Instituto Europeo de Posgrado

FORTALECIMIENTO DE LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA PYME: CASO PICK-UP LLINARS S.L

Trabajo fin de estudio presentado por:	**David Almirón Sánchez.** **Alexis Andrade Muñoz.** **Cristhel Melissa Villao Mackliff.**
Tipo de trabajo:	**Proyecto Fin de Programa**
Director/a:	**Fabricio Echeverria Claustro**
Fecha:	**26 de marzo de 2026**

Índice

1 Resumen

En los últimos años, las pequeñas y medianas empresas del sector hostelero han experimentado un proceso de digitalización creciente.
Este fenómeno ha supuesto una transformación significativa en la manera de gestionar los negocios, ya que la adopción de nuevas tecnologías ha permitido optimizar los procesos internos y mejorar la atención al cliente.
Sin embargo, esta evolución tecnológica ha traído consigo un aumento en la exposición a riesgos informáticos, haciendo necesario prestar especial atención a la seguridad de la información dentro de las organizaciones.
Pick-up Llinars S.L., una empresa dedicada a la hostelería, ha seguido la tendencia del sector y ha integrado herramientas digitales en su operativa diaria.
A pesar de los beneficios obtenidos, la empresa no ha establecido políticas formales de seguridad de la información. Esta carencia ha generado vulnerabilidades que se han materializado en problemas concretos, como incidentes de malware y robo de datos, afectando directamente a la gestión y protección de la información empresarial.
El proyecto se basa en la metodología de investigación-acción para diagnosticar, analizar y planificar soluciones que permitan mejorar la gestión de la seguridad informática, mediante una intervención estructurada y adaptada a las necesidades de la organización.

Palabras clave:
Seguridad de la información.
ISO/IEC 27001.
RGPD.
Gestión de riesgos.
Auditoría de seguridad.
Activos de información.

2 Abstract

In recent years, small and medium-sized enterprises (SMEs) in the hospitality sector have experienced increasing digitalization.
This phenomenon has brought about a significant transformation in how businesses are managed, as the adoption of new technologies has allowed for the optimization of internal processes and improved customer service.

However, this technological evolution has also led to increased exposure to cybersecurity risks, making it necessary to pay special attention to information security within organizations.
Pick-up Llinars S.L., a company dedicated to the hospitality industry, has followed this trend and integrated digital tools into its daily operations. Despite the benefits obtained, the company has not established formal information security policies. This deficiency has generated vulnerabilities that have materialized concrete problems, such as malware incidents and data theft, directly affecting the management and protection of company information.
The project is based on action research methodology to diagnose, analyze, and plan solutions that allow for improved IT security management through a structured intervention adapted to the needs of the organization.

Keywords:
Information Security
ISO/IEC 27001
GDPR
Risk Management
Security Audit
Information Assets

3 Introducción

Este proyecto de aplicación en investigación-acción se centró en la identificación y resolución debido a que hoy en día, la digitalización progresiva de las pequeñas y medianas empresas (PYMES) está transformando profundamente sectores tradicionales como la hostelería. Este proceso conlleva la adopción de tecnologías avanzadas para gestionar cobros, controlar inventarios, manejar documentación, comunicarse con proveedores y administrar recursos humanos. Gracias a esta digitalización, los negocios optimizan procedimientos, minimizan errores, agilizan la toma de decisiones y ofrecen a sus clientes una atención más personalizada y eficiente. No obstante, depender cada vez más de sistemas digitales implica una mayor exposición a amenazas informáticas, como robo de datos, ciberataques, pérdida de información o accesos no permitidos. Así, la seguridad de la información se convierte en un aspecto clave para mantener la continuidad empresarial y la confianza de clientes y colaboradores.

Pick-up Llinars S.L., empresa hostelera fundada en 2017 y ubicada en el centro de Llinars del Vallès (Barcelona), ha experimentado una gran evolución en su modelo de negocio. En los últimos años ha integrado herramientas digitales, desde la gestión de reservas y pedidos hasta el control financiero y la interacción con proveedores. Esta modernización ha mejorado la eficiencia operativa, ampliado los servicios ofrecidos y permitido adaptarse mejor al mercado actual. Sin embargo, dicho avance tecnológico no ha ido acompañado de una política formalizada sobre seguridad de la información, generando así riesgos potenciales para la protección de los datos y la integridad de los sistemas.

Este proyecto consiste en aplicar una metodología de investigación-acción en Pick-up Llinars, un negocio hostelero que ha implementado sistemas digitales básicos sin una política eficaz de seguridad informática. Como consecuencia de no disponer de una protección confiable de datos, la empresa ha sufrido incidentes vinculados a malware y robo de información, permitiendo integrar teoría y práctica en un entorno real. Mediante un enfoque de investigación-acción, se desarrollaron habilidades de diagnóstico, análisis y planificación orientadas a mejorar la eficiencia y efectividad de un proceso crítico en la organización. La estructura del proyecto incluyó una revisión exhaustiva del contexto organizacional y la implementación de una solución factible que responde a las necesidades de la organización y optimiza su desempeño.

3.1 Objetivo General

El objetivo principal del proyecto fue desarrollar una solución operativa al problema de la seguridad de la información para Pick-up Llinars S.L., basado en los principios y requisitos de la norma internacional ISO/IEC 27001:2022 y en las obligaciones legales establecidas por el RGPD. Este modelo debe contemplar la formalización de políticas, procedimientos y controles específicos que permitan fortalecer el proceso de gestión y protección de los activos de información y sistemas tecnológicos de la organización. Asimismo, el modelo

debe facilitar la identificación y evaluación de riesgos, la definición de responsabilidades claras, la formación y sensibilización del personal, y el establecimiento de mecanismos de monitorización y respuesta ante incidentes de seguridad. El objetivo final es garantizar la confidencialidad, integridad y disponibilidad de la información, promover la mejora continua y asegurar el cumplimiento normativo, contribuyendo así a la sostenibilidad, competitividad y reputación de Pick-up Llinars S.L. en el sector de la hostelería.

La intervención se orientó no solo a corregir el problema identificado, sino también a proporcionar una propuesta sostenible que pudiera integrarse a la estructura de la organización, elevando los niveles de eficiencia y alcanzando los estándares de desempeño requeridos en el proceso intervenido.

3.2 Objetivos Específicos

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

1. Evaluar el estado actual de seguridad de la información, analizando en detalle la situación actual de la seguridad de la información dentro de la organización. Esta evaluación permite identificar las fortalezas y debilidades del sistema existente, así como establecer una línea base para la mejora continua.
2. Identificar y clasificar los activos de información, Una vez evaluada la situación, se debe identificar todos los activos de información. Posteriormente, es necesario clasificarlos según su importancia, sensibilidad y el impacto que tendría su pérdida o compromiso, lo que facilitará la gestión de los riesgos asociados.
3. Analizar los riesgos asociados a los sistemas de información, riesgos que afectan a los activos y sistemas de información. Esta etapa se centrará en detectar amenazas y vulnerabilidades, así como en valorar las consecuencias que podrían derivarse de un incidente de seguridad.
4. Definir e implementar controles de seguridad, con base en el análisis de riesgos, es necesario establecer y poner en marcha controles de seguridad adecuados. Estos controles buscan mitigar los riesgos identificados y proteger los activos de información de manera efectiva.
5. Establecer las bases para la implantación de un SGSI, para la futura implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este objetivo asegura que la organización cuente con los procedimientos y estructuras necesarias para gestionar la seguridad de la información de forma sistemática y eficiente.

3.3 Metodología

El proyecto se desarrolló mediante la metodología de investigación-acción, la cual facilitó la colaboración continua entre el equipo de estudiantes y docente asesor. Esta metodología permitió un enfoque sistemático para identificar problemas, formular hipótesis y aplicar soluciones en un contexto real, ajustando las estrategias conforme se

avanzaba en el proyecto. La investigación-acción proporcionó un marco flexible y participativo para ejecutar el proyecto de manera estructurada, generando una intervención bien fundamentada y con alto potencial de impacto.

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

3.3.1 Identificación y Análisis del Problema

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

El análisis inicial pone de manifiesto que el proceso de gestión de activos de información en Pick-up Llinars S.L. ha evolucionado de forma operativa y funcional, permitiendo el desarrollo de las actividades diarias. Sin embargo, se evidencia la carencia de un marco formal estructurado que garantice la protección integral de dichos activos y facilite la adaptación a los estándares y normativas vigentes.

Este diagnóstico revela la necesidad de transitar desde una gestión reactiva y basada en la experiencia hacia un modelo proactivo, documentado y alineado con las buenas prácticas internacionales en seguridad de la información. La formalización de procedimientos y la definición clara de roles y responsabilidades resultan imprescindibles para mitigar riesgos y asegurar la continuidad del negocio.

Estas circunstancias no suponen necesariamente la existencia de incumplimientos graves, pero sí reflejan una ausencia de un sistema de gestión formalizado y alineado con estándares reconocidos como la norma ISO/IEC 27001:2022 o el propio RGPD. Esta situación puede derivar en una menor eficacia en la prevención y gestión de incidentes de seguridad, así como en dificultades a la hora de demostrar cumplimiento ante auditorías o requerimientos legales.

Por tanto, resulta prioritario establecer una estrategia de mejora que contemple la formalización de procesos, la capacitación del personal, la definición de métricas de seguimiento y la integración de la seguridad de la información como un valor transversal en la cultura organizativa de Pick-up Llinars S.L. Solo así se podrá garantizar la protección adecuada de los activos de información y la adaptación continua a los retos actuales y futuros en materia de seguridad y cumplimiento normativo.

3.3.2 Planificación de la Solución

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

3.3.2.1 Definición de Alcance y Recursos

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

4 Identificación y descripción un problema al interior de la organización

Pick-up Llinars S.L. es una empresa del sector de la hostelería ubicada en el municipio de Llinars del Vallès (Barcelona), constituida en el año 2017 y gestionada por tres socios con participación equitativa. El establecimiento se caracteriza por una fuerte actividad estacional, con una plantilla que puede variar entre cuatro trabajadores en temporada baja y hasta doce empleados durante los periodos de mayor actividad. Su modelo de negocio se basa en la restauración y servicio en terraza en una zona céntrica del municipio, lo que convierte al establecimiento en un punto de encuentro habitual para residentes y visitantes.

En los últimos años, la empresa ha incorporado diversas herramientas tecnológicas para apoyar la gestión de su actividad diaria. Entre ellas se encuentran el sistema de punto de venta (TPV) para la gestión de cobros y facturación, plataformas de almacenamiento en la nube para la gestión documental, equipos informáticos para la administración del negocio, sistemas de red inalámbrica que conectan diferentes espacios operativos del establecimiento y sistemas de videovigilancia para la protección de las instalaciones. Asimismo, la empresa gestiona información administrativa y laboral de empleados y mantiene relaciones digitales con proveedores y servicios externos, lo que implica el tratamiento regular de información sensible y datos personales.

A pesar de esta progresiva digitalización, el proceso de gestión y protección de los activos de información no ha evolucionado al mismo ritmo que la incorporación de tecnologías. Durante el análisis preliminar realizado para el presente proyecto se ha observado que la

organización no dispone de un proceso formalizado que regule de manera estructurada la gestión de la seguridad de la información. En la práctica, las decisiones relacionadas con la configuración de sistemas, la asignación de accesos o la realización de copias de seguridad se basan en criterios operativos y en la experiencia de los socios, sin que exista una política documentada, procedimientos definidos o una asignación formal de responsabilidades en materia de seguridad de la información.

Esta situación se manifiesta en diferentes aspectos de la operativa tecnológica de la empresa. Por ejemplo, los sistemas informáticos utilizados para la gestión del negocio se encuentran centralizados en varios equipos con sistema operativo Windows que cumplen funciones administrativas y operativas, incluyendo el equipo que alberga la base de datos del sistema TPV. Esta base de datos contiene información relevante para la gestión de productos, ventas y operaciones diarias, pero su almacenamiento se realiza de manera local sin un sistema automatizado de copias de seguridad externas que garantice su recuperación ante incidentes. Del mismo modo, el acceso a algunos sistemas se realiza mediante cuentas compartidas, lo que dificulta la trazabilidad de las acciones realizadas por los usuarios y limita la capacidad de auditar el uso de los sistemas.

En el ámbito de la infraestructura de red también se observan elementos que evidencian la ausencia de un enfoque sistemático de seguridad. La conectividad entre el local principal y el almacén se realiza mediante un enlace inalámbrico basado en dispositivos de red que permiten extender la conectividad entre ambos espacios operativos. Si bien esta solución resulta funcional desde el punto de vista operativo, no existe un procedimiento formal de gestión, supervisión o control de esta infraestructura. Asimismo, el router principal utilizado para el acceso a internet corresponde al equipo proporcionado por el proveedor de telecomunicaciones, sin que se hayan aplicado medidas específicas de endurecimiento de la configuración de seguridad, como la modificación de credenciales administrativas o la definición de políticas de acceso.

Otra dimensión relevante del problema se relaciona con la gestión de la información personal y administrativa. La empresa almacena documentación laboral y administrativa en servicios de almacenamiento en la nube, incluyendo documentos con datos personales de empleados, tales como contratos laborales, nóminas o documentos de identidad. Aunque el acceso a estos servicios está restringido principalmente a los socios, no existe una clasificación formal de la información ni un procedimiento documentado que establezca criterios de acceso, conservación o eliminación de datos, lo cual dificulta demostrar el cumplimiento sistemático de las obligaciones establecidas en el Reglamento General de Protección de Datos (RGPD).

Las causas que explican esta situación pueden identificarse en varios factores organizativos. En primer lugar, la empresa ha experimentado un crecimiento progresivo en el uso de herramientas tecnológicas sin que se haya producido una adaptación equivalente en sus procesos de gestión interna. En segundo lugar, la naturaleza estacional del negocio implica una rotación significativa de personal durante determinados periodos del año, lo que dificulta la consolidación de prácticas estandarizadas y de formación continua en materia de seguridad de la información. Finalmente, la ausencia de un responsable formal de seguridad y de una política organizativa específica en esta materia

ha provocado que la gestión de la seguridad tecnológica se realice de manera reactiva y basada en la experiencia práctica de los responsables del negocio.

Las consecuencias potenciales de esta situación pueden afectar a diferentes dimensiones del funcionamiento organizacional. Desde el punto de vista operativo, la falta de procedimientos estructurados puede incrementar la dependencia de determinadas personas para resolver incidencias tecnológicas o restaurar sistemas en caso de fallo. Desde la perspectiva de la continuidad del negocio, la inexistencia de copias de seguridad verificadas o de planes de recuperación puede generar riesgos significativos en caso de pérdida de datos o interrupción del sistema TPV. Asimismo, desde el punto de vista normativo, la ausencia de medidas organizativas formalizadas puede dificultar la capacidad de la empresa para demostrar diligencia en el tratamiento y protección de datos personales conforme a lo establecido en el RGPD.

En consecuencia, el problema identificado no se limita únicamente a una cuestión tecnológica, sino que refleja una carencia estructural en la gestión organizativa de la seguridad de la información. Esta situación representa una oportunidad para diseñar e implantar un modelo de gestión basado en buenas prácticas internacionales, como las establecidas en la norma ISO/IEC 27001:2022, que permita a la empresa fortalecer su capacidad para gestionar riesgos tecnológicos, proteger sus activos de información y garantizar la continuidad y fiabilidad de sus operaciones.

4.1 Descripción de la empresa a intervenir

4.1.1 Misión

La misión de Pick-up Llinars S.L. es ofrecer una experiencia gastronómica de calidad en un entorno cercano, dinámico y familiar, proporcionando a clientes y visitantes un espacio de encuentro que contribuya a la vida social del municipio de Llinars del Vallès. La empresa busca diferenciarse mediante la calidad de sus productos, la atención al cliente y la creación de un ambiente que combine restauración, convivencia y vínculo con la comunidad local.

Para ello, la organización se orienta hacia una gestión eficiente de sus recursos, la mejora continua de sus procesos y la incorporación progresiva de herramientas tecnológicas que permitan optimizar la operativa del negocio, garantizando al mismo tiempo la seguridad de la información y el cumplimiento de las obligaciones normativas aplicables.

4.1.2 Visión

La visión de Pick-up Llinars S.L. es consolidarse como un establecimiento de referencia en el municipio de Llinars del Vallès, reconocido por la calidad de su oferta gastronómica, la experiencia ofrecida a sus clientes y su papel como espacio de encuentro para la comunidad local.

En el medio plazo, la empresa aspira a fortalecer su modelo de negocio mediante la modernización de su oferta de productos, la mejora de la rentabilidad e incorporación de buenas prácticas de gestión organizativa y tecnológica. Asimismo, pretende integrar progresivamente estándares de gestión y seguridad que permitan reforzar la protección de la información, la continuidad del servicio y la confianza de clientes, empleados y colaboradores.

Nuestra visión es consolidarnos como la opción número uno en nuestra ciudad, siendo reconocidos por el excelente servicio que ofrecemos y por la alta calidad de nuestras instalaciones. Aspiramos a proporcionar un entorno de comodidad y seguridad para todos nuestros clientes, ya sea que nos visiten por motivos de negocio o de placer. Buscamos que cada persona que elija nuestros servicios experimente una estancia satisfactoria, donde la atención personalizada y las instalaciones cuidadas sean nuestro sello distintivo. Garantizando la total satisfacción y regreso de cada persona que nos visita.

4.1.3 Mapa de procesos

Procesos Estratégicos:
Los procesos estratégicos son aquellos que están relacionados con la planificación y toma de decisiones a largo plazo.

- Dirección General
- Gestión y Finanzas

Procesos Operativos:
Los procesos operativos son aquellos que están relacionados con las actividades diarias y rutinarias. Estos procesos son esenciales para brindar un servicio de calidad a los comensales.

- Ventas y Reservas
- Limpieza
- Mantenimiento
- Compras

Procesos de Apoyo
Los procesos de apoyo son aquellos que brindan soporte a los procesos estratégicos y operativos. Estos procesos son fundamentales para garantizar el buen funcionamiento de la empresa.

- Recursos Humanos
- TI

4.1.4 Descripción del proceso a intervenir

El proceso para intervenir corresponde a la gestión y protección de los activos de información y sistemas tecnológicos. En Pick-up Llinars SL para el desarrollo de su actividad necesita un conjunto de recursos tecnológicos, información y de actividades asociadas a la administración para poder llevar a cabo la operativa diaria del negocio.
La distribución de la organización de estos activos tecnológicos es la siguiente: Local principal del establecimiento y el almacén, donde se encuentra la infraestructura principal de conectividad y gestión administrativa.
El ordenador servidor, se ubica en el almacén, este actúa como punto central para la gestión administrativa del negocio. Con Windows 10 es utilizado exclusivamente por los propietarios de la empresa mediante una cuenta Microsoft. Este ordenador gestiona la información administrativa del negocio y se realiza el almacenamiento de información importante para la empresa. Hay que añadir que el equipo ejecuta la aplicación de gestión BDP Hostelería, utilizada para la gestión de ventas, productos y la configuración entre los dos sistemas de punto de venta.
El servidor se encuentra conectado a la red principal de fibra óptica, esta está instalada en el almacén, entre el tpv pc y el servidor se enlazan mediante un enlace inalámbrico basado en dispositivos Ubiquiti Nanobeam m5. Esta configuración permite que el sistema de gestión instalado en el ordenador del almacén pueda consultar y administrar la información generada en el sistema tpv del local. El Servidor dispone de periféricos conectados mediante interfaces USB, de los cuales están: El escáner utilizado para la digitalización de facturas y albaranes una impresora empelada para tareas administrativas.
En el local donde se encuentra la zona de clientes y mesas, es decir la parte operativa bruta. Encontramos el ordenador TPV, que es el equipo principal para la gestión de cobros y operaciones de venta realizadas por los trabajadores durante la jornada laboral. Este tiene el BDP hostelería en su versión de terminal TPV, pero la base de datos opera en local a través de SQL. Este TPV se registran las ventas del establecimiento como la gestión de productos y comandas. Para poder desarrollar esta función correctamente el local cuenta con 4 impresoras térmicas para tiquets.
El TPV-PC se utiliza para el registro de la jornada laboral de los empleados, utilizando una aplicación desarrollada con Google Script, en el cual los trabajadores deben de identificarse mediante su documento de identidad para registrar su entrada y salida del puesto de trabajo. En la zona de cocina aparte de tener dos impresoras de tickets para las comandas, se dispone de una tablet para activar la reproducción de música del local y el acceso a la trazabilidad de los alimentos también con una aplicación desarrollada con Google Script.
En relación con el almacenamiento de información, la organización utiliza Google Drive como plataforma de almacenamiento en la nube para guardar documentación administrativa y empresarial. Parte de la información generada en el entorno administrativo se sincroniza con esta plataforma, lo que permite a los socios acceder a determinados documentos desde diferentes ubicaciones.

En conjunto, el proceso de gestión de activos de información en Pick-up Llinars S.L. integra los sistemas informáticos, la infraestructura de red, las aplicaciones de gestión y los servicios de almacenamiento digital que permiten el funcionamiento de las actividades administrativas y comerciales del negocio. La correcta administración de estos recursos resulta esencial para garantizar la continuidad operativa del establecimiento y la disponibilidad de la información necesaria para el desarrollo de la actividad empresarial

Activo	Tipo	Ubicación	Función
PC Servidor	Hardware	Almacén	Gestión administrativa y conexión con TPV
TPV	Hardware/Software	Local	Registro de ventas
BDP Hostelería	Software	Servidor / TPV	Gestión de cobros
Base de datos SQL	Software	TPV	Almacenamiento de ventas
Google Drive	Servicio Cloud	Online	Almacenamiento documental
Router ISP	Infraestructura red	Almacén	Conectividad internet
Enlace Ubiquiti	Infraestructura red	Almacén-Local	Conexión de red

Tabla 1: Inventario de activos tecnológicos en Pick-up Llinars S.L.

4.1.5 Descripción del problema que presenta el proceso

Al realizar el análisis del proceso de gestión y protección de los activos de información nos ha permitido observar o identificar que este se desarrolla sin un marco formal de gestión que regule de manera estructurada la administración y protección del entorno tecnológico y de la información que soporta el negocio.
La organización realiza principalmente de forma operativa, la gestión de los recursos tecnológicos y de la información, los responsables del establecimiento adoptan decisiones basadas en la experiencia práctica adquirida en su día a día. Esto supone que muchas de las decisiones no siguen procedimientos ni criterios organizativos al no disponer de políticas internas que establezcan como debe de gestionarse los activos de información dentro de la empresa.
En primer lugar, no disponen de un inventario estructurado de activos de información que permita localizar e identificar de forma sistemática los equipos, sistemas y aplicaciones que forman parte de la organización. En el ámbito de la seguridad de la información, la identificación y clasificación de los activos es esencial para la gestión de riesgos, tal como establece las buenas prácticas recogidas en la norma ISO/IEC 27001:2022.
Asimismo, el proceso carece de procedimientos formales que regulen la administración de los sistemas y el acceso a la información gestionada por la empresa. Los recursos tecnológicos utilizados para la gestión del negocio —incluyendo el sistema TPV, el ordenador de administración ubicado en el almacén y los servicios de almacenamiento en

la nube— se utilizan en el marco de la operativa diaria, pero no existe una política organizativa que establezca criterios definidos para la gestión de usuarios, la administración de permisos o la protección de la información almacenada en estos sistemas.

Otro elemento relevante del proceso es la gestión de la información empresarial almacenada en los distintos sistemas utilizados por la organización. En el caso de Pick-up Llinars S.L., una parte significativa de la información administrativa se almacena en Google Drive, donde se gestionan documentos relacionados con la facturación, la contabilidad, la administración interna del negocio, la documentación laboral de los empleados —incluyendo nóminas y datos personales— y materiales asociados a actividades de marketing y gestión empresarial. Paralelamente, el sistema TPV utilizado por el establecimiento almacena en una base de datos SQL el registro histórico de las operaciones de venta realizadas por la empresa desde el inicio de su actividad en el año 2017.

A pesar de la relevancia de esta información para el funcionamiento del negocio, el proceso analizado no dispone de una estructura organizativa que defina formalmente los criterios para su gestión, almacenamiento y protección. En consecuencia, la administración de estos sistemas y de la información que contienen se realiza sin un modelo estructurado de gestión de seguridad de la información, lo que evidencia la ausencia de un enfoque sistemático alineado con estándares internacionales de buenas prácticas en seguridad de la información.

Desde una perspectiva organizativa, esta situación refleja que el proceso de gestión de activos de información presenta un bajo nivel de formalización, ya que las actividades relacionadas con la administración de sistemas y la gestión de información se realizan sin un marco de gobernanza definido, sin políticas documentadas y sin procedimientos operativos que permitan gestionar de manera estructurada los activos de información utilizados por la organización.

Esta falta de formalización del proceso constituye el problema principal identificado en la organización y justifica la necesidad de diseñar una propuesta de intervención basada en la implantación de un modelo de gestión de seguridad de la información alineado con buenas prácticas internacionales como las establecidas en la norma ISO/IEC 27001:2022, que permita estructurar este proceso y mejorar la gestión de los activos de información dentro de la empresa.

5 Establecimiento de planes de acción para la solución del problema

Con el objetivo de solucionar las debilidades identificadas en el proceso de gestión y protección de los activos de información en Pick-up Llinars S,L, nos planteamos el diseño de un conjunto de planes de acción orientados a fortalecer la gestión de la seguridad de la información dentro de la organización.

Esta propuesta se basa en los principios y requisitos establecidos en la norma internacional ISO/IEC 27001:2022, definiendo un marco de referencia para la posterior implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Estos planes de acción nos permiten estructurar de forma sistemática la gestión de los activos de información, así como el establecimiento de controles que reduzcan el riesgo asociado al uso de sistemas tecnológicos dentro de la organización.

Pick-up Llinars S.L se enfrenta a estos desafíos partiendo de una estructura organizativa limitada, y con una operativa diaria que depende directamente del correcto funcionamiento de sus sistemas informáticos. Para que el cambio sea real, los planes de acción se diseñan teniendo en cuenta las características específicas del negocio.

Con el contexto empresarial expuesto, la estrategia se orienta a establecer medidas organizativas y técnicas que permitan estructurar el proceso de gestión de activos de información, mejorar el control y avanzar hacia un modelo de gestión alineados con las normas y buenas prácticas internacionales.

5.1 Establecimiento de objetivos

Los siguientes objetivos desarrollan y amplían los objetivos específicos definidos en la sección 3.2. En la actualidad la seguridad de la información se ha convertido en un pilar estratégico para las organizaciones debido al aumento en el uso de sistemas digitales para la gestión de operaciones, almacenamiento de información y comunicación con clientes y proveedores. En este sentido y como hemos ido diciendo en los puntos anteriores es esencial la implantación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI), que nos permite establecer un marco estructurado para identificar, evaluar y tratar los riesgos asociados a la información y a los sistemas tecnológicos que la soportan (ISO/IEC, 2022).

En lo referente a la ISO/IEC 27001:2022, nos detalla los requisitos necesarios para el diseño, implementación, mantenimiento y la mejora de forma continuada de un SGSI en nuestra organización. Con el principal objetivo en cuanto a seguridad que son el cumplimiento de la triada: Confidencialidad, integridad y disponibilidad de la información.

Este enfoque de gestión de riesgos propuestos por la norma nos implica la identificación de los activos de información relevantes, el análisis de amenazas y vulnerabilidades que

puedan afectar y aplicar los controles de seguridad pertinentes para reducir los riesgos a niveles aceptables (ISO, 2018).

En nuestro caso de estudio Pick-up Llinars SL, se hace necesario llevar a cabo estas implementaciones para proteger los sistemas utilizados por la organización y garantizar la continuidad de las operaciones. Son muchos los estudios que hablan sobre la implementación de SGSI en las PYMEs. La adopción de marcos estructurados de seguridad contribuye a mejorar la gestión de los sistemas tecnológicos y reducir la exposición a incidentes de seguridad (Behl & Behl, 2017).
A continuación, detallamos los objetivos propuestos:

Objetivo 1. Evaluar el estado actual de seguridad de la información.

Se establece la realización de un diagnóstico del nivel de seguridad existente en los sistemas tecnológicos utilizados por Pick-up Llinars S.L. esto incluye equipos informáticos, aplicaciones de gestión, infraestructuras de red y servicios en la nube, con ello identificaremos las posibles vulnerabilidades y debilidades en la protección de los activos de información.

Objetivo 2. Identificar y clasificar los activos de información

Creación de un inventario estructurado de los activos de información utilizados en la empresa, esto incluye: hardware, software, bases de datos, y documentación digital, de esta manera establecemos un control adecuado sobre los recursos tecnológicos que soportan la actividad del negocio. La identificación de activos es uno de los primeros pasos recomendados en la gestión de la seguridad de la información dentro de los sistemas de gestión basados en ISO/IEC 27001 (ISO/IEC, 2022).

Objetivo 3. Analizar los riesgos asociados a los sistemas de información

Identificar las amenazas y vulnerabilidades que pueden afectar a los activos de información de la empresa, evaluando el impacto potencial que podrían generar sobre la operativa del negocio, la continuidad del servicio y el cumplimiento de la normativa vigente en materia de protección de datos. El análisis de riesgos constituye un componente fundamental dentro de los sistemas de gestión de seguridad de la información, ya que permite priorizar la aplicación de controles en función del nivel de riesgo identificado (ISO, 2018).

Objetivo 4. Definir e implementar controles de seguridad

En todo proceso el establecimiento de controles técnicos, organizativos y procedimentales orientados a reducir los riesgos, son medidas necesarias que están relacionados con la gestión de accesos, protección de sistemas, copias de seguridad, estructura y seguridad de red y gestión de incidentes de seguridad de la información. Alineados con las buenas prácticas establecidas en la norma ISO/IEC 27002 nos proporciona un conjunto de controles de seguridad para establecer un SGSI sólido y permanente en nuestra organización.

Objetivo 5 Establecer las bases para implantación de un SGSI

Diseñar una propuesta de mejora alineada con los requisitos de la norma ISO/IEC 27001:2022 que permita a Pick-up Llinars S.L. avanzar hacia un modelo estructurado de gestión de seguridad de la información adaptado a las características de una pequeña empresa del sector de la hostelería.

5.2 Descripción de la solución

Durante el proceso de auditoría realizado en Pick-up Llinars S.L. se identificaron diversas debilidades en la gestión de los sistemas de información y en la protección de los activos digitales utilizados por la organización. Estas debilidades afectan principalmente a la gestión de accesos, la protección de los sistemas informáticos, la seguridad de la infraestructura de red y la gestión de copias de seguridad.

Con el fin de reducir los riesgos asociados a estas vulnerabilidades, se propone la implantación de un conjunto de medidas de seguridad orientadas a mejorar la protección de los sistemas y la información gestionada por la empresa.

A continuación, se describen los principales problemas identificados durante el diagnóstico y las soluciones propuestas para su mitigación.

1. Ausencia de control de accesos en sistemas informáticos
Problema identificado
Durante el análisis de los sistemas informáticos se observó que los equipos utilizados por la organización emplean credenciales compartidas entre varios trabajadores, lo que dificulta la trazabilidad de las acciones realizadas en los sistemas y aumenta el riesgo de accesos no autorizados a información sensible.
Solución propuesta
Se propone implantar un sistema de gestión de accesos basado en cuentas de usuario individuales para cada trabajador que utilice los sistemas informáticos de la empresa. Asimismo, se establecerán políticas de contraseñas seguras y procedimientos de alta y baja de usuarios.
Control ISO relacionado
ISO/IEC 27002:2022 - Control 5.15 Control de acceso
ISO/IEC 27002:2022 - Control 5.17 Información de autenticación

2. Falta de copias de seguridad estructuradas
Problema identificado
El análisis de la infraestructura tecnológica de Pick-up Llinars S.L. evidenció que el sistema TPV, donde se almacena la base de datos de ventas, no dispone de un sistema

automatizado de copias de seguridad que garantice la recuperación de la información en caso de fallo del sistema.
Solución propuesta
Se propone establecer una política de copias de seguridad periódicas que incluya la realización automática de backups del sistema TPV y de la base de datos SQL asociada, así como su almacenamiento en un entorno seguro separado del sistema principal.
Control ISO relacionado
ISO/IEC 27002:2022 – Control 8.13 Copias de seguridad

3. Infraestructura de red sin protección perimetral
Problema identificado
La infraestructura de red utilizada por la organización carece de dispositivos específicos de seguridad perimetral, lo que puede facilitar accesos no autorizados desde redes externas o la propagación de software malicioso dentro de la red interna.
Solución propuesta
Se propone la implementación de un sistema de firewall que permita controlar el tráfico de red entrante y saliente, así como la segmentación de la red interna para separar los sistemas críticos de otros dispositivos conectados a la red.
Control ISO relacionado
ISO/IEC 27002:2022 – Control 8.20 Seguridad de redes

4. Ausencia de políticas de seguridad de la información
Problema identificado
Durante el proceso de auditoría se constató que la organización no dispone de políticas formales que regulen el uso de los sistemas informáticos ni el tratamiento de la información dentro de la empresa.
Solución propuesta
Se propone elaborar un conjunto de políticas de seguridad de la información que definan las normas de uso de los sistemas tecnológicos, las responsabilidades del personal y los procedimientos relacionados con la gestión de incidentes y la protección de la información.
Control ISO relacionado
ISO/IEC 27002:2022 – Control 5.1 Políticas de seguridad de la información

5. Ausencia de procedimiento de gestión de incidentes
Problema identificado
La organización no dispone de procedimientos definidos para la detección, registro y gestión de incidentes de seguridad relacionados con los sistemas informáticos.
Solución propuesta
Se propone la creación de un procedimiento de gestión de incidentes que establezca los pasos a seguir en caso de detectar un incidente de seguridad, incluyendo su registro, análisis y aplicación de medidas correctivas.
Control ISO relacionado
ISO/IEC 27002:2022 – Control 5.24 Gestión de incidentes de seguridad de la información

5.3 Secuencia de actividades para ejecución de la solución

Para realizar la implementación del modelo de gestión de seguriad de la información propuesto para la organización Pick-up Llinars S.L, establecemos una secuencia de actividades orientadas a implementar las medidas de seguridad definidas en el apartado anterior.
Basandonos en la norma ISO/IEC 27001, que nos estructura los procesos para nuestro SGSI.
Además para garantizar una correcta ejecución de las actividades descritas y asegurar la coordinación entre las diferentes áreas de la organización, se designará a uno de los socios de Pick-up Llinars S.L como responsable interno del proceso de implantación del SGSI.
Tal como establece la norma ISO/IEC 27001:2022, el liderazgo y la asginación clara de responsabilidades son eleemntos clave para asegurar la eficacia de los sistemas de gestión de seguridad de la información (ISO/IEC, 2022).

A continuación, exponemos las principales actividades necesarias para la implantación de la solución propuesta.

1. Inventario de activos de información
La primera actividad consiste en la identificación y documentación de los activos de información utilizados por Pick-up Llinars S.L.
En este proceso se realizará un inventario de los sistemas tecnológicos utilizados por la empresa, incluyendo:
el servidor de administración ubicado en el almacén
el sistema TPV utilizado para la gestión de ventas
la base de datos SQL que almacena la información histórica de transacciones
los dispositivos de red que conectan el almacén con el establecimiento mediante enlaces inalámbricos Ubiquiti
los servicios de almacenamiento en la nube utilizados para la gestión documental.
Este inventario permitirá identificar los activos críticos para la continuidad del negocio y establecer prioridades en su protección.

2. Evaluación de riesgos de seguridad
Una vez identificados los activos de información, se procederá a realizar una evaluación de riesgos que permita identificar las amenazas y vulnerabilidades que pueden afectar a los sistemas utilizados por la organización.
Entre los riesgos identificados se encuentran:
pérdida de información por ausencia de copias de seguridad estructuradas
accesos no autorizados a los sistemas informáticos debido al uso de credenciales compartidas
vulnerabilidades en la infraestructura de red derivadas de la ausencia de dispositivos de seguridad perimetral
exposición de información sensible almacenada en servicios en la nube.
Los resultados de este análisis permitirán priorizar la implantación de medidas de seguridad.
Para la evaluación de riesgos se utilizará una metodología cualitativa basada en la combinación de impacto y probabilidad, siguiendo las recomendaciones de la norma ISO 31000 y del estándar ISO/IEC 27005 para la gestión de riesgos en sistemas de seguridad de la información.

Se utilizará la siguiente escala de valoración:

Nivel	*Impacto*	*Probabilidad*
Bajo	Impacto limitado en la operativa	Poco probable
Medio	Impacto moderado en operaciones	Posible
Alto	Impacto grave en continuidad del negocio	Probable

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de riesgo	Control ISO recomendado
Sistema TPV BDP	Malware o ransomware	Ausencia de antivirus	Alto	Medio	Alto	ISO 27002 – 8.7 Protección contra malware
Base de datos SQL ventas	Pérdida de datos	Backup no automatizado	Alto	Alto	Crítico	ISO 27002 – 8.13 Copias de seguridad
PC servidor administración	Acceso no autorizado	Credenciales compartidas	Medio	Alto	Alto	ISO 27002 – 5.17 Información de autenticación
Google Drive corporativo	Acceso indebido	Gestión de permisos no estructurada	Medio	Medio	Medio	ISO 27002 – 5.15 Control de acceso
Red interna	Intrusión externa	Router sin firewall dedicado	Alto	Medio	Alto	ISO 27002 – 8.20 Seguridad de redes
Conexión Ubiquiti almacén-local	Intercepción de tráfico	Seguridad inalámbrica limitada	Medio	Medio	Medio	ISO 27002 – 8.21 Seguridad de servicios de red
Documentación laboral	Exposición de datos personales	Falta de política de protección de datos	Alto	Medio	Alto	ISO 27002 – 5.34 Protección de datos
Sistema de fichaje	Manipulación de registros	Control de accesos limitado	Medio	Medio	Medio	ISO 27002 – 8.2 Gestión de privilegios
Equipos informáticos	Fallo hardware	Ausencia de plan de continuidad TI	Alto	Bajo	Medio	ISO 27002 – 5.30 Preparación TIC para continuidad

Tabla3: Matriz de evaluación de riesgos basada en ISO/IEC 27005 aplicada a Pick-up Llinars S.L.

Los resultados de la matriz de riesgos muestran que los riesgos con mayor criticidad en la infraestructura tecnológica de Pick-up Llinars S.L. están relacionados principalmente con:
la ausencia de un sistema estructurado de copias de seguridad del TPV,
la falta de protección frente a malware en algunos equipos,
la gestión inadecuada de credenciales y accesos a sistemas,
la ausencia de protección perimetral en la infraestructura de red.
Estos riesgos afectan directamente a la disponibilidad de los sistemas de gestión de ventas, a la protección de la información empresarial y al cumplimiento de la normativa de

protección de datos personales, por lo que deben ser considerados prioritarios dentro del plan de implantación del SGSI.
En base a los resultados obtenidos, se priorizará la implementación de controles de seguridad alineados con el Anexo A de la norma ISO/IEC 27001:2022, con el objetivo de reducir el nivel de riesgo a valores aceptables para la organización.

3. Definición de políticas de seguridad
En esta fase se elaborarán las políticas de seguridad de la información que regularán el uso de los sistemas tecnológicos dentro de la organización.
Estas políticas incluirán aspectos como:
control de accesos a sistemas informáticos
gestión de contraseñas
uso de dispositivos tecnológicos
realización de copias de seguridad
gestión de incidentes de seguridad.

4. Implantación de controles técnicos
Posteriormente se procederá a la implantación de controles técnicos orientados a mejorar la protección de los sistemas informáticos utilizados por la empresa.
Entre las medidas propuestas se encuentran:
instalación de un sistema firewall para proteger la red interna
implementación de un sistema de copias de seguridad automatizadas
instalación de soluciones antivirus en los equipos informáticos
establecimiento de cuentas de usuario individuales para el acceso a los sistemas.

5. Formación y concienciación del personal
La implantación del sistema de seguridad incluirá acciones de formación dirigidas a los trabajadores de la empresa con el objetivo de mejorar el conocimiento sobre buenas prácticas de seguridad digital.

6. Seguimiento y mejora continua
Finalmente, se establecerá un proceso de revisión periódica de las medidas de seguridad implantadas con el fin de evaluar su eficacia y realizar las mejoras necesarias.

5.4 Descripción de recursos necesarios para la ejecución de la solución

Para poder realizar la implantación del modelo de gestión de seguridad de la información en nuestro caso de estudio Pick-up Llinars S.L, será necesario que este disponga de una serie de recursos humanos, tecnológicos y organizativos que permitan ejecutar las medidas de seguridad definidas en los apartados anteriores.
Como la organización es una pequeña empresa en el sector de la hosteleria, la propuesta se basa en la integración de soluciones de seguridad adaptadas al tamaño y recursos de la empresa, se realizarán aquellas medidas que permitan reducir los riesgos identificados sin generar una complejidad operativa innecesaria.

Recursos humanos
Para la ejecución del proyecto se contará con la participación de los tres auditores responsables del análisis y diseño del sistema de gestión de seguridad de la información, así como con la colaboración de la dirección de la empresa.
Tal como se ha indicado en apartados anteriores, uno de los socios de Pick-up Llinars S.L. será designado como responsable interno del proceso de implantación del SGSI, actuando como interlocutor entre la organización y el equipo auditor. Este responsable participará en la recopilación de información necesaria para el análisis de riesgos, la definición de políticas de seguridad y la supervisión de las medidas de seguridad implantadas.
Responsable de Seguridad de la Información (Information Security Manager) Socio designado de Pick-up Llinars S.L. encargado de liderar la implantación del SGSI, supervisar el cumplimiento de las políticas de seguridad y coordinar las acciones con el equipo auditor. Será el responsable de la continuidad y mantenimiento del sistema una vez finalizada la implantación.

Equipo de implantación (Consultores / Auditores de seguridad) Formado por:

- David Almirón
- Alexis Andrade
- Cristhel Villao

Responsables de:

- Análisis del estado actual
- Identificación de riesgos
- Diseño del SGSI
- Implementación de controles
- Elaboración de documentación
- Formación del personal

Recursos tecnológicos
Para mejorar la seguridad de los sistemas informáticos utilizados por la organización se propone la incorporación o mejora de determinados recursos tecnológicos.
Entre los principales recursos tecnológicos necesarios se encuentran:
Software antivirus y antimalware
La instalación de soluciones antivirus en los equipos informáticos de la organización permitirá mejorar la protección frente a amenazas como malware o ransomware, reduciendo el riesgo de comprometer los sistemas utilizados para la gestión del negocio.
Sistema de protección endpoint (Antivirus) Microsoft Defender o equivalente → protección contra malware.
Firewall de red

Se propone la incorporación de un sistema de firewall que permita controlar el tráfico de red entrante y saliente, protegiendo la infraestructura tecnológica frente a accesos no autorizados y ataques externos.
Sistema de copias de seguridad
Se establecerá un sistema de copias de seguridad automatizadas para los datos críticos de la organización, especialmente la base de datos del sistema TPV, con el objetivo de garantizar la disponibilidad de la información en caso de fallo del sistema o incidente de seguridad.
Sistema de backup
Google Drive + automatización → recuperación de datos críticos.
Gestión segura de contraseñas
Se propone la utilización de políticas de contraseñas seguras y, en caso necesario, la utilización de gestores de contraseñas que permitan mejorar la seguridad en el acceso a los sistemas informáticos utilizados por la organización.
Sistema de autenticación
Implementación de MFA en cuentas críticas.
Recursos organizativos
Además de los recursos tecnológicos, la implantación del SGSI requerirá la elaboración de diversos documentos y procedimientos que permitan formalizar la gestión de la seguridad de la información dentro de la empresa.
Entre estos recursos organizativos se incluyen:
políticas de seguridad de la información
procedimientos de gestión de incidentes de seguridad
políticas de copias de seguridad
procedimientos de control de accesos a los sistemas informáticos
acciones de formación y concienciación en ciberseguridad dirigidas al personal de la empresa.
Estos recursos permitirán establecer una base organizativa que facilite la correcta implantación del sistema de gestión de seguridad de la información y su mantenimiento a lo largo del tiempo.
Los recursos tecnológicos identificados en esta sección han sido seleccionados teniendo en cuenta la viabilidad económica y operativa de Pick-up Llinars S.L., priorizando soluciones de bajo coste y fácil implementación, adecuadas a una microempresa del sector de la hostelería.

En este sentido, los recursos tecnológicos contemplados incluyen herramientas de seguridad como antivirus, sistemas de autenticación multifactor (MFA), soluciones de copia de seguridad y configuraciones de red seguras. Estos elementos han sido considerados dentro del presupuesto global del proyecto.

Esta integración entre recursos técnicos y planificación económica permite garantizar la coherencia del proyecto y asegurar la viabilidad de la implantación del SGSI en Pick-up Llinars S.L.

6 Definición del alcance de la solución, partes interesadas, cronograma y presupuestos.

La implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en Pick-up Llinars S.L. se plantea bajo un enfoque realista y adaptado a las características de una microempresa del sector de la hostelería, donde la continuidad operativa del negocio y la limitación de recursos condicionan la estrategia de implementación.

A diferencia de entornos corporativos, donde la seguridad puede desplegarse mediante grandes inversiones y equipos especializados, en este caso se ha optado por un modelo progresivo basado en la priorización de riesgos críticos, la optimización de recursos existentes y la implementación de controles de alto impacto con un coste asumible para la organización.

El objetivo de esta intervención no es la obtención inmediata de la certificación ISO/IEC 27001:2022, sino la adopción de sus principios y buenas prácticas como marco de referencia para mejorar el nivel de seguridad de la información y reducir la exposición a incidentes que puedan afectar al negocio.

6.1 Alcance final de la solución

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) ha sido definido teniendo en cuenta los activos, procesos y riesgos más significativos para la organización, poniendo especial énfasis en aquellos vinculados con la continuidad operativa y la protección de datos sensibles.

La solución comprende los sistemas críticos que sustentan las actividades empresariales, tales como el equipo servidor ubicado en el almacén, el terminal de punto de venta (TPV) del establecimiento, la infraestructura de red —incluyendo router y dispositivos Ubiquiti—, el entorno de almacenamiento en la nube gestionado a través de Google Drive, así como la base de datos SQL asociada al sistema de gestión BDP Hostelería.

Adicionalmente, dentro del alcance se incluyen los principales conjuntos de información administrados por la entidad: datos de ventas, información contable y fiscal, documentación interna y datos personales de los empleados (nóminas y documentación identificativa), todos ellos considerados de alta criticidad tanto operativa como legalmente (conforme al RGPD).

El diseño de este alcance ha estado condicionado por los riesgos detectados en la fase de análisis, destacándose la potencial pérdida de información, el acceso no autorizado a datos sensibles (como nóminas) y la eventual interrupción del TPV, eventos que impactarían directamente en la operación diaria del negocio.

Se han establecido limitaciones específicas para asegurar la viabilidad del proyecto, quedando excluidos aspectos como la certificación formal bajo ISO/IEC 27001, la implantación de soluciones avanzadas propias de grandes corporaciones (por ejemplo, SIEM o SOC) y la renovación de la infraestructura hardware existente.

Estas exclusiones responden a criterios de proporcionalidad y adecuación al contexto empresarial.

Para garantizar la efectividad de la solución propuesta, se cubrirán las necesidades técnicas dentro del presupuesto estimado por la empresa.

Se implementarán controles esenciales de la norma ISO/IEC 27001 dirigidos a mitigar vulnerabilidades de alto impacto, omitiendo temporalmente la certificación oficial por consideraciones vinculadas al estado inicial de desarrollo del negocio hostelero.

- **Protección de accesos y archivos**: Se procederá a una reorganización exhaustiva en la estructura de permisos de Google Drive, aplicando el principio de mínimo privilegio para limitar el acceso a documentación sensible (nóminas, contratos, DNIs). Esta medida se complementará con la obligatoriedad de autenticación multifactor (MFA) para las cuentas gestionadas por socios.
- **Resguardo de transacciones**: Se diseñará e implementará un protocolo automatizado para la realización de copias de seguridad cifradas de la base de datos SQL del sistema BDP Hostelería. Esta acción técnica permitirá la recuperación efectiva del historial de ventas y la funcionalidad del TPV ante fallos de hardware o incidentes como ataques de ransomware.
- **Cumplimiento regulatorio con terceros**: Se formalizarán las obligaciones emanadas del RGPD respecto a la cadena de suministro mediante la redacción y firma de un contrato de tratamiento de datos (DPA) con la gestoría externa encargada del procesamiento de información contable y laboral.

Con el fin de asegurar la viabilidad del plan de acción propuesto, se establece expresamente la prohibición de:

- La adquisición, actualización o sustitución de componentes hardware, dado que el proyecto está diseñado para operar sobre la base de los recursos tecnológicos preexistentes.
- La migración de sistemas hacia arquitecturas empresariales complejas o la contratación de servicios de monitoreo permanente.

Resultados esperados

La implementación del SGSI en Pick-up Llinars S.L. permitirá alcanzar los siguientes resultados:

- Reducción del riesgo de pérdida de información crítica del negocio.

- Mejora del control de accesos a los sistemas y a la información sensible.
- Protección adecuada de datos personales conforme a la normativa RGPD.
- Mayor disponibilidad del sistema TPV y de los sistemas operativos del negocio.
- Disminución de incidencias relacionadas con la seguridad de la información.
- Establecimiento de procedimientos documentados de seguridad.
- Mejora de la concienciación del personal en materia de seguridad de la información.
- Creación de una base estructurada para la mejora continua del SGSI.

Estos resultados permitirán mejorar la resiliencia operativa de la empresa y reducir el impacto de posibles incidentes de seguridad.

Partes interesadas

Para la correcta implementación del SGSI, se identifican las siguientes partes interesadas:

Partes interesadas internas

- Socios de Pick-up Llinars S.L.
- Personal del establecimiento
- Responsable interno de seguridad de la información

Partes interesadas externas

- Gestoría externa
- Proveedores tecnológicos
- Clientes del establecimiento
- Administración pública (Agencia Española de Protección de Datos)
- Auditores del proyecto

La identificación de las partes interesadas permite asegurar la correcta implementación del SGSI y facilitar la coordinación durante la ejecución del proyecto.

6.2 Identificación de responsables de las actividades para ejecución

Dada la estructura organizativa de Pick-up Llinars S.L., caracterizada por la ausencia de un departamento de tecnologías de la información, se ha definido un modelo de responsabilidades claro y centralizado, con el objetivo de garantizar la eficacia en la toma de decisiones y la sostenibilidad del sistema en el tiempo.

En este sentido, se ha designado a uno de los socios de la empresa, concretamente David Almirón, como responsable de Seguridad de la Información. Este rol será clave tanto en la fase de implantación como en la posterior gestión del SGSI, asumiendo funciones de coordinación, supervisión de controles, gestión de incidentes y enlace con el equipo auditor.

El equipo de implantación, formado por los auditores David Almirón, Alexis Andrade y Cristhel Villao, serán responsables del análisis inicial, la evaluación de riesgos, el diseño del sistema, la implementación de las medidas de seguridad y la formación del personal. Su papel será fundamental en la fase inicial, pero progresivamente se transferirá el conocimiento al responsable interno para garantizar la autonomía de la organización.

El personal del establecimiento, aunque no dispone de un perfil técnico especializado, desempeña un papel relevante dentro del sistema de seguridad, siendo responsables del uso adecuado de los sistemas, la protección de credenciales y el cumplimiento de las políticas establecidas. En este caso, se parte de un nivel medio de competencias digitales y una buena predisposición al cambio, lo cual facilita la implantación de las medidas propuestas.

Por último, la gestoría externa actúa como parte interesada en el tratamiento de datos personales, siendo necesario formalizar su rol mediante un contrato de encargado de tratamiento conforme al RGPD.

6.3 Cronograma de ejecución

La planificación temporal del proyecto se ha definido bajo un enfoque progresivo, teniendo en cuenta la disponibilidad limitada de recursos y la necesidad de no interferir en la operativa diaria del negocio. La implantación del SGSI se estructura en fases secuenciales que permiten una adopción gradual de las medidas de seguridad.

Fase	Actividad	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1	Inventario de activos de información	•	•							
2	Evaluación y análisis de riesgos		•	•						
3	Definición de políticas de seguridad			•	•					
4	Implantación de controles técnicos				•	•				
5	Implantación de controles organizativos					•	•			
6	Formación y concienciación del personal						•			
7	Verificación y ajustes del sistema							•	•	
8	Seguimiento y mejora continua								•	•

Tabla 1. Cronograma de actividades.

Descripción del cronograma

El proyecto se inicia con la fase de inventario de activos, considerada fundamental para identificar los recursos críticos de la organización. Esta fase se desarrolla entre abril y mayo, permitiendo establecer una base sólida para el análisis posterior.

A continuación, durante los meses de mayo y junio, se realiza la evaluación de riesgos, en la que se identifican las amenazas y vulnerabilidades que afectan a los activos, priorizando aquellos riesgos con mayor impacto en la continuidad del negocio.

La fase de definición de políticas de seguridad, desarrollada entre junio y julio, permite establecer el marco normativo interno necesario para regular el uso de los sistemas y la protección de la información.

Posteriormente, se lleva a cabo la implantación de controles técnicos, centrados en aspectos como la seguridad de accesos, copias de seguridad y protección de sistemas, seguida de la implementación de controles organizativos orientados a la gestión de usuarios y buenas prácticas.

En septiembre se desarrolla la formación del personal, clave para garantizar la correcta aplicación de las medidas de seguridad, especialmente en un entorno donde los usuarios desempeñan un papel fundamental en la protección de la información.

Finalmente, el proyecto culmina con una fase de verificación, ajuste y mejora continua, que permite evaluar la eficacia de las medidas implementadas y asegurar la evolución del SGSI en el tiempo.

6.4 Presupuesto

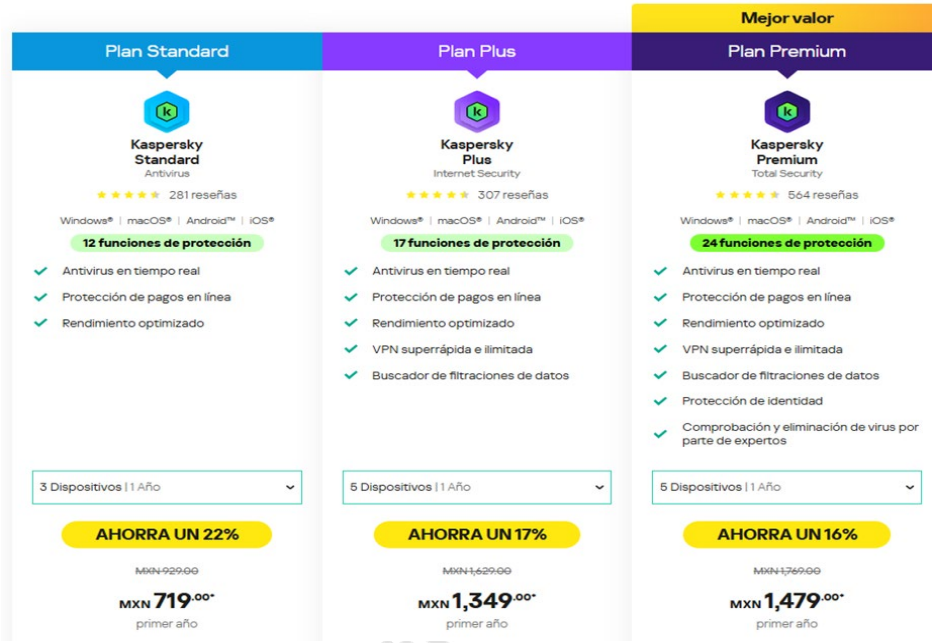
A diferencia de enfoques genéricos, el presupuesto se ha vinculado directamente a las fases del cronograma, permitiendo justificar cada inversión en función de las actividades realizadas.

Fase	Actividad	Coste estimado (€)	Justificación
1	Inventario de activos	500 €	Dedicación técnica para identificación y clasificación de activos
2	Análisis de riesgos	800 €	Elaboración de matriz de riesgos y evaluación de impacto
3	Políticas de seguridad	700 €	Redacción de documentación y definición de procedimientos
4	Controles técnicos	1.800 €	Configuración de red, backups, MFA, antivirus
5	Controles organizativos	400 €	Implementación de gestión de accesos y buenas prácticas
6	Formación	300 €	Capacitación del personal en seguridad
7	Verificación	300 €	Revisión y ajustes del sistema
8	Mejora continua	200 €	Seguimiento inicial del SGSI
9	Antivirus	72 €	Kaspersky Premium
10	Firewall	187 €	Kaspersky Next EDR Foundations
11	Sistema copia de seguridad	192 €	Google Al Pro
TOTAL		**5.451 €**	

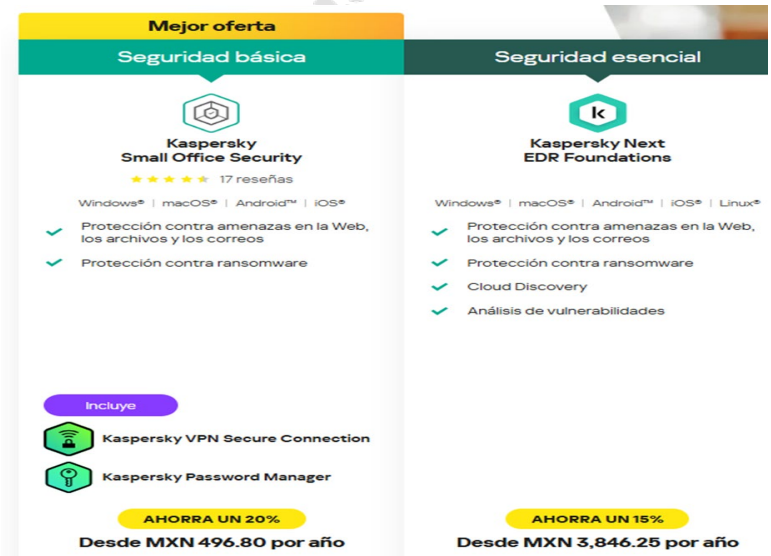
Tabla 2. Presupuesto.

- Fortalecimiento de la gobernanza de la seguridad de la información en una PYME: Caso Pick-up Llinars S.L

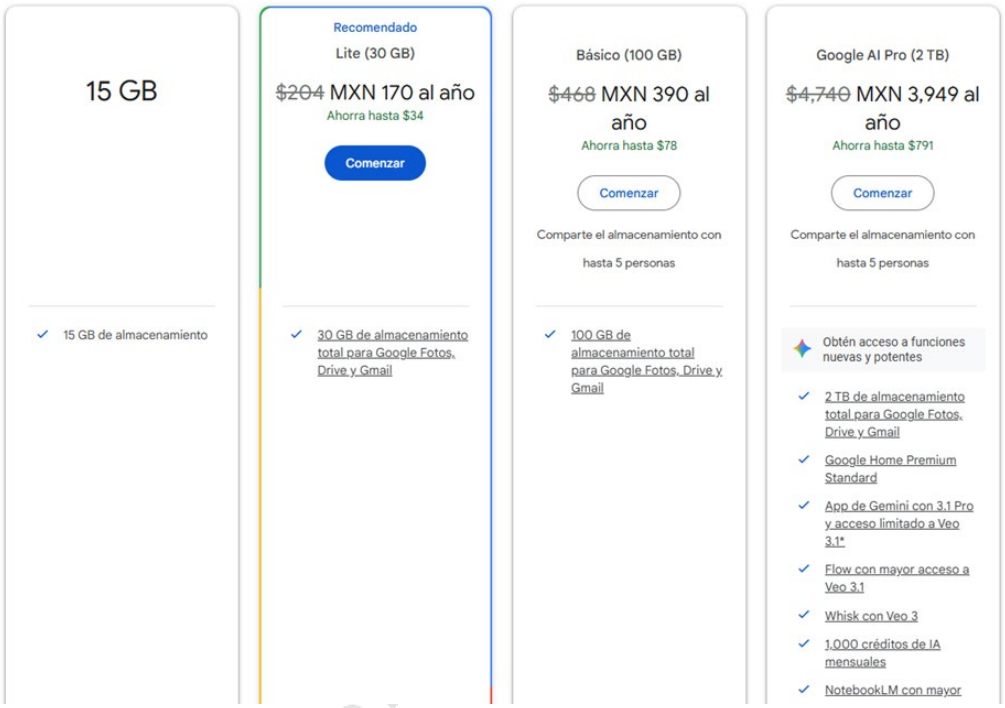
Cotización Antivirus Kaspersky:



Cotización Firewall Kaspersky:



Cotización Sistema Copia Seguridad:



Análisis de la planificación económica

La mayor inversión se concentra en la fase de implantación de controles técnicos, lo cual es coherente con la necesidad de mitigar los riesgos más críticos identificados, como la pérdida de datos, el acceso no autorizado a información sensible y la posible interrupción del servicio del TPV.

Por otro lado, las fases iniciales, como el inventario de activos y el análisis de riesgos, requieren una inversión moderada centrada principalmente en la dedicación técnica y el trabajo de consultoría, mientras que las fases finales presentan un coste reducido al tratarse de tareas de validación y seguimiento.

Este enfoque permite optimizar el uso de los recursos disponibles, garantizando que la inversión realizada tenga un impacto directo en la mejora de la seguridad de la información sin generar costes innecesarios.

La implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en Pick-up Llinars S.L. no debe entenderse únicamente como un coste, sino como una inversión

estratégica orientada a la reducción de riesgos y a la protección de la continuidad del negocio.

En el contexto de la organización, los principales riesgos identificados —pérdida de datos, acceso no autorizado a información sensible (como nóminas) y fallo del sistema TPV— pueden generar impactos económicos significativos, tanto directos como indirectos.

Estimación del impacto económico de un incidente

Se ha realizado una estimación aproximada del impacto que tendría la materialización de los riesgos más críticos:

- **Pérdida de datos (ventas, contabilidad):**
  - Coste de recuperación: 1.000 € – 3.000 €
  - Pérdida de información histórica: impacto operativo elevado
- **Acceso no autorizado a datos personales (RGPD):**
  - Posibles sanciones: hasta 10.000 € en casos leves en PYMEs
  - Daño reputacional y pérdida de confianza
- **Fallo del TPV (interrupción del servicio):**
  - Pérdida estimada diaria: 500 € – 1.500 €
  - Impacto directo en ingresos

Relación inversión vs riesgo

La inversión total estimada para la implantación del SGSI asciende a 5.451 €, lo que resulta significativamente inferior al impacto potencial de un único incidente de seguridad.

En este sentido, la implementación de medidas como copias de seguridad automatizadas, control de accesos y protección de sistemas permite reducir de forma considerable la probabilidad de ocurrencia de estos incidentes y su impacto asociado.

Retorno de la inversión (ROI)

Desde una perspectiva cualitativa, el retorno de la inversión se justifica por:

- Reducción del riesgo de pérdida de información crítica
- Disminución de la probabilidad de sanciones por incumplimiento del RGPD
- Mejora de la continuidad operativa del negocio
- Incremento de la confianza en la gestión de la información

Desde un punto de vista cuantitativo, se puede considerar que la inversión quedaría amortizada con la prevención de un único incidente relevante, como la pérdida de datos o la interrupción del servicio del TPV durante varios días.

Valor estratégico del SGSI

Más allá del retorno económico directo, la implantación del SGSI aporta un valor añadido a la organización, permitiendo establecer una base sólida para el crecimiento futuro, la profesionalización de los procesos internos y una posible evolución hacia la certificación en ISO/IEC 27001.

7 Referencias bibliográficas

LIBRO: ISO 27001 PARA EMPRESAS REALES: MONTAR, IMPLEMENTAR Y NO HACER EL RIDICULO PORQUE SIMULAR CUMPLIMIENTO YA NO CUELA. DE EDITORIAL TRAUMA TECNICO AUTOR PEDRO STEEN RIVAS PÉREZ

LIBRO: ISO/IEC 27001:2022 PASO A PASO IMPLEMENTACION, AUDITORIA Y MEJORA CONTINUA EDGARDO FERNANDEZ CLIMENT

KASPERSKY. (S. F.). *SMALL OFFICE SECURITY*. HTTPS://LATAM.KASPERSKY.COM/LP/SPECIAL-OFFER

KASPERSKY. (S. F.). *SMALL BUSINESS SECURITY*. HTTPS://LATAM.KASPERSKY.COM/SMALL-BUSINESS-SECURITY

GOOGLE. (S. F.). *PLANES DE GOOGLE ONE*. GOOGLE ONE. HTTPS://ONE.GOOGLE.COM/ABOUT/PLANS