutar varias máquinas virtuales con funciones diferenciadas. La virtualización permite agrupar en un único hardware servicios que hoy no están claramente identificados o se ejecutan de forma distribuida, como el servidor de ficheros interno, la base de datos corporativa, los servicios de autenticación o herramientas de gestión internas. Esta estrategia facilita el mantenimiento, la recuperación ante fallos y la posibilidad de ampliar recursos sin necesidad de cambiar continuamente de hardware físico (VMware, 2024).

El servidor propuesto se basará en una arquitectura x86-64 con, al menos, 32 GB de RAM ampliables, procesador de múltiples núcleos y almacenamiento local en configuración RAID 1 o RAID 5 para protección frente a fallos de disco. El hipervisor recomendado es Proxmox VE, solución de virtualización de código abierto que permite gestionar máquinas virtuales y contenedores LXC desde una interfaz web centralizada, sin coste de licencia, y con soporte para snapshots, backups automáticos y migración de máquinas virtuales (VMware, 2024). En una fase inicial, el servidor alojará al menos las siguientes máquinas virtuales:

Máquina virtual	Función	Recursos asignados

VM-AD	Controlador de dominio (Samba AD o Windows Server)	2 vCPU, 4 GB RAM
VM-DB	Servidor de base de datos PostgreSQL	4 vCPU, 8 GB RAM
VM-APP	Servidor de aplicaciones Odoo Enterprise	4 vCPU, 8 GB RAM
VM-FILE	Servidor de ficheros corporativo (Nextcloud o SMB)	2 vCPU, 4 GB RAM
VM-MON	Monitorización y backups (Zabbix + scripts)	2 vCPU, 2 GB RAM

Esta distribución garantiza que cada servicio opere en un entorno aislado, lo que facilita las actualizaciones, reduce el impacto de un fallo en un servicio sobre el resto y permite restaurar snapshots individuales en caso de incidencia sin afectar a la operativa global.

9.4 Almacenamiento corporativo y organización de la información

Un componente esencial de la nueva infraestructura es la definición y puesta en marcha de un espacio de almacenamiento corporativo centralizado, accesible desde los puestos de trabajo de administración, comercial, logística y reparto según perfiles de permiso. Este almacenamiento se implementará mediante un dispositivo NAS (Network Attached Storage) de al menos 4 TB en configuración RAID 1, conectado al switch gestionable de la red de servidores. El NAS alojará la documentación corporativa estructurada en carpetas por área funcional, con permisos asignados conforme al principio de mínimo privilegio: cada usuario o grupo accederá únicamente a las carpetas y archivos necesarios para el desempeño de sus funciones (NIST, 2024).

Desde una perspectiva de gestión de la información, esta medida responde a la necesidad de disponer de un repositorio único y estructurado para la documentación corporativa, evitando duplicidades, pérdidas de versiones y dependencia de los discos locales de los equipos de usuario. Forés Julián et al. (2015) destacan que la organización de la información empresarial en repositorios bien definidos es un requisito para poder explotarla de manera fiable y para garantizar que la empresa conoce en todo momento dónde se encuentra cada tipo de información y quién puede acceder a ella. La estructura de carpetas del NAS se organizará, al menos, en los siguientes niveles: Administración y Contabilidad, Comercial y Atención al Cliente, Logística

y Almacén, Recursos Humanos, IT y Soporte, y Documentación Legal, con subcarpetas normalizadas dentro de cada área.

9.5 Servicios cloud de apoyo

En paralelo a la infraestructura local, la propuesta contempla la adopción de servicios cloud para aquellas funciones que resultan más eficientes cuando se consumen como servicio: correo electrónico corporativo, colaboración ofimática, almacenamiento compartido externo y, potencialmente, la versión cloud de Odoo Enterprise. Esta estrategia sigue el modelo de cloud híbrido, que combina recursos locales y servicios en la nube para ganar flexibilidad y redundancia, siendo especialmente adecuada para organizaciones que desean mantener datos críticos en instalaciones propias sin renunciar a la escalabilidad de los servicios externos (Microsoft Azure, 2024).

Para PacketRoute se recomienda Microsoft 365 Business Basic como plataforma de correo y colaboración (Outlook, Teams, SharePoint), ya que ofrece integración nativa con Active Directory/Entra ID y permite extender las identidades corporativas al entorno cloud sin gestionar infraestructura de correo propia. En caso de que la dirección opte por Odoo Enterprise en modalidad SaaS, los datos operativos residirán en los servidores de Odoo.com bajo acuerdos de nivel de servicio y medidas de protección de datos conformes al RGPD, lo que elimina la necesidad de gestionar el mantenimiento del servidor de aplicaciones en local. La integración entre los servicios cloud y la infraestructura interna se diseñará de forma que los usuarios perciban un entorno coherente, con identidades y permisos alineados, evitando la proliferación de credenciales y puntos de acceso independientes.

9.6 Copias de seguridad y continuidad de servicio

La ausencia de un plan formal de copias de seguridad en PacketRoute S.L. constituye uno de los riesgos más críticos identificados en el diagnóstico. La propuesta establece una estrategia de backup estructurada conforme a la regla 3-2-1: mantener al menos tres copias de los datos, en dos soportes diferentes, una de ellas almacenada en una ubicación física o lógica distinta a la principal (NIST, 2024).

En la práctica, esta estrategia se implementa de la siguiente manera: los datos de las máquinas virtuales se respaldan diariamente mediante las funcionalidades nativas de Proxmox

VE hacia el NAS corporativo; el NAS a su vez replica su contenido crítico de forma semanal hacia un servicio de almacenamiento cloud cifrado —por ejemplo, Backblaze B2 o Azure Blob Storage—; y se mantiene adicionalmente una copia mensual en soporte externo físico almacenado fuera de la sede. La siguiente tabla resume la política de copias de seguridad propuesta.

Tipo de backup	Frecuencia	Destino	Retención
Snapshot VM completo	Diario (23:00 h)	NAS local	7 días
Volcado PostgreSQL (pg_dump)	Diario (00:30 h)	NAS local + cloud cifrado	30 días
Copia NAS → Cloud	Semanal (domingos)	Azure Blob / Backblaze B2	90 días
Copia completa en soporte externo	Mensual	Disco externo off-site	12 meses

Esta política garantiza que, ante un fallo de hardware, un incidente de ransomware o un error humano grave, la empresa pueda recuperar sus datos críticos en un tiempo máximo objetivo (RTO) de cuatro horas y con una pérdida de datos máxima (RPO) de veinticuatro horas, conforme a los objetivos de recuperación definidos en los KPIs del plan estratégico. Todos los procesos de backup incluirán verificación automática de integridad y alertas al responsable de IT en caso de fallo, en línea con las recomendaciones del NIST CSF 2.0 para la función de recuperación (NIST, 2024).

La infraestructura descrita en este capítulo constituye la base física sobre la que se despliega la arquitectura de red propuesta en el capítulo siguiente, y ambas forman en conjunto el soporte tecnológico que sostiene los sistemas de información, la seguridad y la gestión de datos desarrollados en los capítulos posteriores

10 Arquitectura de red corporativa propuesta

10.1 Objetivos de la nueva red

La arquitectura de red propuesta para PacketRoute S.L. busca superar el modelo actual de red plana y sin segmentación, sustituyéndolo por una red corporativa estructurada que mejore la seguridad, la estabilidad y el control del tráfico. El objetivo es que la red deje de ser un mero canal de conexión a internet y pase a ser un recurso diseñado de forma consciente para soportar los sistemas de información, el acceso a la nube, las operaciones logísticas y el trabajo diario de administración y comercial. Los marcos de referencia de ciberseguridad, como el desarrollado por el National Institute of Standards and Technology, consideran que la segmentación de red y el control del tráfico entre segmentos son medidas básicas para reducir la superficie de ataque y contener posibles incidentes (NIST, 2018).

En el caso de PacketRoute, esta arquitectura debe responder a tres necesidades prácticas: separar lógicamente las diferentes áreas de la empresa, proporcionar conectividad segura a los servicios locales y cloud definidos en la infraestructura propuesta y permitir el acceso remoto controlado cuando sea necesario. Todo ello debe conseguirse con un diseño suficientemente sencillo como para ser administrado en una pyme, pero lo bastante estructurado como para sentar las bases de una evolución posteriorLa arquitectura de red propuesta para PacketRoute S.L. tiene como finalidad principal superar el modelo actual de red plana y sin segmentación, sustituyéndolo por una red corporativa estructurada que mejore la seguridad, la estabilidad y el control del tráfico. El objetivo es que la red deje de ser un mero canal de conexión a internet y pase a ser un recurso diseñado de forma consciente para soportar los sistemas de información, el acceso a los servicios cloud, las operaciones logísticas y el trabajo diario de las áreas de administración y comercial. El NIST CSF 2.0 considera que la segmentación de red y el control del tráfico entre segmentos son medidas fundamentales para reducir la superficie de ataque y contener posibles incidentes antes de que se propaguen al resto de la infraestructura (NIST, 2024).

En el caso de PacketRoute, la arquitectura de red debe responder a tres necesidades prácticas simultáneas: separar lógicamente las diferentes áreas de la empresa para evitar que un incidente en un segmento comprometa a otro; proporcionar conectividad segura a los servicios locales y cloud definidos en la propuesta de infraestructura; y permitir el acceso remoto

controlado cuando sea necesario. Todo ello debe conseguirse con un diseño lo suficientemente sencillo como para ser administrado en una pyme, pero suficientemente estructurado como para sentar las bases de una evolución posterior hacia mayor automatización y seguridad avanzada.

10.2 Segmentación lógica mediante VLAN

La red propuesta se organiza en varios segmentos lógicos diferenciados, implementados mediante VLAN y subredes IPv4 independientes. La segmentación mediante VLAN permite dividir una red física en subredes lógicas, aislar el tráfico, controlar los accesos y reducir el impacto de un incidente de seguridad, especialmente relevante cuando distintos tipos de dispositivos comparten la misma infraestructura física (NIST, 2024). En la arquitectura propuesta para PacketRoute se definen cinco VLANs con funciones diferenciadas:

VLAN ID	Nombre	Subred IPv4	Dispositivos incluidos
VLAN 10	Usuarios oficina	192.168.10.0/24	PCs administración, comercial, contabilidad
VLAN 20	Servidores	192.168.20.0/24	Servidor Proxmox, NAS, VM internas
VLAN 30	Logística y almacén	192.168.30.0/24	Terminales almacén, impresoras etiquetas
VLAN 40	Dispositivos móviles reparto	192.168.40.0/24	Smartphones y tablets repartidores
VLAN 50	Invitados	192.168.50.0/24	Dispositivos personales y visitas

Cada una de estas VLANs se implementa como una subred IPv4 propia con su propia puerta de enlace en el switch de capa 3. El tráfico entre VLANs está restringido por defecto y únicamente se permiten los flujos estrictamente necesarios mediante reglas de control de acceso (ACL) configuradas en el firewall perimetral. Por ejemplo, la VLAN 30 de logística necesita acceder al servidor de aplicaciones Odoo en la VLAN 20, pero no debe tener visibilidad sobre los equipos de oficina de la VLAN 10 ni sobre la red de invitados. Este principio de mínimo acceso a nivel de red complementa y refuerza el principio de mínimo privilegio aplicado en la gestión de identidades y permisos descrita en el capítulo 11

10.3 WiFi corporativa y acceso remoto

La red inalámbrica de PacketRoute se organizará en al menos dos SSID diferenciados: uno corporativo, cifrado con WPA3-Enterprise o WPA3-Personal con contraseña robusta, asociado a la VLAN correspondiente según el tipo de dispositivo (VLAN 10 para equipos de oficina o VLAN 30/40 para dispositivos operativos); y otro para invitados, asociado a la VLAN 50, que únicamente permite salida a internet y no tiene visibilidad sobre ningún recurso interno. Esta separación garantiza que los dispositivos personales de visitas o del personal no compartan red con los sistemas corporativos, evitando que un incidente de seguridad en un dispositivo ajeno pueda propagarse a recursos críticos (NIST, 2024).

La WiFi corporativa será gestionada por uno o varios puntos de acceso empresariales —por ejemplo, de la gama Ubiquiti UniFi o Cisco Meraki— administrados desde un controlador centralizado que permita aplicar políticas uniformes, monitorizar el tráfico inalámbrico y detectar dispositivos no autorizados. La autenticación de dispositivos corporativos en la red WiFi se alineará con el directorio de identidades corporativo descrito en el capítulo 11, de modo que únicamente los equipos dados de alta en el sistema puedan conectarse a la VLAN corporativa. En cuanto al acceso remoto, la arquitectura incorpora una VPN corporativa gestionada desde el firewall perimetral mediante WireGuard o OpenVPN, de modo que el personal autorizado pueda acceder a recursos internos desde ubicaciones externas a través de un canal cifrado, sin exponer directamente servicios sensibles a internet. Esta VPN será especialmente útil para tareas de administración de sistemas, soporte técnico remoto y, en su caso, teletrabajo limitado de personal autorizado

10.4 Puntos de salida a internet y hardening básico

La nueva arquitectura se apoya en un firewall perimetral que actúa como punto de salida controlado hacia internet para todas las redes internas. Se propone el uso de un appliance de red con capacidades de firewall, routing y VPN, como pfSense CE o una solución equivalente de Fortinet o Sophos para pymes. Este dispositivo se encargará de filtrar el tráfico entrante y saliente según reglas definidas, limitando los servicios expuestos al exterior y aplicando inspección de estado de las conexiones. Hacia el exterior se permitirán únicamente los servicios imprescindibles para la operativa: navegación web (HTTP/HTTPS), correo saliente y conexiones a proveedores de servicios cloud autorizados. Desde el exterior, únicamente se

aceptarán conexiones entrantes a la VPN corporativa y, en su caso, a servicios publicados de forma controlada mediante proxy inverso (NIST, 2024; CCN-CERT, 2022).

Las buenas prácticas de hardening básico para redes de pequeñas empresas recomiendan, además de la segmentación y el firewall, deshabilitar los servicios y puertos no utilizados en todos los dispositivos de red, cambiar las credenciales por defecto de switches, puntos de acceso y firewall, activar el logging de eventos de red para facilitar el diagnóstico de incidencias y configurar alertas automáticas ante intentos de acceso no autorizados. En PacketRoute, estas medidas se aplicarán como parte del proceso de despliegue de la nueva infraestructura de red, documentando la configuración de cada dispositivo en el repositorio de IT para facilitar la administración y la auditoría posterior.

10.5 Síntesis de la arquitectura propuesta

La arquitectura de red corporativa propuesta consolida un modelo en el que la red deja de ser un entorno plano para convertirse en un sistema de zonas diferenciadas con reglas de comunicación claras y la disponibilidad de los sistemas resultan esenciales para el desarrollo diario de la actividad. La Figura 3 del Apéndice C representa visualmente la arquitectura completa de red y perímetro descrita en este capítulo *(véase Figura 3, Apéndice C)*.

La segmentación lógica mediante VLAN y subredes, la separación de la WiFi corporativa y de invitados, la incorporación de VPN para acceso remoto y el uso de un firewall perimetral con reglas definidas se alinean con las recomendaciones del NIST CSF 2.0 y con las buenas prácticas para redes empresariales modernas (NIST, 2024). Este diseño no pretende agotar todas las posibilidades técnicas disponibles, sino establecer una base sólida y realista para una empresa del tamaño de PacketRoute, sobre la que se puedan construir mejoras posteriores en automatización, monitorización y políticas avanzadas de seguridad. La arquitectura de red descrita en este capítulo actúa como soporte directo de la estrategia de seguridad informática y gestión de identidades desarrollada en el capítulo siguiente.

11 Arquitectura de aplicaciones y tecnologías de implementación

11.1 Modelo general de solución

La propuesta de digitalización de PacketRoute S.L. requiere una arquitectura de aplicaciones que actúe como núcleo integrador de todos los procesos de la empresa. El diagnóstico tecnológico identificó una operativa fragmentada, con información dispersa entre herramientas no conectadas y flujos de trabajo que dependen en exceso de la coordinación manual entre personas. Para superar esta situación, la solución no puede construirse sobre un conjunto de aplicaciones aisladas, sino sobre un modelo estructurado en el que la información de clientes, pedidos, stock, reparto y facturación se gestione desde un núcleo común y trazable.

En este proyecto, ese núcleo se concreta en Odoo Enterprise, seleccionado como plataforma central por su enfoque modular, su integración nativa entre áreas funcionales y su adecuación económica y operativa para una pyme logística del tamaño de PacketRoute. Odoo Enterprise reúne en una única plataforma las funciones de ERP y CRM, eliminando la necesidad de mantener sistemas separados que deban sincronizarse mediante procesos manuales (Wolters Kluwer, 2026; Guerola Navarro, 2021). Esta elección es coherente con el plan estratégico de digitalización definido en el capítulo 7, que establece como objetivo principal sustituir los procedimientos manuales por flujos integrados y trazables sin asumir los costes y plazos de un desarrollo completamente a medida.

La arquitectura resultante se organiza en tres capas funcionales diferenciadas: una capa de acceso, donde se sitúan los distintos puntos de interacción de usuarios y sistemas externos; una capa de negocio, que concentra la lógica operativa de la empresa; y una capa de datos, que actúa como repositorio estructurado y centralizado de toda la información corporativa. Esta organización en capas permite que cada componente cumpla una función específica dentro del conjunto, facilitando el mantenimiento, la evolución futura y la capacidad de añadir nuevos módulos sin alterar la estructura base del sistema.

11.2 Componentes principales de la solución

La solución propuesta para PacketRoute S.L. se articula en torno a cuatro componentes principales que cubren el ciclo operativo completo de la empresa. El primero es Odoo Enterprise con módulos de ventas, compras, inventario, facturación y CRM, que actúa como plataforma

central de gestión. Este sistema permitirá registrar pedidos, reflejar movimientos de almacén, actualizar el inventario en tiempo real y generar la documentación administrativa asociada a cada operación, integrando en un único entorno funciones que hoy se realizan de forma parcialmente manual o con herramientas no conectadas (Wolters Kluwer, 2026).

El segundo componente es la base de datos relacional PostgreSQL, que actúa como repositorio central de la información. Odoo Enterprise se sustenta de forma nativa sobre este motor, por lo que su elección garantiza la coherencia entre la plataforma de gestión y el modelo de datos corporativo definido en el capítulo 13. La bibliografía especializada en sistemas de información empresariales insiste en que la base de datos es el elemento que asegura la integridad, la consulta estructurada y el aprovechamiento posterior de los datos generados por la actividad de la organización (Forés Julián et al., 2015). El tercer componente es el portal web corporativo, accesible desde navegador, que servirá como punto de interacción tanto para el personal interno como para determinadas consultas externas, manteniendo coherencia con la plataforma central y evitando el desarrollo de una interfaz empresarial completa desde cero. El cuarto componente es la solución específica para reparto y operaciones móviles, descrita en detalle en el apartado 11.4.

11.3 Tecnologías propuestas

Desde el punto de vista tecnológico, la solución se apoya en una selección de herramientas que prioriza la integración, la sostenibilidad del mantenimiento y la adecuación al contexto de una pyme en fase de consolidación. En la capa de presentación, las interfaces web de Odoo Enterprise proporcionan acceso estructurado para administración, logística, comercial y seguimiento de entregas, sin necesidad de desarrollar frontales propios para cada área. Este enfoque reduce significativamente los costes de implantación y garantiza que las actualizaciones de la plataforma no requieran refactorizaciones paralelas en componentes auxiliares.

En la capa lógica, la arquitectura se apoya en los mecanismos de integración de Odoo Enterprise mediante APIs REST y conectores nativos. Para automatizaciones complementarias, tareas auxiliares e integraciones puntuales, Python resulta especialmente adecuado, tanto por su encaje con el ecosistema de Odoo como por su utilidad para importar datos, generar informes, programar tareas de sincronización o producir documentación operativa de forma automatizada. Esta separación entre plataforma de gestión centralizada y automatizaciones auxiliares en

Python es coherente con un modelo progresivo de digitalización, en el que no toda mejora debe convertirse en una aplicación compleja desde el primer momento. En la capa de datos, PostgreSQL como motor relacional garantiza la consistencia del modelo, la integridad referencial entre entidades y la capacidad de escalar el volumen de datos sin degradar el rendimiento de las consultas (Forés Julián et al., 2015).

11.4 Solución específica para reparto y operaciones móviles

Uno de los puntos donde la digitalización puede aportar mayor valor inmediato en PacketRoute S.L. es el proceso de reparto. En la situación actual, la asignación de entregas y la confirmación del servicio dependen en exceso de comunicación informal y de registros poco estructurados, lo que genera pérdidas de trazabilidad y dificulta la respuesta ante incidencias. La literatura sobre logística y trazabilidad destaca que registrar el estado del pedido y su localización a lo largo del proceso de distribución es un requisito básico para reducir incidencias y mejorar la calidad del servicio al cliente (Triangle, 2025; Marco, 2026).

Para dar respuesta a esta necesidad, la propuesta incorpora una solución móvil ligera para el personal de reparto, orientada a consultar las entregas asignadas, registrar estados, comunicar incidencias y confirmar la entrega con marca temporal. En la fase inicial, esta capa se plantea como una extensión integrada con Odoo Enterprise mediante interfaz web responsiva o conectores compatibles, priorizando la rapidez de implantación, el menor coste y la sencillez de mantenimiento frente al desarrollo de una aplicación móvil nativa completamente a medida. Este enfoque permite que los repartidores accedan al sistema desde sus dispositivos con una experiencia funcional adecuada, sin que la empresa deba asumir los costes y los riesgos asociados al desarrollo y mantenimiento de una app propia en esta primera etapa.

11.5 Representación visual de la arquitectura propuesta

Con el fin de complementar la descripción técnica de los apartados anteriores, el proyecto incorpora un diagrama de componentes que representa la arquitectura funcional propuesta para PacketRoute S.L. Este tipo de representación resulta especialmente adecuada cuando se desea documentar una solución modular basada en aplicaciones conectadas, ya que permite mostrar los componentes principales del sistema y las dependencias existentes entre ellos de forma clara y estructurada.

El diagrama se organiza en tres capas: acceso, negocio y datos. En la capa de acceso se sitúan los distintos puntos de interacción con el sistema: el portal web para clientes y personal interno, la interfaz móvil de los repartidores y los accesos administrativos. La capa de negocio concentra los servicios que coordinan la operativa principal de la empresa, especialmente la gestión de pedidos, stock, facturación, clientes e incidencias, todos ellos articulados desde Odoo Enterprise. Por debajo de estas dos capas se encuentra la base de datos central PostgreSQL y el entorno de almacenamiento documental, que actúan como soporte común para garantizar la trazabilidad de la información y la disponibilidad de los datos empresariales en todo momento. La representación descrita refleja una solución modular en la que los componentes están conectados mediante una lógica integrada, coherente con el objetivo de centralizar procesos, reducir tareas manuales y facilitar una implantación escalable.

12 Seguridad informática y gestión de identidades

12.1 Enfoque general de seguridad

El modelo de seguridad informática propuesto para PacketRoute S.L. se articula en torno a los principios del NIST Cybersecurity Framework 2.0, que organiza las capacidades de seguridad en seis funciones: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar (NIST, 2024). Este marco resulta especialmente adecuado para pequeñas empresas porque no impone soluciones técnicas específicas, sino que define objetivos de seguridad que cada organización puede alcanzar de forma progresiva y adaptada a su tamaño y contexto. En el caso de PacketRoute, la propuesta no busca implementar controles de seguridad propios de grandes corporaciones, sino garantizar un nivel de protección coherente con los riesgos identificados y con las obligaciones normativas aplicables, en particular el RGPD (Parlamento Europeo y Consejo, 2016), la LOPDGDD (Jefatura del Estado, 2018) y las referencias del ENS en su aplicación a proveedores de servicios a la Administración (CCN-CERT, 2022).

La premisa fundamental del enfoque propuesto es que la seguridad no puede depender únicamente de herramientas técnicas, sino que requiere también políticas claras, formación del personal y procedimientos definidos. Microsoft (2024) subraya que los incidentes de seguridad más frecuentes en pymes no se originan en vulnerabilidades técnicas complejas, sino en contraseñas débiles, permisos excesivos y ausencia de autenticación reforzada. Por este motivo, la propuesta combina medidas técnicas —gestión centralizada de identidades, segmentación de red, cifrado, backups— con medidas organizativas —políticas de uso aceptable, formación básica, procedimiento de respuesta ante incidentes— formando un sistema de seguridad integrado y coherente.

12.2 Gestión de identidades y cuentas de usuario

El pilar central de la gestión de identidades en PacketRoute será la implantación de un servicio de directorio corporativo basado en Samba Active Directory (AD) o, como alternativa, Microsoft Entra ID (anteriormente Azure AD) en su nivel básico, que actuará como repositorio único de usuarios, grupos, equipos y políticas de acceso. La existencia de un directorio centralizado elimina la situación actual, en la que cada aplicación gestiona sus propias

credenciales de forma independiente, y permite aplicar políticas de seguridad uniformes a toda la organización desde un único punto de administración (Microsoft, 2024).

Cada empleado dispondrá de una cuenta nominativa vinculada al directorio corporativo, con nombre de usuario en formato estandarizado (inicial_apellido@packetroute.local) y contraseña que cumpla con la política de complejidad mínima establecida. Se eliminarán todas las cuentas genéricas o compartidas actualmente en uso. Los equipos corporativos se unirán al dominio, de modo que el inicio de sesión quede registrado y auditado, y las políticas de grupo (GPO) puedan aplicarse de forma centralizada para configurar elementos como el fondo de pantalla corporativo, las unidades de red mapeadas, la configuración de actualizaciones o las restricciones de acceso a determinadas funciones del sistema. La siguiente tabla define los grupos de seguridad propuestos y su correspondencia con los perfiles funcionales de la empresa:

Grupo de seguridad	Miembros	Acceso asignado
GRP_Direccion	Director/a general	Todos los recursos, lectura/escritura total
GRP_Administracion	Personal de administración	Documentación administrativa, ERP (módulos de facturación y compras)
GRP_Logistica	Operarios de almacén	ERP (inventario, órdenes de picking), NAS logística
GRP_Comercial	Atención al cliente, comercial	ERP (ventas, CRM), NAS comercial
GRP_Reparto	Repartidores	App móvil de reparto (acceso limitado vía API)
GRP_IT	Administradores de sistemas	Acceso total a infraestructura, cuentas privilegiadas separadas
GRP_RRHH	Recursos humanos	NAS RRHH (datos laborales), acceso restringido a datos de empleados

12.3 Control de accesos y principio de mínimo privilegio

El principio de mínimo privilegio establece que cada usuario, proceso o sistema debe disponer únicamente de los permisos estrictamente necesarios para el desempeño de sus

funciones, y no más. Este principio, ampliamente recogido en los marcos de ciberseguridad de referencia, reduce significativamente el impacto potencial de un error humano, un acceso no autorizado o un incidente de malware, ya que limita el alcance de los daños al contexto de permisos del usuario o proceso comprometido (NIST, 2024).

En PacketRoute, la aplicación del principio de mínimo privilegio se traduce en las siguientes medidas concretas: los permisos sobre carpetas del NAS y sobre los módulos del ERP se asignarán a nivel de grupo, no de usuario individual, lo que facilita la gestión y reduce errores; los administradores de sistemas dispondrán de una cuenta privilegiada separada de su cuenta de usuario habitual, que utilizarán exclusivamente para tareas de administración; ningún usuario tendrá permisos de escritura sobre directorios que no correspondan a su área funcional; y el acceso a los datos de carácter personal —clientes, empleados— quedará restringido a los grupos con necesidad operativa justificada, en cumplimiento del RGPD y la LOPDGDD (Parlamento Europeo y Consejo, 2016; Jefatura del Estado, 2018).

12.4 Autenticación reforzada y protección de credenciales

La autenticación multifactor (MFA) se implantará para todos los accesos remotos y para el acceso a los sistemas más sensibles desde dentro de la red corporativa. Microsoft (2024) señala que la MFA reduce en más de un 99% el riesgo de compromiso de cuentas en entornos corporativos, ya que añade una segunda capa de verificación —habitualmente un código temporal generado por aplicación o SMS— que hace inútil el robo de contraseñas por sí solo. En PacketRoute, la MFA se activará inicialmente para el acceso VPN, para el panel de administración del servidor Proxmox, para el acceso al panel de Odoo con perfil de administrador o dirección y para el correo corporativo en Microsoft 365.

Las contraseñas corporativas seguirán una política de complejidad mínima: longitud de al menos 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos, sin reutilización de las últimas 5 contraseñas y con renovación obligatoria cada 180 días para cuentas estándar y cada 90 días para cuentas privilegiadas. Se desplegará un gestor de contraseñas corporativo —por ejemplo, Bitwarden Teams— para facilitar el cumplimiento de esta política sin que suponga una carga operativa excesiva para los empleados. Queda expresamente prohibido el uso de contraseñas por defecto en cualquier dispositivo o sistema, y

el departamento de IT será responsable de verificar el cumplimiento de esta restricción en cada nuevo dispositivo incorporado a la red

12.5 Políticas internas, trazabilidad y respuesta básica ante incidentes

La componente organizativa de la seguridad se materializa en la definición de una Política de Seguridad de la Información de PacketRoute S.L., documento interno que recoge las normas de uso aceptable de los sistemas, las responsabilidades del personal, los procedimientos básicos de respuesta ante incidentes y los criterios de clasificación de la información. Este documento se redactará en un lenguaje accesible para todo el personal y formará parte del proceso de incorporación de nuevos empleados, que deberán firmar su recepción y aceptación como condición previa al acceso a los sistemas corporativos.

En materia de trazabilidad, todos los sistemas críticos —servidor Proxmox, Odoo, Samba AD, NAS, firewall— mantendrán registros de auditoría (logs) que documenten los accesos, las modificaciones de configuración y los eventos de seguridad relevantes. Estos logs se centralizarán en la máquina virtual de monitorización (VM-MON) mediante una solución de gestión de eventos, como Graylog o el stack ELK en versión básica, y se conservarán durante un mínimo de doce meses conforme a las recomendaciones del ENS y a las exigencias del RGPD en materia de trazabilidad de tratamientos (CCN-CERT, 2022; Parlamento Europeo y Consejo, 2016).

El procedimiento básico de respuesta ante incidentes establecerá, como mínimo, los siguientes pasos: detección y clasificación del incidente, contención inmediata —aislamiento del equipo o segmento afectado—, notificación al responsable de IT y, si procede, a dirección, análisis de la causa raíz, restauración del servicio desde backup verificado, documentación del incidente y revisión de medidas preventivas. En caso de que el incidente implique una brecha de datos personales, se activará el protocolo de notificación a la Agencia Española de Protección de Datos (AEPD) en el plazo de 72 horas establecido por el RGPD, conforme a lo dispuesto en el artículo 33 del Reglamento (Parlamento Europeo y Consejo, 2016; AEPD, 2024).

12.6 Relación con la protección de datos

La gestión de identidades y el control de accesos propuestos no son únicamente medidas de seguridad técnica: constituyen también la base del cumplimiento de las obligaciones en

materia de protección de datos personales. El RGPD establece que las organizaciones deben implementar medidas técnicas y organizativas apropiadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que tratan, teniendo en cuenta los riesgos asociados a cada tratamiento (Parlamento Europeo y Consejo, 2016). La LOPDGDD complementa esta exigencia en el ordenamiento jurídico español, añadiendo disposiciones específicas sobre los derechos digitales de los trabajadores y el tratamiento de datos en el ámbito laboral, especialmente relevantes en una empresa con una plantilla de treinta y cinco personas (Jefatura del Estado, 2018).

En PacketRoute, los tratamientos de datos personales identificados son, al menos, los siguientes: datos de clientes para la gestión de pedidos y facturación, datos de empleados para la gestión laboral y nóminas, y datos de repartidores y terceros vinculados a la operativa. Para cada uno de estos tratamientos, la empresa deberá mantener el Registro de Actividades de Tratamiento exigido por el artículo 30 del RGPD, designar un responsable interno de protección de datos —que en este caso puede ser el responsable de IT—, y garantizar que los derechos de acceso, rectificación, supresión y portabilidad de los interesados puedan ejercerse de forma efectiva. La implantación del directorio corporativo, el control de permisos y la política de retención de datos que se deriva de la estrategia de backup configuran el conjunto de medidas técnicas que darán soporte a este cumplimiento normativo.

La arquitectura de seguridad descrita en este capítulo actúa de forma transversal sobre todos los demás componentes de la propuesta: los sistemas de información, la infraestructura, la red y la gestión de datos no pueden considerarse seguros de forma aislada, sino que su seguridad depende de la coherencia del modelo global de identidades, accesos y políticas definido en estas páginas. Los capítulos siguientes desarrollan la arquitectura de aplicaciones y la gestión de datos corporativos que se apoyan directamente sobre esta base de seguridad.

13 Virtualización, cloud híbrido y continuidad operativa

13.1 Enfoque general

La virtualización y la adopción de servicios en la nube no son fines en sí mismos, sino instrumentos que permiten a PacketRoute S.L. organizar su infraestructura de forma más eficiente, resistente y escalable. El capítulo anterior ha definido el servidor Proxmox VE como plataforma de virtualización principal y el modelo de cloud híbrido como estrategia de despliegue combinada. Este capítulo profundiza en cómo se articulan estos dos elementos —virtualización local y servicios cloud— para garantizar la continuidad operativa de la empresa ante incidencias técnicas, errores humanos o escenarios de crecimiento que excedan la capacidad inicialmente prevista.

La literatura especializada en infraestructuras para pymes coincide en que un modelo de cloud híbrido combina lo mejor de los entornos on-premise y cloud, siendo especialmente adecuado para organizaciones que desean mantener datos críticos en instalaciones propias sin renunciar a la flexibilidad y escalabilidad de los servicios externos (Beservices, 2024; Inmovement IT, 2025). En el caso de PacketRoute, esta premisa se concreta en mantener en la sede los servicios directamente vinculados a la operativa —ERP, base de datos, almacenamiento primario, autenticación— y externalizar hacia la nube aquellas funciones que se benefician de mayor disponibilidad sin datos especialmente sensibles: copias de seguridad externas, herramientas colaborativas y almacenamiento documental de apoyo).

13.2 Virtualización de servicios

La virtualización de servicios en Proxmox VE permite a PacketRoute alojar en un único servidor físico múltiples entornos lógicos aislados, cada uno con sus propios recursos, sistema operativo y política de actualización. Este aislamiento tiene implicaciones prácticas directas: un fallo en la máquina virtual de la aplicación Odoo no afecta a la base de datos, que reside en una VM independiente; una actualización del sistema de monitorización no interrumpe el servicio de ficheros; y una incidencia de seguridad contenida en un entorno no se propaga automáticamente al resto. Las soluciones de virtualización empresarial con capacidades de snapshot, replicación y migración en caliente —como las que ofrece Proxmox VE— se

identifican como herramientas clave para garantizar la disponibilidad de sistemas críticos en entornos de pyme (Anco, 2024; Icorp, 2023).

En PacketRoute, la virtualización se organiza conforme a la tabla de máquinas virtuales definida en el capítulo 9. Cada VM opera con recursos dedicados y cuotas de CPU y RAM que se ajustan en función de la carga real, con posibilidad de expansión dinámica sin necesidad de reinicio si el hipervisor dispone de capacidad disponible. Los snapshots de cada VM se programan diariamente antes del backup nocturno, de forma que cualquier cambio incorrecto en la configuración de un servicio pueda revertirse en cuestión de minutos restaurando el snapshot del día anterior. Este mecanismo actúa como primera línea de recuperación ante fallos de software o configuración, complementando la política de copias de seguridad estructurada descrita en el capítulo 9.

Adicionalmente, se contempla el uso de contenedores LXC para servicios de menor criticidad o de apoyo, como agentes de monitorización, scripts de automatización o instancias de prueba. Los contenedores comparten el kernel del host y tienen un consumo de recursos significativamente inferior al de una VM completa, lo que permite mantener servicios auxiliares operativos sin comprometer los recursos asignados a los sistemas productivos. Esta combinación de VMs completas para servicios críticos y LXC para servicios auxiliares representa una buena práctica habitual en entornos Proxmox de pequeñas y medianas empresas.

13.3 Estrategia de cloud híbrido

La capa cloud de la infraestructura de PacketRoute se organiza en tres niveles de uso diferenciados. El primer nivel es el de productividad y colaboración, cubierto por Microsoft 365 Business Standard, que provee correo corporativo, Microsoft Teams, SharePoint, Planner y Office Online a todos los usuarios con identidades gestionadas desde Entra ID. Este nivel no aloja datos operativos críticos, sino documentación de trabajo, comunicaciones y coordinación interna, por lo que el riesgo de externalización es bajo y los beneficios en disponibilidad y reducción de administración son elevados.

El segundo nivel es el de almacenamiento y backup externo. El NAS corporativo replica semanalmente su contenido hacia un bucket de almacenamiento cloud cifrado —Azure Blob Storage o Backblaze B2—, y los volcados nocturnos de PostgreSQL se transfieren cifrados mediante rclone al mismo destino. Este nivel garantiza que, ante un siniestro físico en la sede

—incendio, robo o fallo catastrófico del hardware— la empresa disponga de una copia completa de sus datos fuera del edificio, conforme a la regla 3-2-1 descrita en el capítulo 9. Todos los datos almacenados en este nivel están cifrados en tránsito y en reposo, y los registros de acceso al bucket se conservan durante doce meses.

El tercer nivel es el de servicios opcionales en la nube, que incluye principalmente la posibilidad de alojar Odoo Enterprise en modalidad SaaS si la dirección así lo decide en una fase posterior. En esta opción, el servidor de aplicaciones y la base de datos pasarían a ser gestionados por Odoo.com bajo acuerdos de nivel de servicio (SLA) documentados y con transferencias de datos conformes al RGPD. Esta decisión permitiría liberar recursos del servidor Proxmox y reducir la carga de administración, a cambio de ceder el control directo sobre el entorno de la aplicación. La propuesta no prejuzga esta elección, sino que diseña la infraestructura para que ambas opciones —local o SaaS— sean técnicamente viables sin rediseño de la arquitectura de red ni de identidades.

13.4 Continuidad operativa

La continuidad operativa de PacketRoute depende de que los sistemas críticos permanezcan disponibles durante el horario de actividad —habitualmente de 7:00 a 22:00 h— y de que, ante una incidencia que los interrumpa, se pueda restablecer el servicio en el menor tiempo posible y con la menor pérdida de datos aceptable. El proyecto define un RTO (Recovery Time Objective) de cuatro horas y un RPO (Recovery Point Objective) de veinticuatro horas como objetivos de recuperación para los servicios críticos, valores coherentes con el tamaño de la empresa y con la criticidad operativa identificada en el análisis.

Para alcanzar estos objetivos, la estrategia de continuidad se apoya en cuatro mecanismos complementarios. El primero es la redundancia de almacenamiento local mediante RAID en el servidor y en el NAS, que protege frente a fallos de disco sin interrumpir el servicio. El segundo es la política de backups y snapshots automáticos descrita en el capítulo 9, que permite restaurar VMs y datos a un estado conocido. El tercero es el SAI (Sistema de Alimentación Ininterrumpida) en el armario rack, que garantiza la operatividad durante cortes eléctricos de corta duración y permite un apagado controlado del sistema en caso de corte prolongado. El cuarto es la réplica en cloud de los backups críticos, que proporciona una copia fuera de la sede para los escenarios de mayor gravedad.

La siguiente tabla resume los escenarios de incidencia previstos, el mecanismo de recuperación asociado y el tiempo estimado de restauración del servicio:

Escenario	Mecanismo de recuperación	RTO estimado
Fallo de disco individual en servidor	RAID (automático, sin interrupción)	0 minutos
Fallo de configuración en una VM	Restauración de snapshot Proxmox	< 30 minutos
Corrupción o borrado de datos en BD	Restauración de volcado pg_dump	< 2 horas
Fallo total del servidor Proxmox	Restauración desde backup NAS o cloud en nuevo hardware	< 4 horas
Siniestro físico en la sede	Restauración desde backup cloud en infraestructura alternativa	< 24 horas

13.5 Aplicación práctica en PacketRoute

La estrategia de virtualización y cloud híbrido se integra de forma coherente con todos los demás componentes de la propuesta. La arquitectura de red segmentada del capítulo 10 proporciona el canal de comunicación seguro entre las VMs, los puestos de trabajo y los servicios cloud. El modelo de identidades del capítulo 11 unifica la gestión de accesos tanto a los recursos locales como a Microsoft 365 y a la VPN corporativa, sin multiplicar credenciales. La base de datos y el ERP descritos en el capítulo 13 se ejecutan sobre las VMs definidas en el servidor Proxmox, y sus datos se respaldan mediante la política de backup integrada en VM-MON. Este encadenamiento entre capas —física, de red, de identidad, de aplicación y de datos— es precisamente lo que distingue una infraestructura diseñada de forma integrada de una acumulación de soluciones parciales, y constituye el objetivo central del presente proyecto de digitalización.

13.6 Representación física de la infraestructura propuesta

La Figura 4 representa la distribución de los servicios virtualizados, la capa de identidad y los mecanismos de continuidad operativa propuestos para PacketRoute S.L. *(véase Figura 4, Apéndice D).*

La distribución descrita garantiza que los elementos más críticos para la operativa diaria —servidor de virtualización, base de datos, NAS y firewall— residan en la sede bajo control directo del responsable de IT, mientras que las copias de seguridad externas y los servicios de colaboración aprovechan la disponibilidad y escalabilidad de la nube. Esta combinación constituye la base física sobre la que se apoya la gestión de datos desarrollada en el capítulo siguiente.

14 Gestión de datos, trazabilidad y protección de datos

La actividad operativa de PacketRoute S.L. genera de forma continua datos relacionados con pedidos, clientes, productos, movimientos de almacén, entregas y facturación. Gestionar estos datos de forma estructurada es una condición necesaria para que el resto de las soluciones propuestas funcionen con coherencia: sin un modelo de datos sólido, los sistemas ERP, CRM y los mecanismos de trazabilidad carecen de base sobre la que operar (Forés Julián et al., 2015). Este capítulo aborda tres dimensiones complementarias: el modelo de datos corporativo, la trazabilidad del ciclo del pedido y el cumplimiento del marco normativo en materia de protección de datos.

14.1 Modelo de datos corporativo

14.1.1 Funcionamiento general del modelo de datos

El sistema de gestión de datos de PacketRoute S.L. se concibe como una capa transversal que da soporte a todas las soluciones propuestas en los capítulos anteriores. Odoo Enterprise, el módulo CRM, el componente de trazabilidad y los mecanismos de facturación convergen en un único modelo relacional centralizado, de manera que cualquier operación realizada desde cualquier sistema quede registrada de forma consistente y trazable (Forés Julián et al., 2015). La implementación se realiza sobre PostgreSQL como sistema gestor de base de datos relacional, con acceso gestionado desde la capa de aplicación de Odoo y lógica interna complementaria definida en PL/pgSQL para procedimientos y triggers.

El modelo sigue los principios de normalización hasta la tercera forma normal (3FN), eliminando redundancias y dependencias transitivas. Esta decisión de diseño garantiza que un mismo dato no se almacene en múltiples tablas, que los cambios se propaguen correctamente a través de las relaciones y que la base de datos pueda escalar sin degradar su coherencia interna a medida que el volumen de actividad de la empresa aumente.

14.1.2 Entidades y relaciones

El modelo se articula en torno a doce entidades que cubren el ciclo operativo completo de la empresa. La entidad Cliente almacena los datos de los destinatarios de pedidos, incluyendo el campo de consentimiento RGPD con fecha de registro y una marca de anonimización

activable. La entidad Proveedor recoge la información de los suministradores de mercancía. Las entidades Categoria y Producto estructuran el catálogo, donde cada producto pertenece a una categoría y dispone de un campo SKU único como identificador comercial. La entidad Stock mantiene la disponibilidad real y reservada por producto en el almacén, mientras que MovimientoStock registra cada variación del inventario con su causa, fecha y usuario responsable.

La entidad central del modelo es Pedido, que conecta cliente, repartidor, estado y fecha, y agrupa las líneas de detalle a través de LineaPedido, donde se especifica el producto, la cantidad y el precio unitario. La entidad EntregaRepartidor registra el resultado de cada intento de entrega con coordenadas GPS, estado y marca de tiempo. La entidad Factura se asocia a un pedido y contiene el importe total, el tipo de IVA y el estado de pago. La entidad Devolucion gestiona el ciclo de las devoluciones con su motivo y estado de resolución. Finalmente, la entidad LogAuditoria registra de forma inmutable las acciones relevantes realizadas sobre los datos: creaciones, modificaciones y eliminaciones, con identificación del usuario y la fecha.

Las relaciones entre entidades responden al siguiente esquema de cardinalidades:

Relación	Cardinalidad	Descripción
Cliente → Pedido	1:N	Un cliente puede tener múltiples pedidos
Pedido → LineaPedido	1:N	Un pedido contiene una o más líneas de producto
Producto → LineaPedido	1:N	Un producto puede aparecer en múltiples pedidos
Pedido → EntregaRepartidor	1:N	Un pedido puede tener múltiples intentos de entrega
Pedido → Factura	1:1	Cada pedido genera exactamente una factura
Pedido → Devolucion	1:N	Un pedido puede generar una o más devoluciones
MovimientoStock → Producto	N:1	Múltiples movimientos afectan a un mismo producto

14.1.3 Restricciones de integridad nativas

La integridad de los datos se garantiza mediante restricciones declaradas directamente en el esquema de la base de datos, antes de que ninguna lógica de aplicación intervenga. Se

aplican claves primarias con tipo SERIAL o UUID según la entidad, claves foráneas con ON DELETE RESTRICT para evitar la eliminación accidental de registros referenciados, restricciones CHECK para validar rangos de valores (por ejemplo, cantidad > 0 en LineaPedido o importe_total >= 0 en Factura) y restricciones UNIQUE para garantizar la unicidad del SKU en Producto y del NIF/CIF en Cliente y Proveedor.

El estado de Pedido se controla mediante un tipo ENUM que limita los valores posibles a: pendiente, confirmado, en_preparacion, en_reparto, entregado, incidencia y cancelado. Esta restricción garantiza que ninguna capa de aplicación pueda registrar un estado no previsto y facilita las transiciones de estado controladas mediante triggers. De forma análoga, el estado de Devolucion se limita a: solicitada, aprobada, rechazada y resuelta, asegurando un ciclo de vida bien definido para cada devolución.

El conjunto completo de restricciones definidas sobre el modelo —incluyendo cláusulas CHECK, ENUM, UNIQUE, NOT NULL y DEFAULT— se recoge íntegramente en el Apéndice H. Su definición sigue el principio de database-first integrity: la protección del dato se establece directamente en el motor, de forma que ninguna capa de aplicación externa pueda eludir las restricciones de integridad *(véase Apéndice H).*

14.1.4 Automatización mediante triggers y procedimientos almacenados

La lógica de negocio que debe ejecutarse de forma automática ante determinados eventos en la base de datos se implementa mediante triggers y funciones PL/pgSQL. Este enfoque garantiza que ciertas reglas críticas se cumplan independientemente de qué capa de aplicación o qué usuario realice la operación, eliminando la posibilidad de que una acción manual o un error en el código de la aplicación omita validaciones esenciales.

Se definen cuatro triggers principales. El primero, `trg_reservar_stock_en_pedido`, se activa tras la inserción de una línea de pedido (AFTER INSERT ON lineapedido) y descuenta la cantidad reservada en la tabla Stock, verificando previamente que el stock disponible sea suficiente. Si la cantidad disponible es insuficiente, lanza una excepción que impide la inserción, asegurando que nunca se confirme un pedido sin disponibilidad real. El segundo, `trg_descontar_stock_en_entrega`, se activa cuando el estado del pedido cambia a 'entregado' (AFTER UPDATE OF estado ON pedido) y convierte la reserva en descuento real del stock, registrando simultáneamente el movimiento en MovimientoStock. El tercero,

`trg_restaurar_stock_en_cancelacion`, se activa ante cancelaciones o incidencias y libera el stock reservado, registrando también el movimiento correspondiente. El cuarto, `trg_auditoria_pedido`, registra en LogAuditoria cualquier cambio de estado en la tabla Pedido, almacenando el estado anterior y el nuevo en formato JSONB para facilitar la auditoría.

Los tres triggers en PL/pgSQL —reducción de stock, auditoría de estados y liberación de reservas por cancelación— junto con el procedimiento almacenado sp_cerrar_pedido se incluyen íntegros en el Apéndice I. Todos ellos operan de forma atómica: si cualquier operación interna falla, el bloque ROLLBACK revierte el conjunto completo, evitando estados inconsistentes en la base de datos *(véase Apéndice I).*

14.1.5 Procedimiento almacenado: gestión de devoluciones

Además de los triggers reactivos, se define un procedimiento almacenado para la gestión completa del ciclo de una devolución. El procedimiento `sp_procesar_devolucion` recibe el identificador de la devolución, la decisión de aprobación o rechazo y una resolución textual opcional. Si la devolución se aprueba, actualiza su estado a 'aprobada', registra la resolución y fecha, y devuelve las unidades al stock mediante un movimiento de tipo 'devolucion'. Si se rechaza, actualiza únicamente el estado y la resolución sin modificar el stock.

El procedimiento almacenado encargado de gestionar el ciclo completo de una devolución —validación del pedido, reversión de stock, actualización de estado y registro de auditoría— se incluye en el Apéndice J *(véase Apéndice J).*

14.1.6 Índices y vistas

Para optimizar el rendimiento de las consultas más frecuentes, se definen índices sobre las columnas más utilizadas en filtros y joins. Los índices prioritarios son: `idx_pedido_cliente` sobre pedido(id_cliente) para acelerar la consulta del historial de pedidos por cliente, `idx_pedido_estado` sobre pedido(estado) para el panel de gestión operativa, `idx_lineapedido_producto` sobre lineapedido(id_producto) para el análisis de ventas por producto, `idx_movimiento_producto_fecha` sobre movimientostock(id_producto, fecha) para el histórico de inventario, e `idx_logauditoria_tabla_fecha` sobre logauditoria(tabla_afectada, fecha) para las consultas de auditoría. Además, tres vistas que simplifican el acceso a la información más consultada desde el ERP y el panel de control.

Los índices y vistas definidos sobre el modelo se recogen en el Apéndice K. Ambas vistas actúan además como capa de control de acceso, permitiendo conceder permisos solo sobre los campos expuestos sin otorgar acceso directo a las tablas subyacentes *(véase Apéndice K).*

14.2 Replicación, backup y análisis de datos

La base de datos PostgreSQL se configura con replicación de streaming hacia un servidor secundario —en una segunda VM en el mismo Proxmox o en un segundo nodo físico en fases posteriores— mediante el protocolo de replicación nativo de PostgreSQL. Esta configuración establece una réplica de lectura en caliente (hot standby) que permite distribuir la carga de consultas analíticas sobre el secundario y actuar como nodo de recuperación ante un fallo del servidor primario, reduciendo el RTO de la base de datos a un tiempo mínimo de conmutación manual o semiautomática (NIST, 2024).

Los volcados completos de la base de datos se programan nocturnamente mediante pg_dump, generando un archivo comprimido con marca de tiempo que se transfiere automáticamente al NAS corporativo y, en una segunda fase, al almacenamiento cloud cifrado mediante rclone. El ciclo de retención automatizado, gestionado por scripts en cron, elimina las copias que superan el período de conservación definido: siete días para las copias diarias, cuatro semanas para las semanales y doce meses para las mensuales. Zabbix verifica diariamente que las copias se hayan completado correctamente y genera una alerta si algún job de backup no finaliza dentro del tiempo esperado.

Para el análisis de los datos generados por la actividad, se propone el uso de Metabase en su versión Open Source, conectado directamente al servidor de réplica PostgreSQL para no impactar en el rendimiento del servidor productivo. Metabase permite crear paneles de control (dashboards) sin necesidad de conocimientos avanzados de SQL, facilitando que el personal directivo y los responsables de área puedan consultar indicadores clave como el volumen de pedidos por día, el porcentaje de entregas exitosas, los productos con mayor rotación, el tiempo medio de preparación o el estado del stock, sin depender del departamento de IT para generar informes. Esta capacidad de análisis autónomo de los datos constituye uno de los activos más relevantes de la digitalización propuesta, ya que permite pasar de una gestión reactiva basada en la intuición a una toma de decisiones apoyada en datos verificados y actualizados (Forés Julián et al., 2015).

14.3 Representación gráfica del modelo

La Figura 5 muestra el diagrama Entidad-Relación completo del modelo de datos corporativo de PacketRoute S.L. El diagrama, elaborado en PlantUML, refleja las doce entidades descritas y sus relaciones de cardinalidad *(véase Figura 5, Apéndice E).*

14.4 Trazabilidad del ciclo del pedido

La trazabilidad del ciclo del pedido es la capacidad de conocer en todo momento en qué estado se encuentra un pedido, quién ha actuado sobre él, cuándo y con qué resultado. Triangle (2025) define la trazabilidad logística como la capacidad de rastrear y documentar la historia, ubicación y recorrido de un producto a lo largo de la cadena de suministro. En PacketRoute, esta capacidad se implementa a través de la combinación del campo de estado en la tabla Pedido, los registros de EntregaRepartidor, los movimientos de MovimientoStock y el log de auditoría, que juntos forman una cadena de eventos vinculada a cada pedido desde su creación hasta su cierre o devolución.

El ciclo de trazabilidad de un pedido sigue la siguiente secuencia de estados y eventos registrados en la base de datos:

Estado pedido	Evento registrado	Tabla afectada
pendiente → confirmado	Validación manual o automática del pedido	pedido, logauditoria
confirmado → en_preparacion	Asignación de tarea al operario de almacén	pedido, logauditoria
en_preparacion (líneas)	Reserva de stock por línea de pedido	stock, movimientostock
en_preparacion → en_reparto	Asignación de repartidor y ruta	pedido, logauditoria
en_reparto → entregado	Confirmación de entrega con coordenadas GPS	entregarepartidor, stock, movimientostock, logauditoria
entregado → (devolución)	Solicitud de devolución por el cliente	devolucion, logauditoria
Resolución devolución	Aprobación o rechazo, ajuste de stock	devolucion, stock, movimientostock

Esta trazabilidad completa garantiza que cualquier incidencia pueda investigarse accediendo a la secuencia de eventos registrada en la base de datos, sin depender de comunicaciones informales entre departamentos. Desde el panel de Metabase, el responsable de IT o de operaciones puede filtrar el historial de un pedido concreto, identificar el momento exacto en que se produjo un error y analizar si el problema responde a un patrón recurrente que deba abordarse de forma sistémica.

14.5 Protección de datos y cumplimiento del RGPD

El diseño del modelo de datos incorpora de forma nativa las medidas técnicas requeridas por el RGPD para el tratamiento de datos personales. Los datos de carácter personal se concentran principalmente en las entidades Cliente, Repartidor y LogAuditoria. El RGPD establece que los datos personales solo pueden conservarse durante el tiempo necesario para los fines para los que se recogen y que, cuando ya no sean necesarios, deben suprimirse o anonimizarse (Parlamento Europeo y Consejo, 2016).

En el modelo propuesto, la entidad Cliente dispone de los campos consentimiento_rgpd, fecha_consentimiento y anonimizado. El campo anonimizado permite ejecutar una operación de pseudonimización sobre los datos del cliente cuando este ejerce su derecho de supresión o cuando expira el período de retención definido en la política de datos: el nombre, el email y el teléfono se sustituyen por valores genéricos no identificables, mientras se conservan los registros de pedidos vinculados por motivos contables y fiscales, cuya retención durante cinco años es obligatoria en virtud de la normativa tributaria española.

El acceso a los datos personales almacenados en la base de datos se controla a nivel de roles de PostgreSQL, alineado con los grupos de seguridad definidos en el capítulo 11. Solo los roles con privilegios explícitos sobre las tablas cliente y repartidor pueden consultar o modificar datos personales; los roles operativos de logística y reparto solo tienen acceso a las columnas funcionales estrictamente necesarias para ejecutar sus tareas. Esta compartimentación técnica de los datos personales se complementa con el Registro de Actividades de Tratamiento exigido por el artículo 30 del RGPD, que la empresa debe mantener actualizado documentando cada tratamiento, su base jurídica, las categorías de datos afectadas y los plazos de conservación definidos (Parlamento Europeo y Consejo, 2016; AEPD, 2024).

El log de auditoría (LogAuditoria) registra de forma automática e inmutable cualquier acción de inserción, modificación o eliminación sobre las tablas que contienen datos personales, identificando el usuario de base de datos responsable y almacenando el estado anterior y posterior de los datos afectados en formato JSONB. Esta trazabilidad de acceso y modificación de datos personales es un requisito implícito del principio de responsabilidad proactiva (accountability) del RGPD, que exige que las organizaciones no solo cumplan la normativa, sino que puedan demostrar ese cumplimiento ante una inspección de la Agencia Española de Protección de Datos (AEPD, 2024).

15 Automatización de procesos

15.1 Automatización de la administración de sistemas

La automatización de las tareas de administración de sistemas reduce la dependencia del factor humano en operaciones repetitivas y críticas, minimiza los errores de configuración y libera al equipo de IT para dedicarse a tareas de mayor valor añadido. En PacketRoute S.L., donde el área de soporte tecnológico opera con recursos reducidos, esta automatización no es una mejora opcional, sino una condición necesaria para que el nuevo entorno sea sostenible sin incrementar la plantilla del departamento. Las herramientas de automatización de infraestructura permiten definir configuraciones como código, aplicarlas de forma consistente sobre múltiples nodos y mantener un registro de cambios auditables, siguiendo el paradigma de Infrastructure as Code (IaC) recomendado en entornos de administración moderna (SEIDOR, 2025).

La herramienta central de automatización de la administración de servidores es Ansible, que se despliega en la máquina virtual VM-MON de Proxmox y se utiliza para gestionar actualizaciones del sistema operativo, despliegue de paquetes, configuración de servicios y aplicación de parches de seguridad sobre todos los nodos del entorno: los cinco servidores virtuales y, opcionalmente, las estaciones de trabajo Linux. Los playbooks de Ansible se almacenan en un repositorio Git privado, lo que garantiza control de versiones, historial de cambios y capacidad de revertir configuraciones en caso de error. Las tareas más relevantes que se automatizan mediante Ansible incluyen la actualización semanal de los sistemas operativos de todas las VMs (sin intervención manual), la configuración uniforme del firewall a nivel de host, la creación automatizada de nuevos usuarios en el sistema operativo cuando se dan de alta en el directorio corporativo, y la verificación del estado de los servicios críticos con reinicio automático en caso de caída inesperada.

En las estaciones de trabajo Windows del personal de oficina, la automatización de configuraciones se gestiona mediante Group Policy Objects (GPO) definidos en Active Directory. Las GPO permiten distribuir de forma centralizada políticas de seguridad, configurar unidades de red mapeadas por perfil de usuario, establecer restricciones de uso del sistema operativo, gestionar actualizaciones de Windows mediante WSUS y desplegar aplicaciones corporativas de forma silenciosa. Esta combinación de Ansible para la capa de servidores Linux

y GPO para los clientes Windows cubre la totalidad del parque tecnológico con una estrategia coherente y sin duplicar esfuerzos.

15.2 Monitorización del entorno tecnológico

La monitorización continua del entorno tecnológico es la capacidad de conocer en todo momento el estado de salud de los sistemas, anticiparse a fallos antes de que impacten en la operativa y disponer de un registro histórico de métricas que facilite el diagnóstico de problemas. En PacketRoute, esta función se implementa mediante Zabbix, una plataforma de monitorización de código abierto que permite supervisar servidores, máquinas virtuales, servicios de red, bases de datos y dispositivos de red desde una única interfaz centralizada, con alertas configurables y umbrales de aviso por correo, SMS o mensaje en Teams (Zabbix, 2024).

Los agentes de Zabbix se instalan en cada máquina virtual del servidor Proxmox y en el NAS corporativo, recogiendo métricas en tiempo real de CPU, memoria RAM, espacio en disco, latencia de red, estado de los servicios críticos (PostgreSQL, Odoo, Samba, Proxmox) y temperatura del hardware. En el switch gestionable y en el firewall pfSense se activa la recogida de datos SNMP, de modo que Zabbix pueda monitorizar también el tráfico de red por interfaz, el estado de los puertos y posibles eventos de seguridad perimetral. Los umbrales de alerta se configuran de forma que el responsable de IT reciba una notificación por Teams y por correo ante cualquier situación que requiera intervención: uso de CPU superior al 90% durante más de cinco minutos, espacio en disco inferior al 15%, caída de un servicio crítico o fallo en el último backup nocturno. Las métricas históricas se conservan durante tres meses en la propia base de datos de Zabbix, lo que permite análisis de tendencias y detección de degradaciones progresivas antes de que se conviertan en incidentes.

15.3 Gestión automática de copias de seguridad

La política de copias de seguridad definida en el capítulo 9 se automatiza íntegramente mediante scripts programados, eliminando la dependencia del factor humano en una de las tareas más críticas del entorno IT. Se programó el siguiente script Bash, programado mediante cron en VM-MON con ejecución a las 00:30 horas, ejecuta el volcado completo de PostgreSQL, lo comprime y lo transfiere cifrado al NAS corporativo y al almacenamiento cloud *(véase Apéndice L)*.

Los snapshots de las máquinas virtuales de Proxmox se gestionan mediante la tarea de backup nativa del hipervisor, configurada desde la interfaz web de Proxmox VE para ejecutarse diariamente a las 23:00 horas sobre las cinco VMs definidas, con destino al NAS corporativo y retención de siete copias. Esta configuración nativa garantiza que los backups de VM no dependan de scripts externos y puedan monitorizarse directamente desde el panel de Proxmox. Zabbix verifica diariamente que los archivos de backup generados existan y tengan un tamaño razonable, generando una alerta en Teams si algún job falla o produce un archivo de tamaño anómalamente pequeño

15.4 Despliegue automatizado de software

La actualización y el despliegue de software en un entorno con múltiples máquinas virtuales es una tarea que, sin automatización, exige intervención individual en cada nodo. En PacketRoute, los playbooks de Ansible gestionan este proceso de forma centralizada, permitiendo aplicar cambios simultáneos y homogéneos sobre todos los nodos del inventario con un único comando.

El playbook de Ansible utilizado para el despliegue y actualización homogénea de software en todos los servidores del inventario se incluye íntegro en el Apéndice M *(véase Apéndice M)*.

La ejecución de este playbook desde VM-MON se programa semanalmente mediante Ansible AWX (la versión open source del panel de control de Ansible), que también registra el historial de ejecuciones y permite revisar el estado de cada tarea por nodo. En las estaciones de trabajo Windows, el despliegue de actualizaciones de seguridad se gestiona mediante Windows Server Update Services (WSUS), configurado para aprobar automáticamente las actualizaciones críticas y de seguridad publicadas por Microsoft y distribuirlas a los equipos cliente durante el horario de baja actividad.

15.5 Diagrama de actividad - Flujo de automatización operativa

La figura 6 muestra el diagrama que representa el flujo automatizado que cubre el ciclo nocturno de mantenimiento, desde la monitorización continua hasta la respuesta ante incidencias *(véase Figura 6, Apéndice F)*.

16 Trabajo remoto y herramientas colaborativas

La capacidad de trabajar de forma remota y de colaborar en tiempo real entre departamentos no es exclusiva de grandes organizaciones. Para PacketRoute S.L., contar con un entorno de trabajo digital cohesionado resulta especialmente relevante en las áreas de administración, atención al cliente e IT, donde buena parte de las tareas no requieren presencia física pero sí acceso continuo a documentación, sistemas y comunicación interna. Este capítulo define la plataforma colaborativa corporativa, el modelo de acceso remoto seguro y el sistema de gestión documental que dan soporte a este entorno, integrándose con la arquitectura de red del capítulo 10 y con el modelo de identidades del capítulo 11.

16.1 Plataforma colaborativa corporativa

La suite Microsoft 365 Business Standard se adopta como plataforma central de productividad y colaboración, en coherencia con la infraestructura de identidades basada en Entra ID (Azure AD) y con la estrategia de cloud híbrido definida en el capítulo 12. Microsoft 365 integra en una única suscripción las herramientas de ofimática, comunicación, gestión de proyectos y almacenamiento en la nube, eliminando la necesidad de contratar soluciones independientes y facilitando la administración centralizada de licencias y permisos desde un único panel (Microsoft, 2024).

Microsoft Teams actúa como núcleo de la comunicación interna, centralizando mensajería instantánea, videollamadas, canales temáticos por departamento y la gestión de reuniones internas. Los documentos de trabajo se almacenan y comparten a través de SharePoint Online, que permite el control de versiones, el acceso por roles y la edición simultánea desde cualquier dispositivo, con la posibilidad de recuperar versiones anteriores de cualquier fichero sin intervención del departamento IT. Microsoft Planner gestiona las tareas operativas de los equipos de administración e IT con tableros Kanban que ofrecen visibilidad del estado de cada actividad. Esta integración entre comunicación, documentación y gestión de tareas dentro de un mismo ecosistema reduce la fragmentación de la información, uno de los problemas estructurales identificados en el diagnóstico de la empresa.

La siguiente tabla resume la asignación de herramientas Microsoft 365 por perfil de usuario en PacketRoute:

Herramienta	Administración/ Contabilidad	Comercial/Atención cliente	Logística/ Almacén	Reparto	IT/Dirección
Outlook (correo)	✓	✓	✓	✓	✓
Teams (mensajería)	✓	✓	✓	Lectura	✓
SharePoint (documentos)	✓	✓	Solo logística	—	✓
Planner (tareas)	✓	✓	—	—	✓
Forms (formularios)	✓	✓	—	✓ entrega	✓

16.2 Acceso remoto seguro

El modelo de acceso remoto de PacketRoute S.L. se articula sobre la VPN corporativa WireGuard configurada en el firewall pfSense del capítulo 10, combinada con la autenticación multifactor del capítulo 11. Esta combinación garantiza que cualquier conexión desde el exterior cifre el tráfico en tránsito y verifique la identidad del usuario antes de conceder acceso a los recursos internos, siguiendo el principio de confianza cero en el acceso desde redes no controladas (Skyone, 2025).

El acceso remoto se segmenta por perfil de usuario. El personal de administración puede acceder a SharePoint, el ERP y el correo corporativo. El equipo IT accede adicionalmente a la consola de Zabbix, al panel de Proxmox y a los servidores mediante SSH con autenticación por clave. La dirección dispone de acceso a los dashboards de Metabase y a los informes del CRM. Esta segmentación impide que una credencial comprometida en un perfil de bajo privilegio pueda alcanzar sistemas críticos (INCIBE, s.f.). Los dispositivos personales que acceden a recursos corporativos en remoto quedan restringidos a un entorno controlado, evitando que datos sensibles se almacenen en equipos fuera del perímetro corporativo.

16.3 Gestión documental digital

La situación de partida de PacketRoute refleja una gestión documental dispersa entre correos electrónicos, carpetas locales no sincronizadas y registros físicos parciales. La propuesta

centraliza toda la documentación corporativa en dos capas complementarias: SharePoint Online para la documentación de trabajo y colaboración en tiempo real, y el NAS corporativo para el archivo de documentación operativa de larga retención —contratos, facturas, albaranes físicos— con acceso controlado por VPN desde dentro de la red corporativa.

SharePoint Online se organiza en bibliotecas de documentos por departamento, con permisos heredados de los grupos de Entra ID definidos en el capítulo 11: la biblioteca de Administración solo es accesible para GRP_Administracion y GRP_Direccion; la de Logística únicamente para GRP_Logistica e IT; la de Comercial para GRP_Comercial y GRP_Direccion. El control de versiones está activo en todas las bibliotecas, con retención de hasta cincuenta versiones anteriores y restauración en un clic. En el entorno logístico, los repartidores pueden acceder desde su dispositivo móvil a los albaranes de entrega del día mediante Microsoft Forms, registrar la firma digital del receptor y sincronizar el estado de entrega con el ERP en tiempo casi real, cerrando el ciclo de trazabilidad definido en el capítulo 13. Los documentos con valor legal —contratos, facturas, documentación fiscal— se configuran con retención automática alineada con la política de datos, garantizando el cumplimiento del RGPD también en la capa documental (AEPD, 2024).

17 Impacto de la digitalización

La propuesta de digitalización diseñada para PacketRoute S.L. no se concibe como un conjunto de herramientas tecnológicas aisladas, sino como un modelo de transformación que afecta de forma transversal a la productividad, la eficiencia operativa, la seguridad, la toma de decisiones y la competitividad de la organización. Este capítulo analiza el impacto esperado en cada una de estas dimensiones, contrastándolo con la situación de partida descrita en el diagnóstico tecnológico.

17.1 Productividad

La principal fuente de pérdida de productividad identificada en PacketRoute era la dependencia de procesos manuales y la ausencia de integración entre sistemas, que obligaba al personal a dedicar tiempo a tareas de transcripción, verificación y coordinación informal entre departamentos. La implantación del ERP elimina esta duplicidad al centralizar la gestión de pedidos, inventario, facturación y compras en un único sistema, automatizando el ciclo completo desde la recepción del pedido hasta el cierre contable. Estudios sobre el impacto de la digitalización en pymes del sector logístico reportan incrementos de productividad de hasta un 65% tras la implantación de soluciones integradas de gestión (Red.es, citado en España Digital, 2025), resultado coherente con la envergadura de los cambios propuestos para una organización que partía de una madurez digital media-baja.

En términos concretos, la automatización de la gestión documental mediante SharePoint elimina el tiempo dedicado a buscar versiones de documentos entre carpetas locales y correos electrónicos. La asignación automática de pedidos a través del ERP evita la transcripción manual desde redes sociales. Los scripts de backup automático liberan al responsable de IT de la tarea diaria de gestión de copias. La herramienta de monitorización Zabbix elimina la necesidad de verificar manualmente el estado de los sistemas, ya que cualquier anomalía genera una alerta proactiva. El conjunto de estas mejoras reduce la carga operativa manual del equipo en una estimación conservadora de entre dos y cuatro horas-persona diarias en las áreas de administración e IT, tiempo que puede redirigirse hacia tareas de mayor valor estratégico.

17.2 Eficiencia operativa

La digitalización del ciclo del pedido, la trazabilidad del inventario y la automatización de la preparación y el reparto reducen directamente los tiempos de procesamiento y el margen de error operativo. Investigaciones recientes señalan que la digitalización logística permite reducir los tiempos de ciclo entre un 20% y un 40% y mejorar la precisión del inventario de forma significativa (Ortega Méndez, 2024). En PacketRoute, la transición de un control manual de stock a un modelo gestionado por la base de datos con triggers de reserva automática y alertas de stock crítico en Metabase elimina las discrepancias entre el stock físico y el registrado, uno de los problemas operativos más recurrentes detectados en el diagnóstico.

La introducción de trazabilidad completa del pedido, desde su registro hasta la confirmación de entrega con geolocalización, permite también medir por primera vez indicadores de rendimiento operativo reales: tiempo medio de preparación, porcentaje de entregas en primer intento, tasa de incidencias por repartidor o productos con mayor frecuencia de devolución. Esta capacidad de medir lo que antes era opaco es, en sí misma, un salto cualitativo en la eficiencia operativa, ya que convierte la gestión de la operativa en un proceso basado en datos verificados en lugar de percepciones subjetivas.

17.3 Seguridad

El impacto en seguridad es quizás el más difícil de cuantificar en términos directos, pero también uno de los más relevantes en términos de riesgo para la empresa. La situación de partida exponía a PacketRoute a riesgos significativos: pérdida irrecuperable de datos ante un fallo de hardware, acceso indiscriminado a recursos corporativos por ausencia de segmentación de red, credenciales compartidas y débiles, y ausencia de trazabilidad de acciones sobre los sistemas. Cualquiera de estos riesgos, de materializarse, podría suponer una interrupción prolongada de la actividad, pérdida de datos de clientes y potenciales sanciones por incumplimiento del RGPD de hasta 20 millones de euros o el 4% de la facturación anual global (Parlamento Europeo y Consejo, 2016).

La propuesta elimina o reduce significativamente todos estos riesgos. El sistema de backup 3-2-1 con verificación automática garantiza la recuperabilidad de los datos críticos con un RPO de 24 horas y un RTO de 4 horas. La segmentación de red por VLAN contiene posibles incidentes dentro del segmento afectado. El directorio corporativo con MFA reduce

drásticamente el riesgo de compromiso de cuentas. Y el log de auditoría inmutable proporciona la trazabilidad necesaria tanto para la investigación de incidentes como para la demostración de cumplimiento del RGPD ante la AEPD (AEPD, 2024).

17.4 Toma de decisiones

Antes de la digitalización, la toma de decisiones en PacketRoute dependía del conocimiento práctico acumulado por ciertas personas y de informes manuales poco frecuentes. La implantación del ERP integrado con Metabase transforma este modelo en un sistema de información que pone a disposición de la dirección y de los responsables de área indicadores actualizados en tiempo real sobre el estado del negocio. Los dashboards de Metabase conectados al servidor de réplica de PostgreSQL permiten consultar sin conocimientos técnicos avanzados métricas como el volumen de pedidos por estado y canal, los productos con mayor rotación, la eficiencia de entrega por repartidor, los márgenes por línea de producto o el estado del stock con alertas de reposición automáticas.

Esta capacidad de análisis autónomo de los datos —sin depender del departamento IT para generar informes— constituye uno de los activos más relevantes de la digitalización propuesta, ya que permite pasar de una gestión reactiva a una toma de decisiones apoyada en datos verificados y actualizados (Forés Julián et al., 2015). A medio plazo, la acumulación de datos históricos abre la posibilidad de análisis predictivos: previsión de demanda por temporada, detección anticipada de clientes con riesgo de churn o planificación de compras a proveedores con base en tendencias de rotación.

17.5 Competitividad

El impacto global de la digitalización sobre la competitividad de PacketRoute S.L. se manifiesta en dos dimensiones: la mejora de la experiencia del cliente y la capacidad de escalar la actividad sin incrementar proporcionalmente los costes operativos. La trazabilidad completa del pedido permite ofrecer al cliente actualizaciones de estado en tiempo real y tiempos de entrega más precisos, elementos que se han convertido en expectativas estándar en el comercio electrónico y que antes PacketRoute no podía garantizar de forma sistemática (Mecalux, 2019). La reducción de errores de stock y de incidencias en el reparto mejora directamente la satisfacción del cliente y reduce los costes asociados a gestión de devoluciones y reclamaciones.

Desde el punto de vista de la escalabilidad, la infraestructura virtualizada y la arquitectura de cloud híbrido permiten a PacketRoute absorber aumentos de volumen —ya sea por crecimiento orgánico o por incorporación de nuevos clientes ecommerce— sin necesidad de rediseñar la infraestructura tecnológica. El servidor Proxmox puede ampliar la capacidad de las VMs existentes o añadir nuevas sin interrumpir el servicio. El ERP en la nube escala automáticamente con la demanda. Y la estructura de red segmentada puede incorporar nuevos segmentos o nuevas sedes sin alterar la topología base. Este potencial de crecimiento ordenado y controlado es, en última instancia, el argumento más sólido a favor de acometer la inversión que se detalla en el capítulo siguiente.

18 Plan de implantación

El plan de implantación define la secuencia de actuaciones necesarias para materializar la propuesta de digitalización descrita en los capítulos anteriores, distribuyendo el trabajo en seis fases con solapes controlados y dependencias funcionales claramente establecidas. El horizonte temporal del proyecto es de dieciséis semanas (cuatro meses) desde la decisión de inicio. Este plazo resulta realista para una empresa del tamaño de PacketRoute si se cuenta con el apoyo de la dirección, la implicación del responsable de IT y la colaboración de un proveedor externo que apoye el despliegue del ERP y la migración de datos. Se asume que las compras de hardware se realizan durante la semana 1 y llegan antes del inicio de la fase 2.

18.1 Fase 1: Análisis y preparación (semanas 1–2)

Esta fase constituye el punto de partida operativo del proyecto. Su objetivo es traducir el diseño técnico a una planificación de ejecución concreta: validar los requisitos de hardware con proveedores, preparar el entorno de red existente para los cambios de la siguiente fase y establecer los procedimientos de comunicación interna con el personal. También se completa en esta fase la auditoría de los datos existentes —registros de clientes, productos y proveedores— para planificar su limpieza y migración al nuevo ERP (Clavei, 2023). Los entregables clave son el inventario tecnológico actualizado y la hoja de ruta de dependencias entre componentes.

18.2 Fase 2: Infraestructura y red (semanas 3–6)

La segunda fase aborda la capa física y de conectividad sobre la que se apoyarán todos los sistemas posteriores. Se lleva a cabo la instalación y configuración del servidor Proxmox VE con las cinco VMs base, el NAS corporativo en configuración RAID 1, la arquitectura de red segmentada con VLANs mediante el switch de capa 3, y el firewall pfSense como perímetro de seguridad. El servidor secundario para replicación PostgreSQL se configura a partir de la semana 4. La fase concluye con la validación de conectividad entre todos los segmentos, el acceso VPN desde el exterior y la operatividad del almacenamiento compartido.

18.3 Fase 3: Seguridad e identidades (semanas 5–7)

Con la infraestructura base operativa, la tercera fase despliega la capa de seguridad y gestión de identidades. Se instala y configura Samba Active Directory o Windows Server AD en VM-AD, se definen las unidades organizativas, grupos y GPOs, y se integra Microsoft Entra ID para la gestión de identidades cloud y el acceso a Microsoft 365. La MFA se activa para todos los usuarios en esta fase, junto con las políticas de contraseñas y el sistema de permisos sobre carpetas compartidas. Zabbix se despliega también en esta fase para comenzar la monitorización del entorno desde el primer momento en que los sistemas están operativos.

18.4 Fase 4: Sistemas de información y base de datos (semanas 6–11)

Esta es la fase de mayor duración y complejidad técnica. Se instala y configura PostgreSQL en VM-DB con el modelo de datos completo definido en el capítulo 13, incluyendo triggers, procedimientos almacenados, índices, vistas y replicación en streaming hacia el nodo secundario. Sobre esta base se despliega Odoo Enterprise en VM-APP, que se parametriza con los datos maestros de PacketRoute: clientes, productos, proveedores, tarifas y flujos de trabajo. La migración de datos se ejecuta en dos etapas: primero los datos maestros limpiados en la fase 1, y después los datos transaccionales históricos necesarios para la continuidad operativa (Corponet, 2026). La fase concluye con pruebas funcionales de los flujos completos —ciclo de pedido, facturación, control de stock— antes de avanzar a la formación de usuarios.

18.5 Fase 5: Automatización, colaboración y herramientas (semanas 10–14)

Con los sistemas core operativos, esta fase despliega las capas de productividad y automatización. Se configuran los playbooks de Ansible, los scripts de backup automatizado del capítulo 14, los dashboards de Metabase y los flujos de trabajo en Microsoft 365 con Teams, SharePoint y Planner. En paralelo, se forma al personal en el uso del ERP, el CRM y las herramientas colaborativas mediante sesiones por departamento adaptadas al perfil de cada área (MRPeasy, 2025). La formación no se concibe como un evento puntual sino como un proceso con sesiones de seguimiento y documentación de procedimientos internos que el personal pueda consultar de forma autónoma.

18.6 Fase 6: Pruebas, ajustes y puesta en producción (semanas 13–16)

La fase final combina pruebas de integración sobre el entorno completo con los ajustes derivados de los resultados de la formación y con la puesta en producción gradual por áreas. El go-live comienza por el área de logística y almacén —el núcleo operativo de la empresa— y se extiende al resto de departamentos en las semanas siguientes (Corponet, 2026). Durante las dos semanas de arranque se mantiene soporte intensivo por parte del equipo IT para resolver incidencias en tiempo real. El plan de recuperación ante desastres se valida también en esta fase mediante una simulación de fallo del servidor principal y restauración desde el nodo secundario.

18.7 Diagrama de Gantt: Cronograma de implantación

La representación visual del cronograma se incluye en el Apéndice G (véase Figura 7, Apéndice G). La siguiente tabla resume las mismas fases en formato compacto:

Fase / Actividad	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
F1: Análisis y preparación	■	■														
F2: Infraestructura y red			■	■	■	■										
F3: Seguridad e identidades					■	■	■									
F4: Sistemas de información						■	■	■	■	■	■					
F5: Automatización y colaboración										■	■	■	■	■		
F6: Pruebas y puesta en producción													■	■	■	■

19 Estimación económica

La presente estimación tiene carácter orientativo y está basada en precios de mercado actuales para los componentes y servicios propuestos. Su objetivo no es definir un presupuesto ejecutivo cerrado, sino ofrecer una valoración aproximada que permita evaluar la viabilidad económica de la propuesta dentro del contexto de una empresa pequeña en fase de consolidación. Los costes se dividen en inversión inicial —hardware, licencias y servicios de implantación— y coste recurrente anual una vez el sistema está operativo.

19.1 Inversión inicial: Hardware

Componente	Descripción	Cantidad	Precio unitario (€)	Total (€)
Servidor Proxmox	Dell PowerEdge T350, 32GB RAM, 2×SSD 1TB RAID1	1	2.800	2.800
NAS corporativo	Synology DS923+, 2×HDD 4TB RAID1	1	950	950
SAI	APC Smart-UPS 1500VA	1	420	420
Switch L3 gestionable	Ubiquiti USW-Pro-24	1	520	520
Firewall	Protectli VP2420 (pfSense)	1	380	380
APs WiFi	Ubiquiti U6-Pro (×2)	2	180	360
Armario rack 12U	Rack cerrado con ventilación	1	310	310
****Total Hardware****				****5.740****

19.2 Inversión inicial: Software y licencias

Concepto	Descripción	Coste (€)
Odoo Enterprise (16 usuarios, 1 año)	Licencia base + módulos ventas, inventario, compras, contabilidad, CRM	4.800
Consultoría implantación ERP	Parametrización, migración de datos, formación inicial (40 h externas)	3.200
Bitwarden Teams (1 año, 35 usuarios)	Gestor de contraseñas corporativo	180
Certificado SSL corporativo (3 años)	Para servicios publicados externamente	90
****Total Software e implantación****		****8.270****

19.3 Coste recurrente anual

Concepto	Descripción	Coste anual (€)
Microsoft 365 Business Standard	35 usuarios × 12,5 €/mes × 12	5.250
Odoo Enterprise (renovación anual)	Licencia 16 usuarios	4.800
Almacenamiento cloud backups	Backblaze B2 ~500 GB/mes	96
Dominio corporativo y DNS	Renovación anual	25
Bitwarden Teams	35 usuarios	180
Mantenimiento hardware (estimado)	SAI baterías, consumibles	200
****Total recurrente anual****		**10.551**

19.4 Resumen de inversión y viabilidad

Concepto	Importe (€)
Inversión inicial total (hardware + software + implantación)	14.010
Coste recurrente anual (año 1 tras implantación)	10.551
Coste total año 1	24.561
Coste total año 2 en adelante (solo recurrente)	10.551

La inversión inicial de 14.010 € representa aproximadamente el coste de un trabajador a tiempo completo durante cuatro meses en el tejido pyme español, una cifra asumible para una empresa que gestiona 70 pedidos diarios y que aspira a crecer en volumen (España Digital, 2025). El retorno sobre la inversión (ROI) se materializa de forma combinada: la reducción de errores de stock elimina costes de devolución y pérdida de mercancía; la automatización de tareas manuales libera horas de trabajo que pueden redirigirse a crecimiento comercial; y la mejora en la experiencia del cliente reduce la tasa de abandono y facilita la captación de nuevos contratos de ecommerce. Con una estimación conservadora de ahorro operativo de 1.500 €/mes a partir del sexto mes de implantación —basada en la reducción de horas manuales y errores operativos—, la inversión inicial quedaría amortizada en aproximadamente dieciocho meses, un horizonte perfectamente razonable para una decisión estratégica de esta naturaleza (Ortega Méndez, 2024).

20 Conclusiones

La propuesta de digitalización desarrollada en este proyecto aborda de forma integral y coherente los desafíos tecnológicos que PacketRoute S.L. enfrenta como empresa logística en fase de consolidación. El análisis de la empresa y el diagnóstico tecnológico previo han permitido identificar con precisión las ineficiencias de partida: procesos manuales sin integración, red plana sin segmentación, ausencia de backups formales, gestión de identidades inexistente y tratamiento de datos personales sin garantías suficientes. La propuesta formulada a lo largo de los capítulos 8 al 18 responde de forma directa a cada uno de estos problemas con soluciones técnicas proporcionadas al tamaño de la empresa, fundamentadas en marcos de referencia reconocidos —NIST CSF 2.0, RGPD, LOPDGDD, ENS— y articuladas de manera que formen un sistema coherente en lugar de una acumulación de herramientas aisladas.

El núcleo de la solución es la implantación de Odoo Enterprise como plataforma ERP/CRM sobre un servidor Proxmox VE virtualizado, con una base de datos PostgreSQL diseñada desde cero para PacketRoute e integrada con mecanismos de trazabilidad, triggers de automatización y lógica de negocio embebida. Esta capa de datos se complementa con una infraestructura de red segmentada en cinco VLANs, un firewall pfSense como perímetro de seguridad, VPN WireGuard para acceso remoto y WiFi corporativa con SSID separados. La gestión de identidades centralizada en Active Directory con MFA, los scripts de automatización en Bash y Ansible, los backups automáticos con verificación mediante Zabbix, y la plataforma colaborativa Microsoft 365 completan un ecosistema tecnológico que transforma radicalmente el modelo de funcionamiento de la empresa.

Desde el punto de vista normativo, el proyecto integra el cumplimiento del RGPD y la LOPDGDD no como una capa añadida, sino como una dimensión transversal del diseño: el modelo de datos incluye campos de consentimiento y anonimización, los permisos se asignan conforme al principio de mínimo privilegio, el log de auditoría proporciona la trazabilidad de accesos y modificaciones sobre datos personales, y la política de retención documental en SharePoint se alinea con los plazos legales de conservación. Este enfoque de privacidad desde el diseño (privacy by design) es precisamente el que el RGPD espera de las organizaciones responsables del tratamiento (Parlamento Europeo y Consejo, 2016).

El impacto esperado es significativo en todas las dimensiones analizadas: productividad, eficiencia operativa, seguridad, toma de decisiones y competitividad. La estimación de retorno

sobre la inversión sitúa el punto de equilibrio en torno a los dieciocho meses, con una inversión inicial de 14.010 € asumible para el perfil de la empresa y un coste recurrente anual de 10.551 € coherente con los beneficios operativos y estratégicos generados. La planificación en seis fases durante dieciséis semanas garantiza una implantación ordenada, con pruebas antes del go-live y soporte intensivo durante el arranque.

La transformación digital propuesta no agota todas las posibilidades futuras de PacketRoute, sino que establece la base tecnológica sobre la que la empresa podrá construir mejoras en etapas posteriores: automatización avanzada de rutas de reparto, análisis predictivo de demanda, integración de dispositivos IoT en el almacén o expansión hacia nuevas sedes. Precisamente por ello, todos los componentes de la arquitectura han sido diseñados con criterios de escalabilidad: el servidor Proxmox es ampliable sin rediseño, el modelo de datos es extensible, la arquitectura de red admite nuevos segmentos y la gestión de identidades en la nube escala con el número de usuarios. En este sentido, el presente proyecto no concluye con la puesta en producción del sistema, sino que la identifica como el punto de partida de una organización que, por primera vez, dispone de la base tecnológica necesaria para crecer de forma ordenada, segura y competitiva.

20.1 Nota sobre herramientas de elaboración

El presente proyecto ha sido elaborado íntegramente por el autor, Julio Isaac Navarro Navarrete, como trabajo final del ciclo de Administración de Sistemas Informáticos en Red (ASIX I) del CIFP Francesc Borja Moll de Palma, bajo la supervisión del profesor Bartomeu Segura Duran. Para la redacción, estructuración y revisión del documento se ha utilizado asistencia de herramientas de inteligencia artificial generativa como apoyo en la formulación de ideas y en la expresión escrita, sin que esto implique en ningún caso que el análisis, el diseño técnico, la toma de decisiones o el juicio profesional hayan sido delegados en dichas herramientas. Toda la arquitectura técnica, las decisiones de diseño, el modelo de datos, el código SQL y los scripts incluidos en este documento han sido diseñados, validados y supervisados por el autor, quien asume la responsabilidad íntegra del contenido presentado.

Los diagramas incluidos en los apéndices del presente proyecto han sido elaborados mediante PlantUML, una herramienta de diagramación basada en texto que permite generar representaciones visuales estructuradas a partir de código descriptivo en lenguaje plano

(PlantUML, 2024). Este enfoque permite mantener los diagramas bajo control de versiones, modificarlos con precisión y exportarlos en formatos de alta resolución SVG sin depender de herramientas de diseño gráfico.

PlantUML soporta de forma nativa la notación UML estándar, lo que ha permitido generar el organigrama de componentes (Figura 1), el diagrama de actividades del proceso operativo (Figura 2), los diagramas de arquitectura de seguridad (Figuras 3 y 4), el diagrama entidad-relación del modelo de datos (Figura 5), el diagrama de flujo de automatización (Figura 6) y el diagrama de Gantt de implantación (Figura 7), todos ellos coherentes con la notación empleada en el marco teórico y en la propuesta técnica del proyecto. La sintaxis de cada diagrama fue definida manualmente por el autor a partir de los requisitos técnicos de cada apartado, garantizando que el contenido representado responde al diseño propio del proyecto y no a una generación automática de contenido.

21 Referencias Bibliográficas

Agencia Española de Protección de Datos (AEPD). (2024). Guía práctica para las evaluaciones de impacto en la protección de los datos personales. https://www.aepd.es

Centro Criptológico Nacional (CCN-CERT). (2022). Esquema Nacional de Seguridad: guía de implantación. https://www.ccn-cert.cni.es

Clavei. (2023). Implementación de un ERP: ¿por dónde empezamos? https://www.clavei.es/blog/implementacion-de-un-erp/

Cloudflare. (2024). ¿Qué es el principio de privilegio mínimo? Zero Trust. https://www.cloudflare.com/es-es/learning/access-management/principle-of-least-privilege/

Compusoluciones. (2025). Automatización híbrida: Linux y Windows con Ansible. https://www.compusoluciones.com/blog/automatizacion-hibrida-linux-y-windows-con-ansible/

Corponet. (2026). Etapas de implementación de un ERP para impulsar el crecimiento. https://blog.corponet.com/etapas-de-implementacion-de-un-erp

Cyberzaintza. (2024). Gestión de identidades y accesos. Euskadi.eus. https://ciberseguridad.euskadi.eus/ciberpedia/buenas-practicas/gestion-de-identidades-y-accesos/

Databay Solutions. (2025). Guía de implantación Odoo 2025: fases, costes y errores. https://databay.solutions/blog/guia-implantacion-odoo

DC Seguridad. (2025). Guía práctica: cómo hacer segura mi red de la empresa. https://dcseguridad.es/guia-practica-como-hacer-segura-mi-red-de-la-empresa/

Driv.in. (2025). Del papel a la nube: gestión documental digital en logística. https://driv.in/blog/gestion-documental-digital-logistica

España Digital. (2025). El Gobierno presenta el balance del Kit Digital, con más de 860.000 ayudas concedidas. https://espanadigital.gob.es/va/actualidad/el-gobierno-presenta-el-balance-del-kit-digital

Forés Julián, B., Ferrer Gilabert, S., Puig Denia, A., Boronat Navarro, M., y Lapiedra Alcamí, R. (2015a). Bases de datos para la gestión de los sistemas de información en la empresa: una aplicación a través de Access. Universitat Jaume I.

Forés Julián, B., Puig Denia, A., y Fernández Yáñez, J. M. (2015b). Bases de datos. Publicacions de la Universitat Jaume I.

Fustibus. (2025). Proxmox: virtualización económica sin licencias. https://fustibus.com/es/blog/consultoria/proxmox-virtualizacion-economica-sin-licencias

Guerola Navarro, V. (2021). Customer Relationship Management (CRM): gestión de relaciones con los clientes. Universitat Politècnica de València. https://riunet.upv.es/handle/10251/161904

Hotaka. (2025). El poder del trabajo colaborativo: cómo Microsoft Teams está transformando las empresas. https://www.hotaka.io/en_GB/blog/

Ibis Computer. (2024). Cloud híbrida para pymes: flexibilidad y seguridad en la nube. https://ibiscomputer.com/cloud-hibrida-pymes-flexibilidad-seguridad/

Icorp. (2023). Alta disponibilidad como parte de la estrategia operativa de TI. https://icorp.com.mx/blog/alta-disponibilidad-como-parte-de-la-estrategia-operativa-de-ti/

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). Ciberseguridad en el teletrabajo. https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

Initelia. (2024). Aprovecha Microsoft 365 en tu empresa. https://initelia.es/herramientas-de-microsoft-365-para-empresas/

Inmovement IT. (2025). Cloud híbrido vs cloud privado: qué le conviene a tu empresa. https://www.inmoveit.com/cloud-hibrido-vs-cloud-privado-que-le-conviene-a-tu-empresa/

Invgate. (2025). Plan de transformación digital: creación, división por fases y ejecución. https://blog.invgate.com/es/plan-de-transformacion-digital

IONOS. (2025). Precios de Microsoft 365 en 2025: planes y costes. https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/office-365-precios-y-modelos-de-licencia/

IT-Consulting.es. (2025). Monitorización de la salud del servidor: Zabbix y Grafana para alertas en tiempo real. https://it-consulting.es/monitorizacion-de-la-salud-del-servidor-zabbix-y-grafana-para-alertas-en-tiempo-real/

Jefatura del Estado. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Boletín Oficial del Estado, 294. https://www.boe.es/eli/es/lo/2018/12/05/3

Konica Minolta. (2026). Gestión documental y datos en la nube. https://www.konicaminolta.es/es-es/gestion-it-mantenimiento-informatico/gestion-documental-nube-beneficios

Lagahe. (2024). Transformación digital y decisiones basadas en datos: claves para la competitividad empresarial. https://lagahe.com/blog/transformacion-digital-decisiones-basadas-datos-claves-competitividad-empresarial/

Marco, J. A. (2026). Logística 5.0: transporta tu logística al mundo digital. LID Editorial.

MCM Tech. (2025). ¿Cómo garantizar la continuidad operativa con soluciones en la nube? https://blog.mcmtechco.com/continuidad-operativa

Mecalux. (2019). La transformación digital en logística. https://www.mecalux.es/blog/transformacion-digital-logistica

Metabase. (2024). Metabase documentation: open source BI for everyone. https://www.metabase.com/docs/latest/

Microsoft. (2024a). Libro de trabajo: brechas de autenticación multifactor. Microsoft Learn. https://learn.microsoft.com/es-es/entra/identity/monitoring-health/workbook-mfa-gaps

Microsoft. (2024b). Configurar la autenticación multifactor para Microsoft 365. Microsoft Learn. https://learn.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

Microsoft. (2025). Cómo funciona: autenticación multifactor de Microsoft Entra. Microsoft Learn. https://learn.microsoft.com/es-es/entra/identity/authentication/concept-mfa-howitworks

Microsoft Azure. (2024). ¿Qué es el cloud computing? https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-cloud-computing

Ministerio de la Presidencia. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, 106. https://www.boe.es/eli/es/rd/2022/05/03/311

MRPeasy. (2025). Guía de migración de ERP para pequeñas empresas. https://www.mrpeasy.com/blog/es/migracion-de-erp/

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Versión 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2024). El marco de seguridad cibernética (CSF) 2.0 del NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

Object Management Group. (2017). Unified Modeling Language (UML), Version 2.5.1. https://www.omg.org/spec/UML/2.5.1

Openwebinars. (2022). Potencia el trabajo colaborativo con Microsoft 365. https://openwebinars.net/blog/potenciar-el-trabajo-colaborativo-de-tu-equipo-con-microsoft-365

Ortega Méndez, J. X. (2024). Efectos de la transformación digital en la eficiencia operativa de la cadena de suministro. Prometeo Sociedad del Conocimiento, 2. https://dialnet.unirioja.es/servlet/articulo?codigo=10599421

Palo Alto Networks. (s.f.). ¿Qué es el principio del mínimo privilegio? https://www.paloaltonetworks.es/cyberpedia/what-is-the-principle-of-least-privilege

Parlamento Europeo y Consejo. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). Diario Oficial de la Unión Europea, L 119, 1–88. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Perplexity AI. (2025). Perplexity AI: conversational search and research assistant. https://www.perplexity.ai

PlantUML. (2024). PlantUML Language Reference Guide. https://plantuml.com

Protecciondatos-lopd.com. (2024). Responsable del tratamiento de datos: quién es y qué obligaciones tiene. https://protecciondatos-lopd.com/empresas/responsable-tratamiento/

Red Hat. (2026). Ansible: ¿qué es y cómo funciona? https://www.redhat.com/es/topics/automation/learning-ansible-tutorial

SAPI. (2025). Cómo medir el retorno de inversión (ROI) de la transformación digital en una pyme. https://sapi.es/blog/como-medir-el-retorno-de-inversion-roi-de-la-transformacion-digital-en-una-pyme

SAP News Spain. (2024). La digitalización logística: una guía esencial para transformar operaciones. https://news.sap.com/spain/2024/06/la-digitalizacion-logistica/

Seidor. (2025). Automatización estratégica: cómo Ansible transforma las operaciones TI. https://www.seidor.com/es-es/blog/automatizacion-estrategica-ansible-transforma-operaciones-ti

Sirtek. (2025). Cuánto cuesta implementar Odoo en una empresa pequeña. https://www.sirtek.es/cuanto-cuesta-implementar-odoo-en-una-empresa-pequena

Skyone. (2025). VPN para teletrabajo: defensa contra ataques modernos. https://skyone.solutions/es/blog/cibersegua/trabajo_remoto_y_ciberseguridad/

Toyota Forklifts. (2024). La digitalización en el sector logístico: ventajas e importancia. https://blog.toyota-forklifts.es/digitalizacion-logistica

Transworld. (2025). Importancia de la segmentación de red y las VLAN. https://transworld.pe/i-news/importancia-de-la-segmentacion-de-red-y-las-vlan/

Triangle. (2025). Trazabilidad logística: qué es, tipos y su importancia. https://www.triangle.es/noticias/trazabilidad-logistica/

Universitat de València — Departament d'Informàtica. (s.f.). Un sistema de gestión de pedidos: modelo relacional. http://informatica.uv.es/iiguia/DBD/Teoria/capitulo_5.pdf

Vinchin. (2025). ¿Cómo funciona la fijación de precios de Proxmox? https://www.vinchin.com/es/vm-backup/proxmox-pricing.html

VMware. (2024). ¿Qué es la virtualización? https://www.vmware.com/es/topics/glossary/content/virtualization.html

Wolters Kluwer. (2026). Software ERP: qué es, tipologías y ejemplos. https://www.wolterskluwer.com/es-es/expert-insights/que-es-un-software-erp-tipos-y-ejemplos

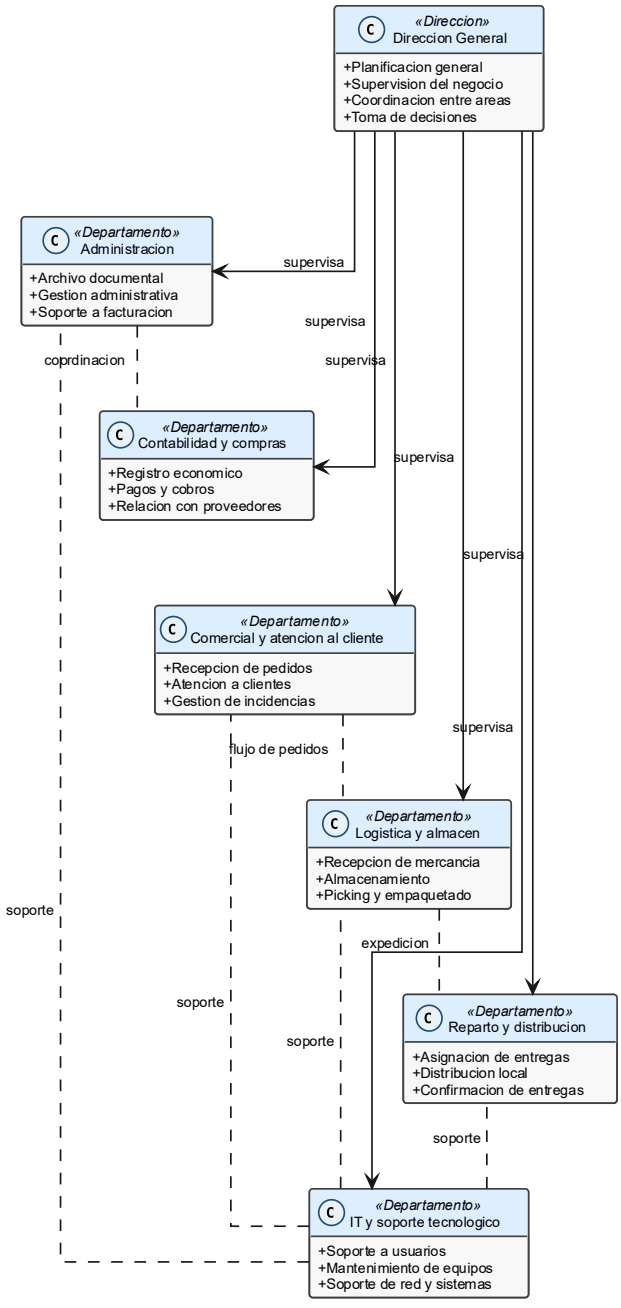
Zabbix. (s.f.). Monitoreo de TI empresarial con Zabbix. https://www.zabbix.com/la/enterprise_monitoring

PlantUML. (2024). PlantUML Language Reference Guide. https://plantuml.com

22 Apéndices

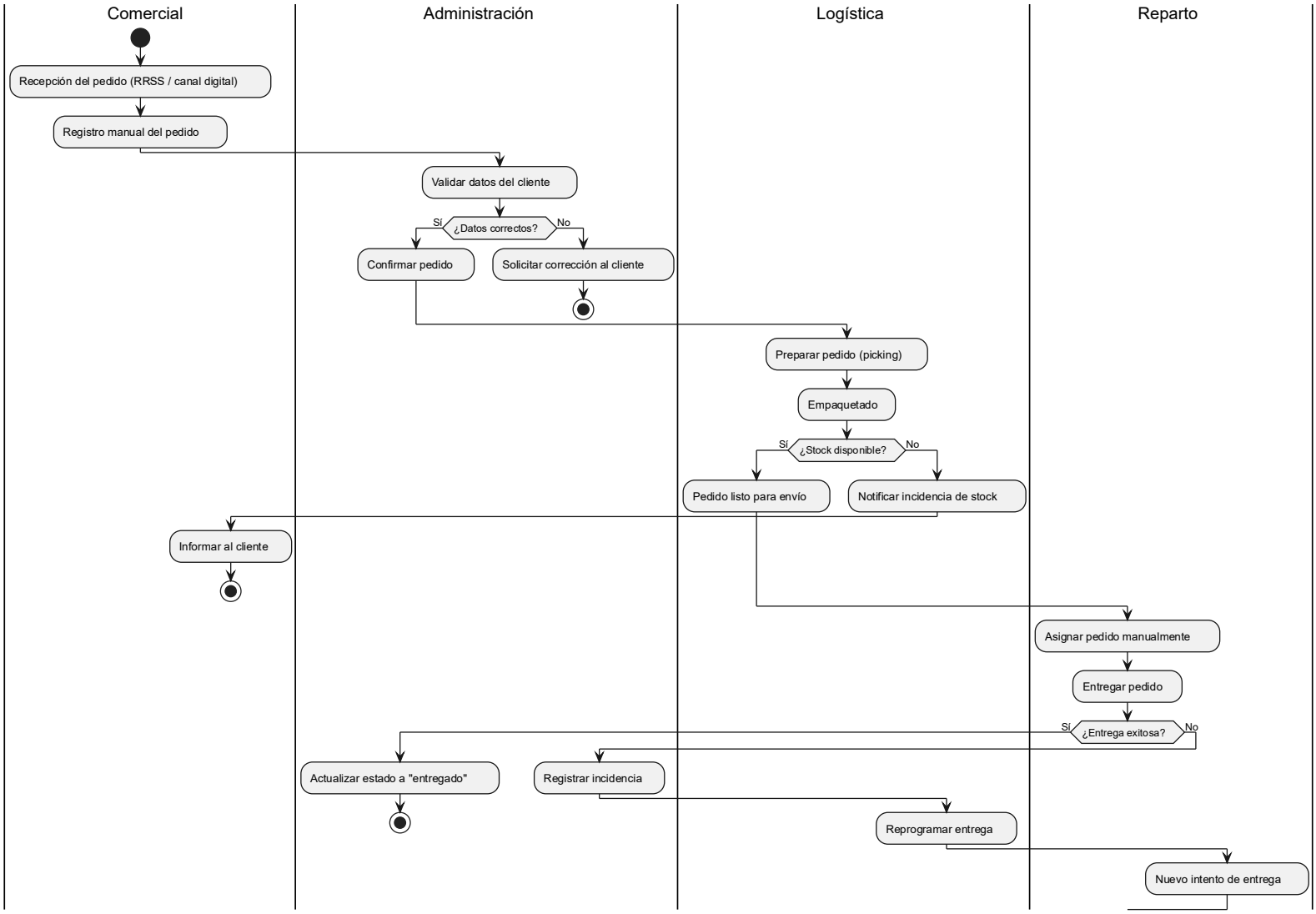
22.1 Apéndice A — Figura 1: Organigrama corporativo de PacketRoute S.L.

La figura muestra la estructura organizativa funcional de PacketRoute S.L., con Dirección General en el nivel superior y las áreas operativas y de soporte distribuidas por departamentos: Administración, Contabilidad y Compras, Comercial y Atención al Cliente, Logística y Almacén, Reparto y Distribución, e IT y Soporte Tecnológico.



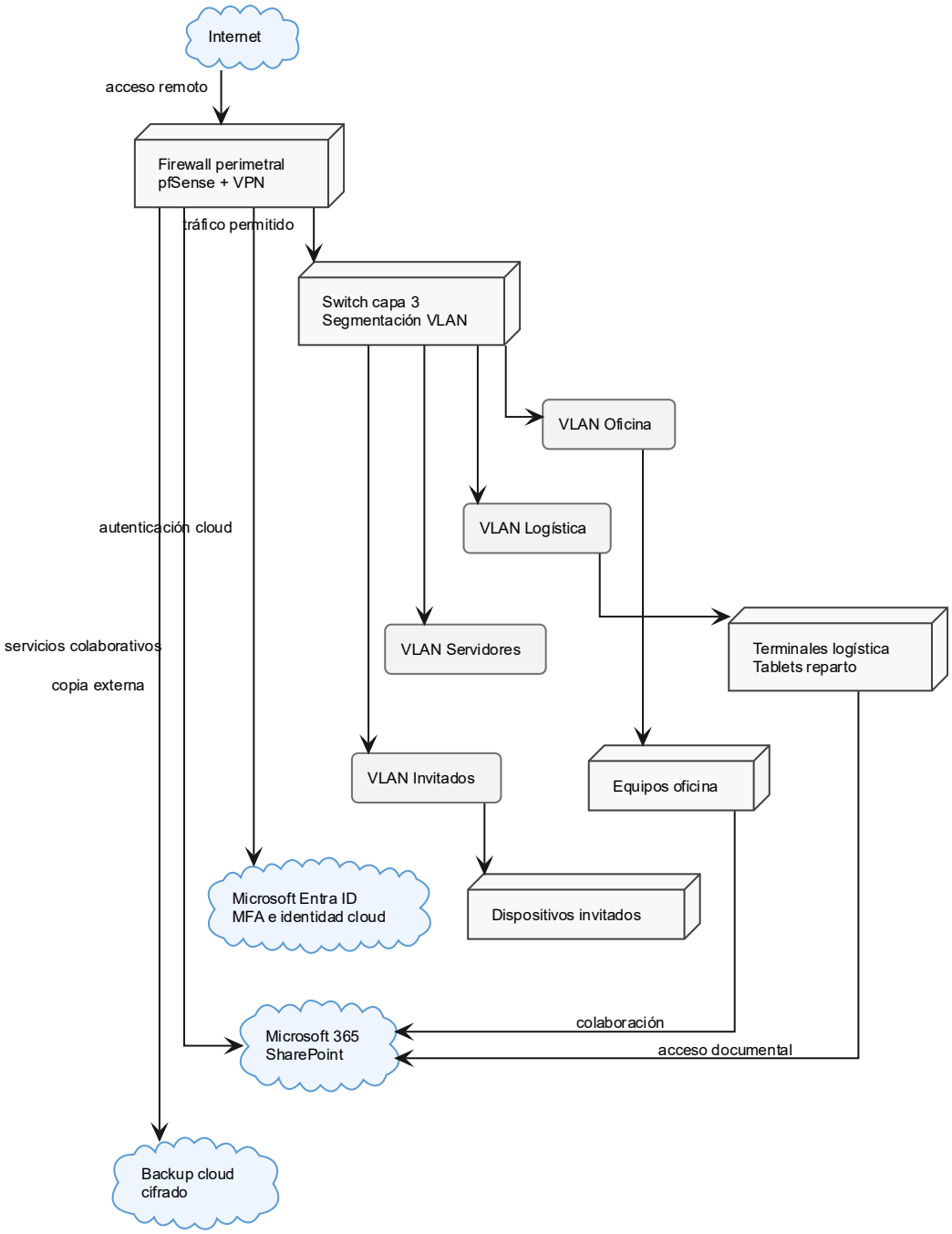
22.2 Apéndice B — Figura 2: Diagrama de actividades del proceso operativo actual

La figura representa el proceso operativo actual de la empresa desde la recepción del pedido hasta su cierre administrativo, distinguiendo la intervención de cada área funcional mediante swimlanes: Comercial/Atención al Cliente, Logística y Almacén, Reparto y Distribución, Administración y Contabilidad, e IT y Soporte.



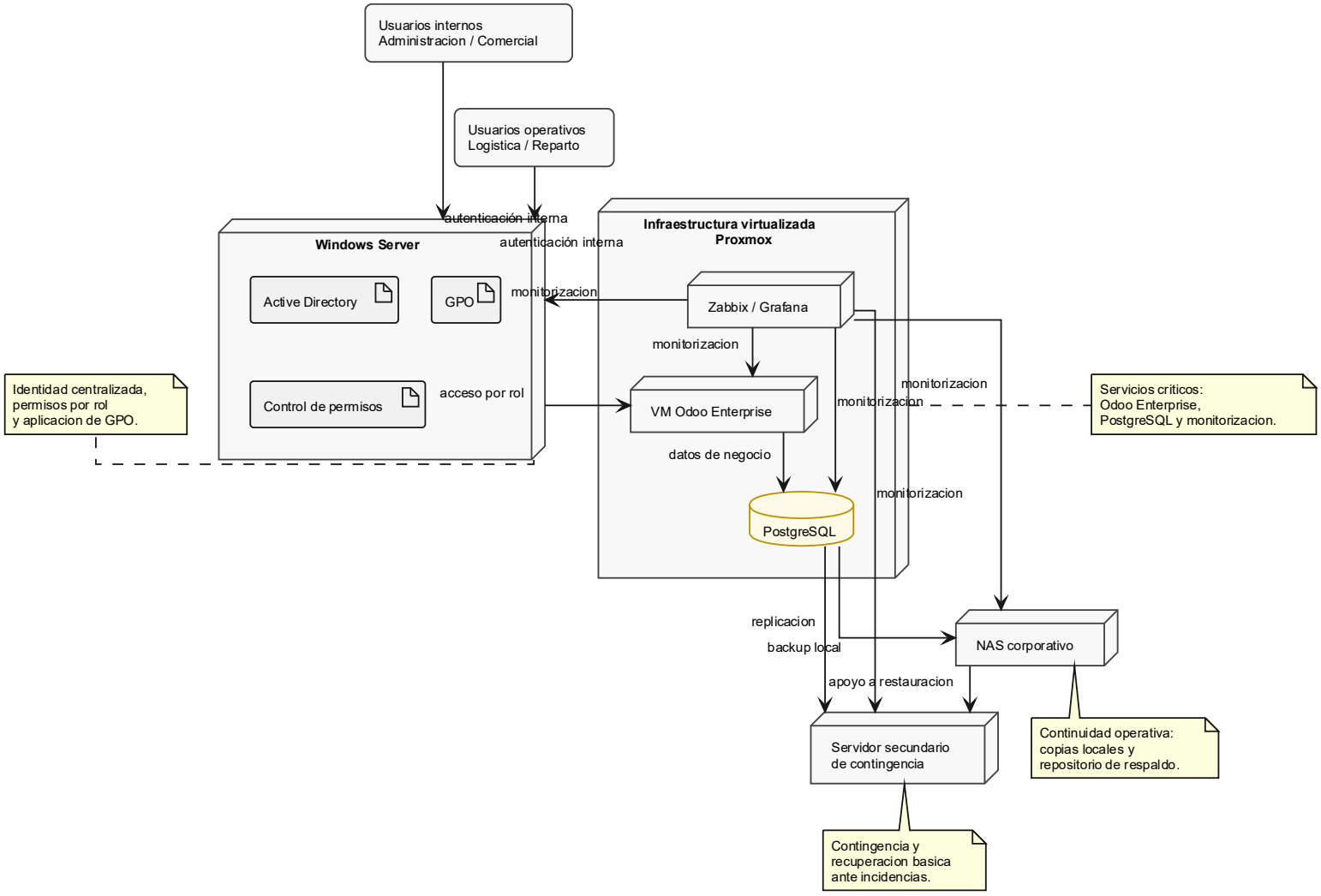
22.3 Apéndice C — Figura 3: Arquitectura de perímetro, red y acceso seguro

La figura muestra la capa de perímetro, red y acceso seguro, incluyendo Internet, firewall pfSense, switch de capa 3, segmentación por VLAN (VLAN10 Oficinas, VLAN20 Servidores, VLAN30 Logística, VLAN40 Reparto/Móvil, VLAN50 Invitados), puntos de acceso WiFi con SSID diferenciados y conexión con los servicios cloud principales (Microsoft 365, Backblaze B2, Odoo Cloud).



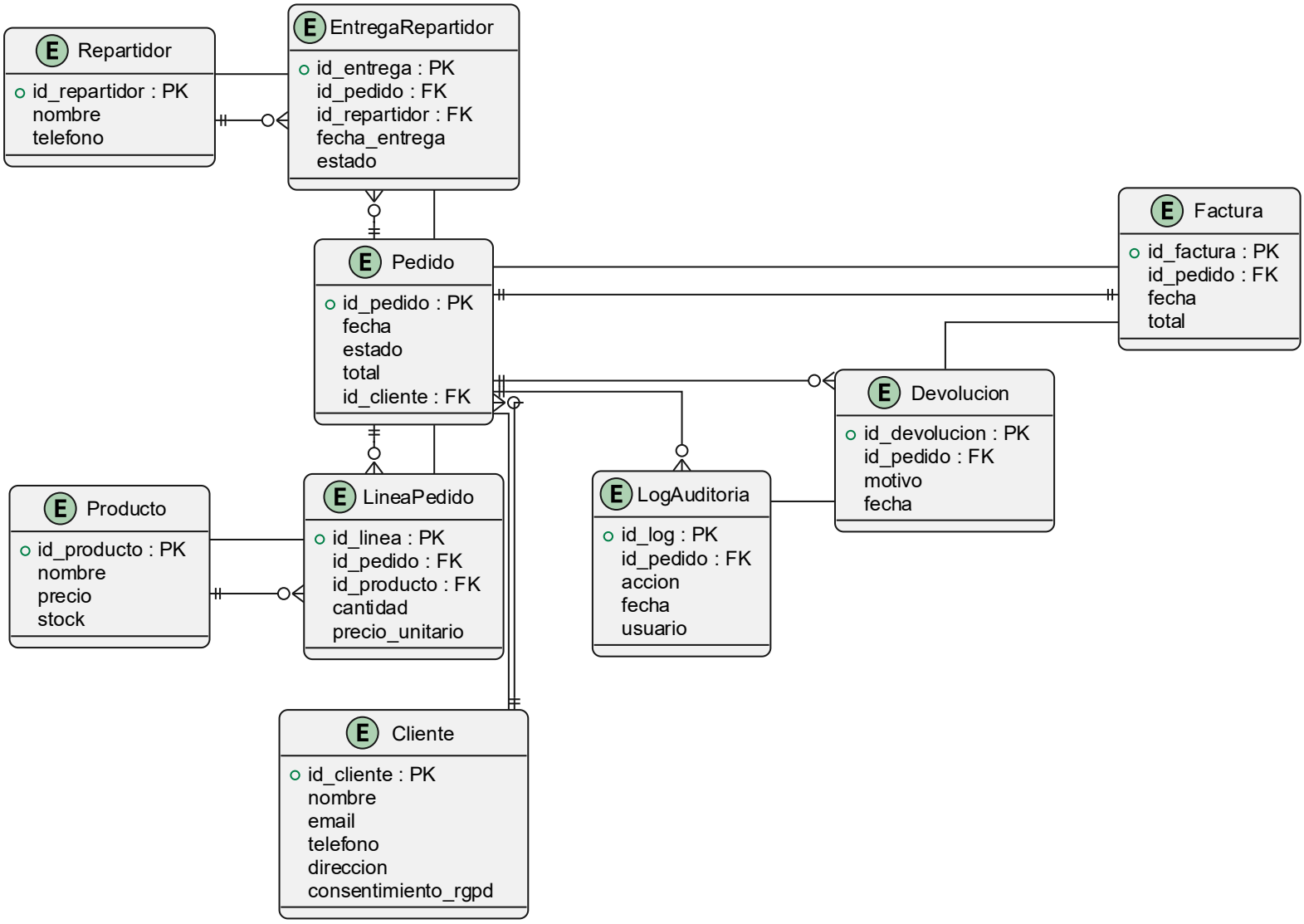
22.4 Apéndice D — Figura 4: Arquitectura de identidad, control de acceso, monitorización y continuidad

La figura representa la capa interna de seguridad, con identidad corporativa centralizada en Active Directory y Microsoft Entra ID, control de permisos por grupos y GPOs, MFA, servicios críticos virtualizados en Proxmox VE (VM-AD, VM-APP, VM-DB, VM-FILE, VM-MON), monitorización con Zabbix y mecanismos básicos de continuidad operativa (servidor secundario de replicación PostgreSQL, NAS corporativo, backups cloud).



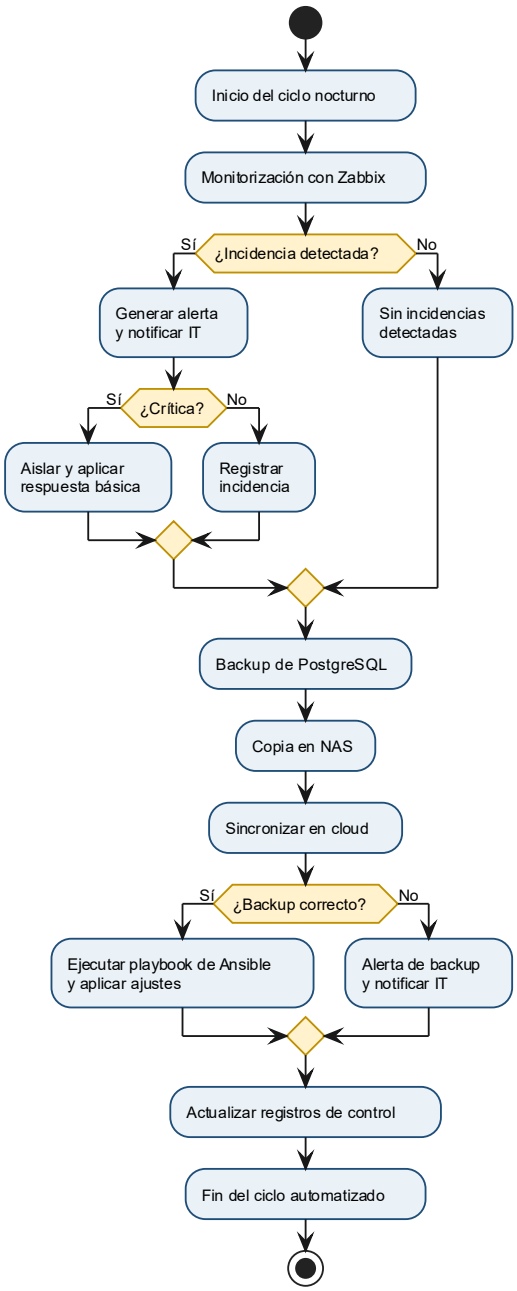
22.5 Apéndice E — Figura 5: Diagrama Entidad-Relación del modelo de datos corporativo

La figura muestra el modelo Entidad-Relación del sistema de datos corporativo de PacketRoute, incluyendo las doce entidades principales (Cliente, Empleado, Proveedor, Producto, Almacen, Pedido, LineaPedido, EntregaRuta, Repartidor, MovimientoStock, AuditoriaRegistro, Devolucion) y sus relaciones estructurales con cardinalidades y claves foráneas.



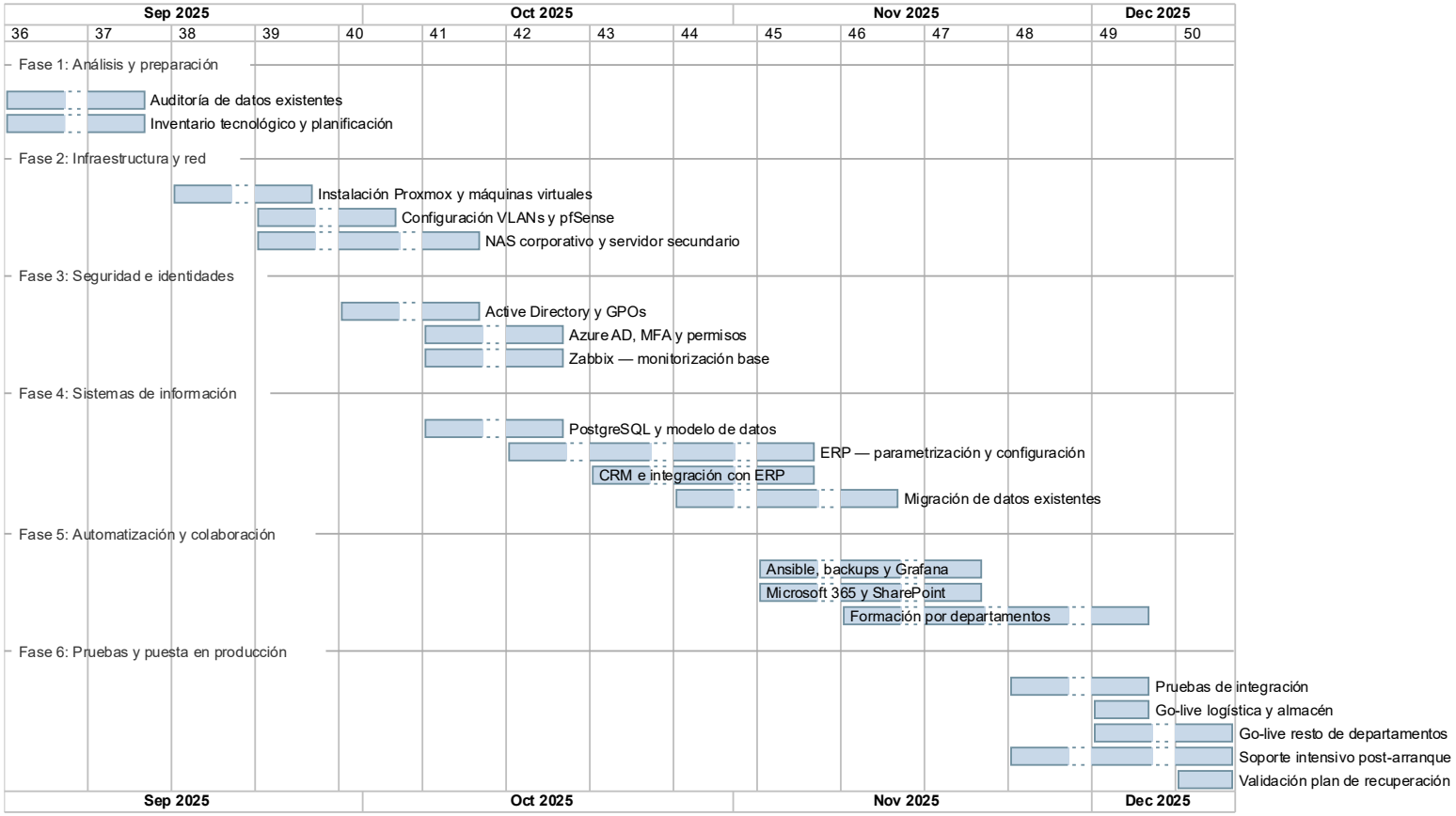
22.6 Apéndice F — Figura 6: Diagrama de actividad — Flujo de automatización operativa

La figura representa el flujo automatizado del ciclo nocturno de mantenimiento: snapshots de VMs en Proxmox (23:00 h), backup de PostgreSQL con script Bash (00:30 h), transferencia cifrada a NAS y cloud mediante rclone, verificación por Zabbix, actualización semanal con Ansible y respuesta automática ante servicios caídos, con bifurcaciones de alerta por Teams y email ante fallos en cualquier etapa.



22.7 Apéndice G — Figura 7: Diagrama de Gantt — Cronograma de implantación

La figura muestra la planificación temporal del proyecto de digitalización de PacketRoute S.L. en seis fases distribuidas a lo largo de dieciséis semanas: F1 Análisis y preparación (S1-S2), F2 Infraestructura y red (S3-S6), F3 Seguridad e identidades (S5-S7), F4 Sistemas de información y base de datos (S6-S11), F5 Automatización, colaboración y herramientas (S10-S14) y F6 Pruebas y puesta en producción (S13-S16), con los solapes entre fases representados gráficamente.



22.8 Apéndice H — Listado de código 1: Restricciones de integridad nativas del modelo de datos

El presente apéndice recoge las restricciones de integridad definidas directamente sobre el esquema de base de datos de PacketRoute S.L. en PostgreSQL. Se incluyen restricciones de tipo CHECK para validar rangos y valores permitidos, cláusulas ENUM para campos con valores cerrados como el estado del pedido o el tipo de movimiento, restricciones UNIQUE sobre identificadores comerciales como el SKU, y valores por defecto DEFAULT aplicados a campos de auditoría y control. Su definición en capa de motor garantiza que ninguna aplicación externa pueda vulnerar la coherencia del dato.

```
-- Creación del esquema de PacketRoute en PostgreSQL
-- Versión: 1.0 | Gestor: PostgreSQL 16 | Codificación: UTF-8

-- ============================================================
-- TABLA: categoria
-- ============================================================
CREATE TABLE categoria (
    id_categoria  SERIAL PRIMARY KEY,
    nombre        VARCHAR(100) NOT NULL UNIQUE,
    descripcion   TEXT
);

-- ============================================================
-- TABLA: proveedor
-- ============================================================
CREATE TABLE proveedor (
    id_proveedor  SERIAL PRIMARY KEY,
    nombre        VARCHAR(150) NOT NULL,
    cif           VARCHAR(20)  NOT NULL UNIQUE,
    telefono      VARCHAR(20),
    email         VARCHAR(150),
    activo        BOOLEAN      NOT NULL DEFAULT TRUE
);

-- ============================================================
-- TABLA: producto
-- ============================================================
CREATE TABLE producto (
    id_producto   SERIAL PRIMARY KEY,
    id_categoria  INT          NOT NULL REFERENCES categoria(id_categoria) ON
DELETE RESTRICT,
    id_proveedor  INT          NOT NULL REFERENCES proveedor(id_proveedor) ON
DELETE RESTRICT,
    sku           VARCHAR(50)  NOT NULL UNIQUE,
    nombre        VARCHAR(200) NOT NULL,
    descripcion   TEXT,
    precio_venta  NUMERIC(10,2) NOT NULL CHECK (precio_venta >= 0),
```

```
    activo        BOOLEAN      NOT NULL DEFAULT TRUE
);

-- ============================================================
-- TABLA: stock
-- ============================================================
CREATE TABLE stock (
    id_stock        SERIAL PRIMARY KEY,
    id_producto     INT  NOT NULL REFERENCES producto(id_producto) ON DELETE
RESTRICT UNIQUE,
    cantidad_real   INT  NOT NULL DEFAULT 0 CHECK (cantidad_real >= 0),
    cantidad_reservada INT NOT NULL DEFAULT 0 CHECK (cantidad_reservada >= 0),
    stock_minimo    INT  NOT NULL DEFAULT 5,
    ultima_actualizacion TIMESTAMPTZ NOT NULL DEFAULT NOW()
);

-- ============================================================
-- TABLA: movimientostock
-- ============================================================
CREATE TABLE movimientostock (
    id_movimiento  SERIAL PRIMARY KEY,
    id_producto    INT          NOT NULL REFERENCES producto(id_producto) ON
DELETE RESTRICT,
    tipo_movimiento VARCHAR(20) NOT NULL CHECK (tipo_movimiento IN
('entrada','salida','ajuste','devolucion')),
    cantidad       INT          NOT NULL CHECK (cantidad != 0),
    motivo         TEXT,
    usuario        VARCHAR(100) NOT NULL,
    fecha          TIMESTAMPTZ  NOT NULL DEFAULT NOW()
);

-- ============================================================
-- TABLA: cliente
-- ============================================================
CREATE TABLE cliente (
    id_cliente      SERIAL PRIMARY KEY,
    nombre          VARCHAR(150) NOT NULL,
    nif             VARCHAR(20)  NOT NULL UNIQUE,
    email           VARCHAR(150),
    telefono        VARCHAR(20),
    direccion       TEXT,
    consentimiento_rgpd BOOLEAN NOT NULL DEFAULT FALSE,
    fecha_consentimiento DATE,
    anonimizado     BOOLEAN NOT NULL DEFAULT FALSE,
    fecha_alta      DATE NOT NULL DEFAULT CURRENT_DATE
);

-- ============================================================
-- TABLA: repartidor  (subconjunto del personal)
-- ============================================================
CREATE TABLE repartidor (
    id_repartidor  SERIAL PRIMARY KEY,
    nombre         VARCHAR(150) NOT NULL,
    telefono       VARCHAR(20),
    matricula      VARCHAR(15),
```

```
    activo         BOOLEAN NOT NULL DEFAULT TRUE
);

-- ============================================================
-- TABLA: pedido
-- ============================================================
CREATE TYPE estado_pedido AS ENUM (
    'pendiente','confirmado','en_preparacion',
    'en_reparto','entregado','incidencia','cancelado'
);

CREATE TABLE pedido (
    id_pedido       SERIAL PRIMARY KEY,
    id_cliente      INT            NOT NULL REFERENCES cliente(id_cliente) ON
DELETE RESTRICT,
    id_repartidor   INT            REFERENCES repartidor(id_repartidor) ON DELETE
SET NULL,
    estado          estado_pedido  NOT NULL DEFAULT 'pendiente',
    fecha_pedido    TIMESTAMPTZ    NOT NULL DEFAULT NOW(),
    fecha_entrega_prevista DATE,
    observaciones   TEXT
);

-- ============================================================
-- TABLA: lineapedido
-- ============================================================
CREATE TABLE lineapedido (
    id_linea       SERIAL PRIMARY KEY,
    id_pedido      INT            NOT NULL REFERENCES pedido(id_pedido) ON DELETE
CASCADE,
    id_producto    INT            NOT NULL REFERENCES producto(id_producto) ON
DELETE RESTRICT,
    cantidad       INT            NOT NULL CHECK (cantidad > 0),
    precio_unitario NUMERIC(10,2) NOT NULL CHECK (precio_unitario >= 0)
);

-- ============================================================
-- TABLA: entregaRepartidor
-- ============================================================
CREATE TABLE entregarepartidor (
    id_entrega     SERIAL PRIMARY KEY,
    id_pedido      INT            NOT NULL REFERENCES pedido(id_pedido) ON DELETE
RESTRICT,
    fecha_intento  TIMESTAMPTZ    NOT NULL DEFAULT NOW(),
    estado_entrega VARCHAR(30)    NOT NULL CHECK (estado_entrega IN
('exitosa','fallida','parcial')),
    latitud        NUMERIC(10,7),
    longitud       NUMERIC(10,7),
    observaciones  TEXT
);

-- ============================================================
-- TABLA: factura
-- ============================================================
CREATE TABLE factura (
```

```
    id_factura     SERIAL PRIMARY KEY,
    id_pedido      INT            NOT NULL REFERENCES pedido(id_pedido) ON DELETE
RESTRICT UNIQUE,
    numero_factura VARCHAR(30)    NOT NULL UNIQUE,
    fecha_emision  DATE           NOT NULL DEFAULT CURRENT_DATE,
    importe_total  NUMERIC(10,2)  NOT NULL CHECK (importe_total >= 0),
    tipo_iva       NUMERIC(5,2)   NOT NULL DEFAULT 21.00,
    estado_pago    VARCHAR(20)    NOT NULL DEFAULT 'pendiente'
        CHECK (estado_pago IN ('pendiente','pagada','anulada'))
);

-- ============================================================
-- TABLA: devolucion
-- ============================================================
CREATE TYPE estado_devolucion AS ENUM
('solicitada','aprobada','rechazada','resuelta');

CREATE TABLE devolucion (
    id_devolucion  SERIAL PRIMARY KEY,
    id_pedido      INT                NOT NULL REFERENCES pedido(id_pedido) ON
DELETE RESTRICT,
    fecha_solicitud TIMESTAMPTZ       NOT NULL DEFAULT NOW(),
    motivo         TEXT               NOT NULL,
    estado         estado_devolucion  NOT NULL DEFAULT 'solicitada',
    resolucion     TEXT,
    fecha_resolucion DATE
);

-- ============================================================
-- TABLA: logauditoria
-- ============================================================
CREATE TABLE logauditoria (
    id_log         BIGSERIAL PRIMARY KEY,
    tabla_afectada VARCHAR(50)  NOT NULL,
    id_registro    INT          NOT NULL,
    accion         VARCHAR(10)  NOT NULL CHECK (accion IN
('INSERT','UPDATE','DELETE')),
    usuario        VARCHAR(100) NOT NULL,
    fecha          TIMESTAMPTZ  NOT NULL DEFAULT NOW(),
    datos_anteriores JSONB,
    datos_nuevos     JSONB
);
```

22.9 Apéndice I — Listado de código 2: Automatización mediante triggers y procedimientos almacenados

Este apéndice contiene los tres triggers PL/pgSQL implementados sobre el modelo de datos, junto con el procedimiento almacenado sp_cerrar_pedido. El primer trigger gestiona la reducción automática de stock al confirmar una línea de pedido. El segundo registra en la tabla AuditoriaRegistro cualquier cambio de estado sobre las entidades críticas, almacenando el valor anterior y el nuevo en formato JSONB. El tercer trigger libera las unidades reservadas cuando un pedido es cancelado. El procedimiento sp_cerrar_pedido coordina el cierre completo del ciclo transaccional de forma atómica, con bloque ROLLBACK ante cualquier fallo interno.

```
-- ============================================================
-- FUNCIÓN: actualizar stock al insertar línea de pedido
-- ============================================================
CREATE OR REPLACE FUNCTION fn_reservar_stock()
RETURNS TRIGGER AS $$
DECLARE
    v_disponible INT;
BEGIN
    SELECT (cantidad_real - cantidad_reservada)
    INTO v_disponible
    FROM stock
    WHERE id_producto = NEW.id_producto;

    IF v_disponible IS NULL THEN
        RAISE EXCEPTION 'Producto % sin registro de stock.', NEW.id_producto;
    END IF;

    IF v_disponible < NEW.cantidad THEN
        RAISE EXCEPTION 'Stock insuficiente para el producto %. Disponible: %,
solicitado: %.',
            NEW.id_producto, v_disponible, NEW.cantidad;
    END IF;

    UPDATE stock
    SET cantidad_reservada = cantidad_reservada + NEW.cantidad,
        ultima_actualizacion = NOW()
    WHERE id_producto = NEW.id_producto;

    RETURN NEW;
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER trg_reservar_stock_en_pedido
AFTER INSERT ON lineapedido
FOR EACH ROW EXECUTE FUNCTION fn_reservar_stock();

-- ============================================================
-- FUNCIÓN: descontar stock real al marcar pedido como entregado
```

```
-- ============================================================
CREATE OR REPLACE FUNCTION fn_cerrar_stock_en_entrega()
RETURNS TRIGGER AS $$
BEGIN
    IF NEW.estado = 'entregado' AND OLD.estado IS DISTINCT FROM 'entregado' THEN

        UPDATE stock s
        SET cantidad_real      = s.cantidad_real - lp.cantidad,
            cantidad_reservada = s.cantidad_reservada - lp.cantidad,
            ultima_actualizacion = NOW()
        FROM lineapedido lp
        WHERE lp.id_pedido = NEW.id_pedido
          AND s.id_producto = lp.id_producto;

        INSERT INTO movimientostock (id_producto, tipo_movimiento, cantidad,
motivo, usuario)
        SELECT lp.id_producto, 'salida', lp.cantidad,
               'Entrega pedido #' || NEW.id_pedido, 'sistema'
        FROM lineapedido lp
        WHERE lp.id_pedido = NEW.id_pedido;

    END IF;
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER trg_descontar_stock_en_entrega
AFTER UPDATE OF estado ON pedido
FOR EACH ROW EXECUTE FUNCTION fn_cerrar_stock_en_entrega();

-- ============================================================
-- FUNCIÓN: liberar reserva al cancelar o registrar incidencia
-- ============================================================
CREATE OR REPLACE FUNCTION fn_liberar_stock_en_cancelacion()
RETURNS TRIGGER AS $$
BEGIN
    IF NEW.estado IN ('cancelado', 'incidencia')
       AND OLD.estado NOT IN ('cancelado', 'incidencia', 'entregado') THEN

        UPDATE stock s
        SET cantidad_reservada = s.cantidad_reservada - lp.cantidad,
            ultima_actualizacion = NOW()
        FROM lineapedido lp
        WHERE lp.id_pedido = NEW.id_pedido
          AND s.id_producto = lp.id_producto;

        INSERT INTO movimientostock (id_producto, tipo_movimiento, cantidad,
motivo, usuario)
        SELECT lp.id_producto, 'ajuste', lp.cantidad,
               'Liberación reserva pedido #' || NEW.id_pedido || ' (' ||
NEW.estado || ')',
               'sistema'
        FROM lineapedido lp
        WHERE lp.id_pedido = NEW.id_pedido;
```

```
    END IF;
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER trg_restaurar_stock_en_cancelacion
AFTER UPDATE OF estado ON pedido
FOR EACH ROW EXECUTE FUNCTION fn_liberar_stock_en_cancelacion();

-- ============================================================
-- FUNCIÓN: auditoría automática de cambios en pedido
-- ============================================================
CREATE OR REPLACE FUNCTION fn_auditoria_pedido()
RETURNS TRIGGER AS $$
BEGIN
    INSERT INTO logauditoria (
        tabla_afectada, id_registro, accion,
        usuario, datos_anteriores, datos_nuevos
    ) VALUES (
        'pedido',
        COALESCE(NEW.id_pedido, OLD.id_pedido),
        TG_OP,
        current_user,
        CASE WHEN TG_OP = 'INSERT' THEN NULL ELSE to_jsonb(OLD) END,
        CASE WHEN TG_OP = 'DELETE' THEN NULL ELSE to_jsonb(NEW) END
    );
    RETURN COALESCE(NEW, OLD);
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER trg_auditoria_pedido
AFTER INSERT OR UPDATE OR DELETE ON pedido
FOR EACH ROW EXECUTE FUNCTION fn_auditoria_pedido();
```

22.10 Apéndice J — Listado de código 3: Procedimiento almacenado — Gestión de devoluciones

El apéndice recoge el procedimiento almacenado encargado de gestionar el ciclo completo de una devolución en PacketRoute S.L. El procedimiento valida que el pedido referenciado existe y se encuentra en un estado susceptible de devolución, revierte las unidades devueltas al stock disponible, actualiza el estado del pedido y genera el registro de auditoría correspondiente. Toda la operación se ejecuta dentro de un bloque transaccional, de forma que un fallo en cualquiera de sus pasos revierte el conjunto sin dejar el sistema en un estado inconsistente.

```
-- ============================================================
-- PROCEDIMIENTO: procesar devolución (aprobar o rechazar)
-- ============================================================
CREATE OR REPLACE PROCEDURE sp_procesar_devolucion(
    p_id_devolucion  INT,
    p_aprobada       BOOLEAN,
    p_resolucion     TEXT DEFAULT NULL
)
LANGUAGE plpgsql AS $$
DECLARE
    v_id_pedido  INT;
    v_nuevo_estado estado_devolucion;
BEGIN
    SELECT id_pedido INTO v_id_pedido
    FROM devolucion
    WHERE id_devolucion = p_id_devolucion
      AND estado = 'solicitada';

    IF NOT FOUND THEN
        RAISE EXCEPTION 'Devolución % no encontrada o ya procesada.',
p_id_devolucion;
    END IF;

    IF p_aprobada THEN
        v_nuevo_estado := 'aprobada';

        UPDATE stock s
        SET cantidad_real = s.cantidad_real + lp.cantidad,
            ultima_actualizacion = NOW()
        FROM lineapedido lp
        WHERE lp.id_pedido = v_id_pedido
          AND s.id_producto = lp.id_producto;

        INSERT INTO movimientostock (id_producto, tipo_movimiento, cantidad,
motivo, usuario)
        SELECT lp.id_producto, 'devolucion', lp.cantidad,
               'Devolución aprobada #' || p_id_devolucion, current_user
        FROM lineapedido lp
```

```
        WHERE lp.id_pedido = v_id_pedido;
    ELSE
        v_nuevo_estado := 'rechazada';
    END IF;

    UPDATE devolucion
    SET estado           = v_nuevo_estado,
        resolucion       = p_resolucion,
        fecha_resolucion = CURRENT_DATE
    WHERE id_devolucion = p_id_devolucion;

    COMMIT;
END;
$$;
```

22.11 Apéndice K — Listado de código 4: Índices y vistas SQL

Este apéndice incluye los índices definidos sobre las columnas de mayor frecuencia de consulta en el modelo relacional: estado en la tabla Pedido, id_cliente en LineaPedido, id_producto en MovimientoStock y fecha_pedido par a consultas temporales. Se incluyen también las dos vistas materializadas del sistema: v_pedidos_activos, que expone los pedidos en curso con sus líneas y cliente asociado, y v_stock_critico, que filtra los productos cuya disponibilidad real cae por debajo del umbral mínimo definido. Ambas vistas actúan además como capa de control de acceso, limitando los campos visibles sin necesidad de conceder permisos directos sobre las tablas base.

```
-- Índices
CREATE INDEX idx_pedido_cliente        ON pedido(id_cliente);
CREATE INDEX idx_pedido_estado         ON pedido(estado);
CREATE INDEX idx_lineapedido_producto  ON lineapedido(id_producto);
CREATE INDEX idx_movimiento_prod_fecha ON movimientostock(id_producto, fecha);
CREATE INDEX idx_logauditoria_tf       ON logauditoria(tabla_afectada, fecha);

-- Vista: pedido completo con cliente y número de líneas
CREATE VIEW v_pedidos_resumen AS
SELECT
    p.id_pedido,
    c.nombre                              AS cliente,
    c.email,
    p.estado,
    p.fecha_pedido,
    p.fecha_entrega_prevista,
    COUNT(lp.id_linea)                    AS num_lineas,
    SUM(lp.cantidad * lp.precio_unitario) AS importe_total
FROM pedido p
JOIN cliente c    ON c.id_cliente  = p.id_cliente
LEFT JOIN lineapedido lp ON lp.id_pedido = p.id_pedido
GROUP BY p.id_pedido, c.nombre, c.email,
         p.estado, p.fecha_pedido, p.fecha_entrega_prevista;

-- Vista: stock disponible por producto con alerta de mínimo
CREATE VIEW v_stock_disponible AS
SELECT
    pr.sku,
    pr.nombre                                          AS producto,
    ca.nombre                                          AS categoria,
    s.cantidad_real,
    s.cantidad_reservada,
    (s.cantidad_real - s.cantidad_reservada)           AS disponible,
    s.stock_minimo,
    CASE WHEN (s.cantidad_real - s.cantidad_reservada) <= s.stock_minimo
         THEN TRUE ELSE FALSE END                      AS alerta_reposicion
FROM stock s
JOIN producto  pr ON pr.id_producto  = s.id_producto
```

```
JOIN categoria ca ON ca.id_categoria = pr.id_categoria;

-- Vista: devoluciones pendientes de resolución
CREATE VIEW v_devoluciones_pendientes AS
SELECT
    d.id_devolucion,
    p.id_pedido,
    c.nombre   AS cliente,
    d.motivo,
    d.fecha_solicitud,
    d.estado
FROM devolucion d
JOIN pedido  p ON p.id_pedido  = d.id_pedido
JOIN cliente c ON c.id_cliente = p.id_cliente
WHERE d.estado IN ('solicitada', 'aprobada');
```

22.12 Apéndice L — Listado de código 5: Script Bash — Volcado automatizado de PostgreSQL (backup_postgres.sh)

El apéndice contiene el script de shell encargado de la copia de seguridad nocturna de la base de datos de PacketRoute S.L. El script realiza un volcado comprimido mediante pg_dump, transfiere el resultado cifrado hacia el almacenamiento NAS local y hacia el servicio cloud configurado en rclone, y aplica una política de retención automática que elimina las copias con más de siete días de antigüedad. Está diseñado para ejecutarse como tarea programada mediante cron en el servidor de base de datos.

```
#!/usr/bin/env bash
# backup_postgres.sh — PacketRoute S.L.
# Volcado diario de PostgreSQL hacia NAS y cloud (rclone)

set -euo pipefail

DB_NAME="packetroute_db"
DB_USER="backup_user"
FECHA=$(date +%Y%m%d_%H%M)
BACKUP_DIR="/mnt/nas/backups/postgresql"
ARCHIVO="${BACKUP_DIR}/pg_${DB_NAME}_${FECHA}.sql.gz"
RETENTION_DAYS=7
LOG="/var/log/backup_postgres.log"

echo "[$(date)] Iniciando backup de ${DB_NAME}" >> "${LOG}"

# Volcado y compresión
PGPASSFILE="/etc/pgpass_backup" pg_dump -U "${DB_USER}" "${DB_NAME}"     | gzip >
"${ARCHIVO}"

if [ $? -eq 0 ]; then
    echo "[$(date)] Backup completado: ${ARCHIVO}" >> "${LOG}"
else
    echo "[$(date)] ERROR: Fallo en pg_dump" >> "${LOG}"
    exit 1
fi

# Transferencia cifrada a cloud mediante rclone
rclone copy "${ARCHIVO}" backblaze:packetroute-backups/postgresql/     --config
/etc/rclone.conf     >> "${LOG}" 2>&1

# Eliminación de copias antiguas (retención 7 días)
find "${BACKUP_DIR}" -name "pg_${DB_NAME}_*.sql.gz"     -mtime +${RETENTION_DAYS}
-delete

echo "[$(date)] Backup y retención completados." >> "${LOG}"
```

22.13 Apéndice M — Listado de código 6: Playbook YAML — Actualización de servidores (playbook_update_servers.yml)

Este apéndice recoge el playbook de Ansible utilizado para la actualización coordinada del sistema operativo en todos los nodos del inventario de PacketRoute S.L. El playbook aplica las actualizaciones disponibles de forma secuencial y controlada sobre cada servidor, garantizando que todos los nodos mantienen el mismo nivel de parcheo sin intervención manual. Está preparado para ejecutarse tanto en servidores Debian/Ubuntu como en distribuciones derivadas, e incluye una tarea de reinicio condicional que solo se activa cuando el sistema lo requiere.

```
---
# playbook_update_servers.yml — PacketRoute S.L.
# Actualización del sistema operativo en todos los servidores

- name: Actualización de servidores PacketRoute
  hosts: packetroute_servers
  become: true
  serial: 1
  tasks:

    - name: Actualizar caché de paquetes
      apt:
        update_cache: yes
        cache_valid_time: 3600

    - name: Instalar actualizaciones disponibles
      apt:
        upgrade: dist
        autoremove: yes
        autoclean: yes

    - name: Verificar si se requiere reinicio
      stat:
        path: /var/run/reboot-required
      register: reboot_required

    - name: Reiniciar si es necesario (con delay de seguridad)
      reboot:
        msg: "Reinicio por actualización del sistema"
        pre_reboot_delay: 10
        reboot_timeout: 120
      when: reboot_required.stat.exists

    - name: Registrar resultado
      lineinfile:
        path: /var/log/ansible_updates.log
        line: "{{ inventory_hostname }} actualizado el {{
```

```
ansible_date_time.iso8601 }}"
        create: yes
```