



UNIVERSIDAD DE GRANADA

Cuaderno de prácticas

Administración de Sistemas y Seguridad

Máster Profesional en Ingeniería Informática

Curso académico 2022/2023

Autores

Juan José Peiró Garrido

José Alberto Gómez García

Lucas Gutiérrez Durán

José Antonio Pilartes Magalhães

Índice

| | |
|---|-----------|
| Descripción de la organización..... | 5 |
| Objetivos..... | 5 |
| Visión..... | 6 |
| Descripción del sistema..... | 7 |
| 1. Planificación del sistema de información (PSI)..... | 9 |
| 1.1 Identificación de las necesidades de Infraestructura Tecnológica..... | 9 |
| 1.2 Selección de la arquitectura tecnológica..... | 11 |
| 2. Desarrollo del Sistema de Información..... | 16 |
| 2.1. Estudio de la Viabilidad del Sistema (EVS)..... | 16 |
| 2.1.1. Establecimiento del alcance del sistema..... | 16 |
| 2.1.2. Estudio de la situación actual..... | 16 |
| 2.1.3. Definición de requisitos del sistema..... | 17 |
| 2.1.4. Descripción, valoración y selección de las alternativas de solución... | 17 |
| 3. Análisis del Sistema de Información (ASI)..... | 19 |
| 3.1. Definición del sistema..... | 19 |
| 3.1.1. Definición del entorno tecnológico..... | 19 |
| 3.1.2. Identificación de los usuarios del sistema..... | 20 |
| 3.2. Establecimiento de los requisitos..... | 21 |
| 3.2.1. Obtención, análisis y validación de requisitos..... | 21 |
| 3.2.2. Especificación de casos de uso..... | 23 |
| 3.3. Migración de datos y carga inicial..... | 24 |
| 3.4. Elaboración del modelo de procesos..... | 25 |
| 3.4.1. Características de los modelos de procesos del sistema..... | 25 |
| 3.4.2. Localización geográfica de la matriz de procesos..... | 27 |
| 3.5. Especificación del plan de pruebas..... | 27 |
| 3.5.1. Alcance de las pruebas..... | 27 |
| 3.5.2. Requisitos del entorno de pruebas..... | 27 |
| 3.5.3. Pruebas de aceptación del sistema..... | 28 |
| 4. Diseño del Sistema de Información (DSI)..... | 30 |
| 4.1. Requisitos de diseño y construcción..... | 30 |
| 4.1.1 Módulos del sistema..... | 30 |
| 4.1.2 Servidores de datos y de aplicaciones..... | 31 |
| 4.1.3. Conectividad en conexiones y red..... | 31 |
| 4.2. Especificación del entorno tecnológico..... | 32 |
| 4.2.1. Hardware..... | 32 |
| 4.2.2. Software..... | 33 |
| 4.2.3. Comunicaciones..... | 33 |
| 4.3. Requisitos de operación y seguridad..... | 34 |

| | |
|--|-----------|
| 4.4. Distribución de los datos..... | 34 |
| 4.5. Entorno de pruebas..... | 35 |
| 4.6. Requisitos de implantación..... | 36 |
| 5. Construcción del Sistema de Información (CSI)..... | 38 |
| 5.1. Preparación del entorno de generación y construcción..... | 38 |
| 5.2. Generación del código de los componentes y procedimientos..... | 39 |
| 5.3. Ejecución de las pruebas unitarias..... | 40 |
| 5.4. Ejecución de las pruebas de integración..... | 40 |
| 5.5. Elaboración de los manuales de usuario..... | 41 |
| 5.6. Definición de la formación de usuarios finales..... | 41 |
| 5.7. Construcción de los componentes y procedimientos de migración y carga inicial de datos..... | 41 |
| 5.8. Aprobación del sistema de información..... | 42 |
| 6. Implantación y Aceptación del Sistema (IAS)..... | 43 |
| 6.1. Establecimiento del plan de implantación..... | 43 |
| 6.1.1. Definición del plan de implantación..... | 43 |
| 6.1.2. Especificación del equipo de implantación..... | 43 |
| 6.2. Formación necesaria para la implantación..... | 44 |
| 6.3. Incorporación del sistema al entorno de operación..... | 45 |
| 6.4. Carga de datos al entorno de operación..... | 45 |
| 6.5. Pruebas de implantación del sistema..... | 46 |
| 6.5.1. Preparación de las pruebas..... | 46 |
| 6.5.2. Realización de las pruebas..... | 46 |
| 6.5.3. Evaluación de las pruebas..... | 46 |
| 6.6. Preparación del mantenimiento del sistema..... | 47 |
| 6.6.1. Establecimiento de la infraestructura..... | 47 |
| 6.6.2. Formalización del plan de mantenimiento..... | 47 |
| 6.7. Presentación y aprobación del sistema..... | 48 |
| 6.7.1 Convocatoria de la presentación del sistema..... | 48 |
| 6.7.2. Aprobación del sistema..... | 48 |
| 6.8. Paso a producción..... | 48 |
| 6.8.1. Preparación del entorno de producción..... | 48 |
| 6.8.2. Activación del sistema en producción..... | 49 |
| 7. Mantenimiento del Sistema de Información (MSI)..... | 50 |
| 7.1. Registro de la petición..... | 50 |
| 7.1.1. Registro de la petición..... | 52 |
| 7.1.2. Asignación de la petición..... | 53 |
| 7.2. Análisis de la petición..... | 54 |
| 7.2.1. Verificación y Estudio de la Petición..... | 54 |
| 7.2.2. Estudio de la propuesta de la solución..... | 55 |
| 7.3. Preparación de la implementación de la Modificación..... | 56 |

| | |
|---|----|
| 7.3.1. Identificación de Elementos Afectados..... | 56 |
| 7.3.2. Establecimiento de un plan de acción..... | 57 |
| 7.3.2. Especificación del plan de pruebas de regresión..... | 58 |
| 7.4. Seguimiento y Evaluación de los Cambios hasta la Aceptación..... | 59 |
| 7.4.1. Seguimiento de los cambios..... | 59 |
| 7.4.2. Aprobación y Cierre de la Petición..... | 60 |

Descripción de la organización

Kobiran es una de las cadenas de supermercados más importantes de la ciudad de Granada y está tomando la decisión de mejorar su sistema informático. Para ello contacta con nosotros, de manera que podamos desarrollar un sistema informático que mejore considerablemente la gestión de la empresa.

La empresa cuenta con diferentes edificios a lo largo de la ciudad, pero todos siguen la misma estructura y disposición de los elementos. La infraestructura de una tienda da soporte físico tanto a la venta de los productos, como para poder contener todo el equipo informático necesario para la gestión del software que tienen actualmente.

Se cuenta en la primera planta con toda la zona de venta de los productos, en la cual existen diferentes estanterías con los productos a comprar. Se cuenta también con una zona de carnicería y otra de pescadería. Además, también se encuentra la zona de cobro con las cajas registradoras. También se cuenta con un ascensor para acceder a la planta baja y escaleras para acceder tanto a la planta baja como al segundo piso.

En la segunda planta podemos encontrar la zona dedicada al equipo informático del supermercado. Existe una zona específica para los servidores del local y otra en la que se encuentran los técnicos informáticos. En esta última zona también se incluye la sala de videovigilancia del local. Esta planta solo cuenta con escaleras.

Se cuenta también con una planta baja en la que se ubican los almacenes de los productos. Uno para los productos congelados y otro para los productos frescos como frutas, verduras, etc. Esta planta cuenta con ascensor y escaleras.

Por último, también se cuenta con una zona exterior de parking que está gestionada por una barrera inteligente que actualmente es independiente del sistema informático.

Objetivos

El objetivo principal de la empresa es la implementación de un sistema informático completo que sea capaz de abarcar aquellos campos que requieren gestión tales como:

- Servicios web
- Automatización de los cobros
- Control de los productos
- Recursos humanos

- Seguridad
- Parking

Además, como objetivo secundario, se busca también la integración de todos los diferentes sistemas actuales que son independientes, como el parking. De manera que, de manera conjunta, todo se pueda gestionar como un único sistema informático del local.

Por otro lado, otro objetivo secundario es también buscar la integración y comunicación de los diferentes locales ubicados en la ciudad. De esta manera, cada local no sería independiente de los demás, sino que se podrían beneficiar los unos de los otros en lo que al sistema informático se refiere.

Visión

A corto plazo, se pretende mejorar la gestión de cada local de manera que haya una mejor organización. Esto facilitará la escalabilidad de la empresa. De esta manera, a medio y largo plazo se pretende que la empresa sea reconocida a nivel nacional, generando de esta manera grandes ganancias al negocio. También se pretende que, a nivel internacional, la empresa pueda ser reconocida por su sistema informático en cuanto a la gestión y control de los diferentes departamentos.

Descripción del sistema

El sistema informático que se pretende desarrollar va a contar en primera instancia con la siguiente lista de módulos principales:

Gestión de inventario

Con este módulo se pretende la gestión y administración de los productos que se almacenan en los almacenes de la planta subterránea. De manera diaria se controlará la caducidad de los alimentos perecederos y realizará de manera automática un análisis de las compras que se deben realizar en un futuro para poder mantener siempre abastecido el almacén del supermercado.

Control de parking

Este módulo gestionará la barrera del parking. Controlará que el cliente acceda correctamente al parking y comprobará su salida. En caso de que un cliente se exceda en el tiempo de parking, el sistema incrementará el coste de la plaza y se guardará una alerta en una base de datos.

Este módulo irá ligado al módulo de gestión de clientes, de manera que se pueda almacenar en un cliente los datos de las veces que ha utilizado el parking del local.

Gestión de videovigilancia

Este módulo gestionará lo referente a la seguridad, en especial a la videovigilancia del local. Todos los datos se almacenarán en los servidores del local y se borrarán los datos que tengan más de 1 semana para no ocupar demasiado espacio de almacenamiento.

Gestión de personal

Este módulo gestionará y administrará el personal que trabaje dentro de un local, de manera que, de manera obligada, cada trabajador del supermercado debe tener un perfil. Además, existirán diferentes roles, de manera que en función de la tarea del trabajador, podrá realizar una gestión diferente.

Este módulo se relaciona estrechamente con el de control de horarios y el de control de fichajes.

Control de horarios

Este módulo gestionará los horarios de los diferentes trabajadores del supermercado. De manera que, el sistema mantendrá un registro de todos los horarios para poder facilitar diferentes tareas como las extensiones de la jornada laboral, las vacaciones, etc. Para ello se creará, por ejemplo, un portal web por el cual se pueda realizar rápidamente este control de manera eficaz y segura.

Control de fichajes

De manera similar al módulo anterior, se creará otro módulo que gestione las entradas y las salidas de cada trabajador, de manera que se pueda controlar de manera concreta si un trabajador ha acudido a su puesto de trabajo a la hora a la que debía y si ha trabajado las horas de su jornada laboral. Esta característica se puede añadir en el portal web comentado en el módulo anterior, de manera que también se pueda gestionar desde ahí.

Gestión de clientes

Por último, se propone un módulo para poder gestionar a los clientes, de manera que se puedan facilitar diferentes ofertas a los mismos a través de una plataforma web o vía correo electrónico. Se puede facilitar un formulario para aquellos que quieran hacerse clientes y beneficiarse de diferentes ofertas.

Por otro lado, la empresa se podría ver beneficiada ganando la fidelización de los clientes. También se podría monitorizar diferentes parámetros como el parking comentado anteriormente, o las ofertas que canjea.

1. Planificación del sistema de información (PSI)

En primer lugar llevaremos a cabo la planificación del sistema de información donde conseguiremos un marco estratégico referente para nuestro sistema de Información. En esta fase elaboramos la arquitectura de información necesaria así como un plan que nos sirva de ayuda para nuestros objetivos estratégicos.

1.1 Identificación de las necesidades de Infraestructura Tecnológica

Los diferentes componentes hardware de los que se compondrá la infraestructura tecnológica del sistema que queremos desarrollar son:

Servidores

Para informatizar un supermercado se requieren varios servidores y componentes de red, dependiendo de la magnitud y complejidad del negocio, en nuestro caso al pensar en una empresa grande con distintas secciones y con posibilidad de expansión necesitamos al menos los siguientes servidores:

1. Servidor de punto de venta (POS)

Este servidor maneja las transacciones de venta y es el encargado de procesar los pagos. También puede gestionar el inventario y las promociones.

2. Servidor de base de datos

Este servidor almacena los datos del inventario, los precios, los clientes y los proveedores, entre otros datos importantes del supermercado. Además regula el control de fichajes previamente descrito y los horarios de los empleados.

3. Servidor de correo electrónico

Este servidor gestiona los correos electrónicos del personal del supermercado y también puede ser utilizado para la comunicación con los clientes y proveedores.

4. Servidor de seguridad

Este servidor es responsable de garantizar la seguridad de la red y los datos del supermercado, incluyendo el control de acceso y la gestión de las contraseñas. Además llevará a cabo tareas de video vigilancia.

5. Servidor de copias de seguridad

Este servidor realiza copias de seguridad de los datos del supermercado para evitar la pérdida de información importante.

Dentro estas alternativas podemos elegir principalmente entre comprar y elegir por nuestra cuenta los servidores para cada una de las funciones previamente

Puntos de venta (POS)

Son necesarios para realizar transacciones de venta de productos, lo que incluye un ordenador, una pantalla táctil, un lector de códigos de barras, un lector de tarjetas de crédito o débito, y una impresora de recibos.

Sistema de vigilancia

Se requiere de un sistema de vigilancia con cámaras de seguridad para monitorear y registrar los movimientos dentro del supermercado, incluyendo la entrada, la salida y las áreas de estacionamiento.

Sistema de control de acceso

Para gestionar el acceso de los empleados y clientes a ciertas áreas restringidas del supermercado, se requerirá un sistema de control de acceso que incluya dispositivos de lectura de tarjetas/códigos, y software para gestionar el acceso.

Dispositivos móviles

Los empleados necesitarán dispositivos móviles, como smartphones o tablets, para acceder a la información del supermercado o para realizar ciertas operaciones, como la gestión del inventario.

Sistema de sonido

Es necesario contar con un sistema de sonido para realizar anuncios y alertas en el supermercado, como anuncios de promociones, llamados a los empleados, o avisos de emergencia.

Interconexión de los elementos (tipo de conexión)

Existen diversos tipos de conexión que dependerá del tipo de dispositivo por lo que se usarán varios tipos de conexiones simultáneamente. Las opciones a explorar son: conexión Ethernet, Wi-Fi, bluetooth, fibra óptica, cable coaxial...

Disponibilidad y servicios críticos

En un entorno donde se manejan grandes cantidades de información, los procesos que se ejecutan para llevar a cabo estas tareas pueden requerir un tiempo significativo. Por lo tanto, cualquier interrupción o falla en el acceso a los datos puede causar una pérdida de productividad y retrasar el proceso de toma de decisiones.

Además, la disponibilidad constante también es importante para garantizar la integridad de los datos. Los sistemas que manejan grandes cantidades de datos pueden estar sujetos a errores, fallos de hardware o software, o incluso ciberataques. Si la disponibilidad no es constante, cualquier interrupción podría provocar la pérdida de datos o la corrupción de los mismos. De ahí que debemos asegurarnos que haya un buen suministro de electricidad para evitar que se caiga y haya un corte en la disponibilidad.

Contratación de terceros

Además de disponibilidad constante de los datos, también es importante atender a factores como la redundancia en el almacenamiento y la replicación de datos en múltiples ubicaciones. También es importante contar con sistemas de monitoreo y alerta temprana que permitan detectar cualquier problema antes de que cause un impacto significativo en la disponibilidad de los datos. Podemos delegar estas responsabilidades en otras empresas para este fin.

1.2 Selección de la arquitectura tecnológica

Servidores

En la implantación de los servidores podemos elegir entre tener nuestros servidores localmente o desplegar una plataforma cloud, no optamos por el sistema cloud debido a los altos costes que estos tienen a largo plazo para la empresa, de todas formas estos tienen múltiples ventajas y podría llevarse a cabo también, además no podemos tener un control de la infraestructura, lo cual es muy importante para el caso de los supermercados.

Aquí se puede ver algunas de las ventajas de cloud, pero como hemos comentado debido al costo a largo plazo y la falta de control total en la infraestructura, se ha optado por usar nuestros servidores locales.

1. Accesibilidad remota

Los servidores cloud se pueden acceder a través de internet desde cualquier lugar y dispositivo con conexión a internet, lo que significa que los gerentes y empleados pueden acceder a la información del supermercado desde cualquier lugar y en cualquier momento. Si incluimos una nueva tienda podemos coordinar fácilmente con las existentes independientemente donde se ubique.

2. Escalabilidad

Los servidores cloud se pueden escalar fácilmente según las necesidades del supermercado, lo que significa que se pueden agregar o eliminar recursos según sea necesario sin tener que invertir en hardware adicional. Lo que es bueno dependiendo a las necesidades de negocio de las distintas tiendas (si por ejemplo cerramos una tienda simplemente podremos eliminar recursos cuando se necesite, en caso de servidores locales supondría pérdida de dinero de los servidores comprados).

3. Seguridad

Los servidores cloud suelen tener mejores medidas de seguridad y protección de datos que los servidores locales, ya que las empresas que los administran suelen contar con personal especializado y herramientas de seguridad avanzadas para proteger la información. Lo que hace que podamos despreocuparse por estas facetas, aunque en nuestro caso de los supermercados no contamos con una gran cantidad de datos sensibles.

4. Continuidad del negocio: Los servidores cloud suelen ofrecer medidas de continuidad del negocio en caso de desastres naturales, fallos de hardware o de software, lo que garantiza que el supermercado pueda seguir operando sin interrupciones.

Ahora veamos las ventajas de los servidores locales que es lo que usaremos en la implantación de nuestro sistema de supermercados y será por las siguientes razones:

1. Control total sobre la infraestructura: Al mantener todos los servidores localmente, tienes un control total sobre tu infraestructura informática. Puedes administrar y configurar los servidores de acuerdo con tus necesidades específicas sin depender de proveedores externos.
2. Mayor privacidad y seguridad de los datos: A pesar de que en el cloud se cuenta con personal especializado, al no utilizar servicios en la nube, tenemos un mayor control sobre la privacidad y seguridad de tus datos. No hay riesgo de que terceros accedan a la información confidencial o que los servidores en la nube sufran violaciones de seguridad.
3. Latencia reducida: Al tener los servidores localmente, los tiempos de respuesta pueden ser más rápidos y la latencia se reduce. Esto es especialmente beneficioso si tu sistema informático requiere una

comunicación rápida con otros dispositivos o si manejas un alto volumen de transacciones en tiempo real.

4. Menor dependencia de la conectividad a Internet: Al mantener todos los servidores localmente, no dependes completamente de la conectividad a Internet. El sistema informático seguirá funcionando de manera interna sin depender de la nube.
5. Costos a largo plazo: Aunque inicialmente puede requerir una inversión más alta para adquirir y mantener los servidores locales, a largo plazo puede resultar más económico que depender de servicios en la nube. Al no estar pagando tarifas recurrentes por el uso de servicios en la nube, puedes reducir los costos operativos a largo plazo.

Conexiones

Debido a la gran variedad de dispositivos en nuestro, usaremos los distintos tipos de conexión, estas conectarán tanto los dispositivos del supermercado como los dispositivos a los distintos servidores y a internet:

1. Conexión Ethernet

Esta es una de las conexiones más comunes para dispositivos que requieren una conexión a Internet o a una red local. Se utiliza para conectar puntos de venta, cámaras de seguridad, sistemas de sonido, y otros dispositivos que necesitan acceso a la red.

2. Conexión inalámbrica Wi-Fi

Las conexiones inalámbricas son una excelente opción para dispositivos que necesitan movilidad. En un supermercado, se pueden utilizar para dispositivos portátiles como lectores de códigos de barras, tablets, y smartphones.

3. Conexión Bluetooth

Este tipo de conexión inalámbrica es excelente para dispositivos de corto alcance como pueden ser los sistemas de sonido, micrófonos y básculas.

4. Conexión por cable coaxial

Esta conexión se utiliza a menudo para transmitir señales de vídeo y audio a través de cables. Puede ser una buena opción para conectar cámaras de seguridad y sistemas de sonido.

Disponibilidad y servicios críticos

Para el problema de la disponibilidad se ha optado por usar generadores supletorios. El uso de generadores supletorios es una medida de contingencia esencial para asegurar la continuidad del servicio en caso de fallo en el suministro eléctrico. En la implementación de un sistema de venta, es importante tener en cuenta que la pérdida de electricidad podría significar la suspensión del servicio, lo que a su vez podría tener consecuencias negativas para la empresa y sus clientes.

Con la inclusión de los generadores supletorios, se garantiza que la venta no se detendrá en caso de un corte de energía. Además, estos generadores también permitirán la correcta suspensión de los dispositivos y equipos, asegurando la integridad de la información y la continuidad del servicio. Esto junto a los servidores de respaldo nos asegurará de que siempre se pueda dar un servicio continuo evitando así pérdidas económicas.

Contratación de terceros

Buscando en internet podemos encontrar diversas ofertas para evitar la redundancia en el almacenamiento, la replicación de datos en múltiples ubicaciones y con sistemas de monitoreo informáticos:

1-Pure Storage: Es una empresa de almacenamiento de datos con sede en California que ofrece soluciones de almacenamiento de datos all-flash y sistemas de gestión de datos en la nube. Su enfoque en la eficiencia de almacenamiento y la simplificación del manejo de datos puede ayudar a reducir la redundancia en el almacenamiento y la replicación de datos en múltiples ubicaciones. Pure Storage también ofrece soluciones de monitoreo informático avanzado para mejorar la gestión y el rendimiento del almacenamiento.

2-Rubrik: Es una empresa de gestión de datos en la nube que ofrece soluciones de backup y recuperación de datos, así como replicación de datos en múltiples ubicaciones. Rubrik se enfoca en la simplicidad y la automatización para simplificar la gestión de datos y reducir la redundancia en el almacenamiento. También cuenta con herramientas de monitoreo informático para asegurar el correcto funcionamiento de sus sistemas.

3-Dell EMC: Es una empresa de tecnología de la información que ofrece una amplia gama de soluciones de almacenamiento y gestión de datos. Su enfoque en la infraestructura de almacenamiento moderna puede ayudar a reducir la redundancia en el almacenamiento y la replicación de datos en múltiples ubicaciones. Dell EMC también ofrece herramientas de monitoreo informático para garantizar la salud y el rendimiento de sus sistemas. Además, su amplia gama de soluciones puede adaptarse a las necesidades específicas de su empresa.

De entre todas las opciones que hemos expuesto, en nuestro caso en particular, la mejor de todas es Rubrik.

Rubrik ofrece soluciones de backup y recuperación de datos (que ya tenemos nosotros mismos también), así como replicación de datos en múltiples ubicaciones, lo que es especialmente útil para empresas con múltiples sedes. Además, Rubrik se enfoca en la simplicidad y la automatización para simplificar la gestión de datos, lo que puede ser útil en un entorno de múltiples servicios informáticos. Rubrik también tiene una plataforma en la nube que puede ayudar a unificar la gestión de datos en múltiples servicios cloud, lo que podría ser útil para su empresa si utiliza varios servicios cloud. Por último, Rubrik también cuenta con herramientas de monitoreo informático para asegurar el correcto funcionamiento de sus sistemas, lo que es esencial para cualquier empresa que dependa de múltiples servicios informáticos. En general, Rubrik es una excelente opción para nuestra empresa ya que estamos buscando una solución de gestión de datos en un entorno de múltiples sedes y servicios cloud para nuestros distintos supermercados distribuidos.

2. Desarrollo del Sistema de Información

En esta sección se va a describir las etapas a seguir a la hora de desarrollar un sistema bajo el punto de vista de la administración de sistemas.

2.1. Estudio de la Viabilidad del Sistema (EVS)

Consiste en el análisis de un conjunto concreto de necesidades para proponer una solución a corto plazo, que tenga en cuenta restricciones técnicas, económicas, legales y operativas, como objetivo de la asignatura haremos más hincapié en las restricciones técnicas.

2.1.1. Establecimiento del alcance del sistema

Para el alcance hemos tenido en cuenta los requisitos determinantes que define la empresa en la descripción del sistema. Las necesidades del sistema pueden incluir o determinar a los siguientes usuarios:

- Administradores de servidores.
- Administradores de base de datos.
- Administradores de redes.
- Equipo de Seguridad.
- Empleados.

2.1.2. Estudio de la situación actual

En esta sección comentaremos la situación actual del sistema de la empresa en la perspectiva de administración de sistemas.

- Elementos físicos actuales
 - Servidores, distribuidos debidos a que son contrataciones cloud
 - Red cableada en las zonas de las cajas
 - Equipamiento para el monitoreo de videovigilancia
 - Barrera automática del parking, toda su gestión es independiente del sistema informático
- Usuarios participantes en el sistema actual
 - Administradores de redes
 - Informáticos
 - Personal servicios de terceros

Se puede obtener toda esta información con más detalle en la sección Descripción de la Organización.

2.1.3. Definición de requisitos del sistema

En esta etapa se detallarán los requisitos generales que deberá contar el sistema desde el punto de vista de la administración de sistema.

Políticas de seguridad

- Los edificios tendrán dispositivos de autenticación por datos biométricos, permiso manejado por tarjeta de acceso, también se dispondrá llave física para el personal para que sea accesible caso ocurra algún inconveniente con las modalidades de acceso antes mencionadas.
- En los casos de las plantas donde se encuentran los servidores el acceso será disponible solamente a personas autorizadas.
- La conexión remota a los servidores será permitida a los respectivos administradores solamente.
- Los accesos a los servidores serán monitorizados y almacenados en registros “*loggers*” con todo el historial de cuando fueron producidos (fecha, hora y lugar).
- Los backups de los servidores se harán en un corto periodo de tiempo y en las últimas horas del día.

Gestión de cambios

- Los posibles cambios que se requiere de la administración del sistema debe ser evaluado y aprobado, para que se pueda realizar esta acción habrá que entregar un informe a cada uno de los administradores del sistema implicado con un estudio que involucre la viabilidad de la propuesta.

2.1.4. Descripción, valoración y selección de las alternativas de solución

En este apartado se va a proponer elementos del sistemas teniendo en cuenta la arquitectura y los requisitos analizados en las sesiones anteriores.

- Matriz Procesos, localización geográfica: Los servidores serán reubicados en la planta superior del edificio. La gestión de los dispositivos del parking, pasará también en la planta donde se encuentran los servidores.
- Matriz de Datos, localización geográfica: El servidor de almacenamiento de datos se basará en un clúster conformado por almacenamiento SSD.
- Entorno tecnológico y comunicaciones: El entorno tecnológico se ha descrito y evaluado en la sección 1.2.

- Estrategia de implantación global del sistema: Hemos propuesto una estrategia conformada por los diferentes requisitos para evaluar la viabilidad de la implantación.
 - Instalación de un servidor propio compuestos por 7 blades, uno para cada aplicación del sistema, en sala refrigerada:
 - Business Intelligence
 - Administración de tareas
 - Control de acceso
 - Control de horas
 - Control de inventario
 - Control del sistema de seguridad
 - Gestión del Parking
 - Instalación de una red de tipo LAN en todas las plantas de los edificios y los almacenes aprovechando la instalación anterior.
 - Instalación de puntos de acceso inalámbrico en todas las plantas del edificio.
 - Instalación de los puntos de fichaje (control de horas) en los puntos establecidos para ello.
 - Instalación de cada uno de los controles de acceso y su correspondiente restricción de apertura de puerta en los puntos clasificados como restringidos.
 - Correcta instalación y configuración de cada una de las tablets que requerirá el sistema y su reparto a los respectivos responsables de ellas.

Teniendo en cuenta la situación económica actual de la empresa se ha llegado a la conclusión de que poseen recursos necesarios para adquirir todo el equipamiento mencionado anteriormente e invertir en la mejora de su gestión y así cumplir su visión como organización.

3. Análisis del Sistema de Información (ASI)

En este apartado se detalla el sistema a desarrollar y en el que implantar el producto software. Nos centraremos únicamente en las actividades en las que la administración de sistemas está directamente implicada.

3.1. Definición del sistema

3.1.1. Definición del entorno tecnológico.

En esta sección se realizará los elementos hardware y servicios de terceros elegidos para componer la arquitectura que se definió en apartados anteriores.

- Para los servidores, se deciden utilizar los chasis [ThinkSystem SR645 V3](#). Este chasis permite instalar dos procesadores AMD EPYC de 4º generación (la última disponible en la actualidad). Se decide utilizar [AMD EPYC 9354](#) al ofrecer un buen balance de núcleos y memoria caché L3.

En este chasis se puede equipar hasta 6 TB de memoria RAM DDR5 en 24 ranuras, aunque inicialmente se planteará equiparlos con 512 GB de RAM en 8 sticks de 64GB cada uno, pudiendo escalar estos de ser necesarios en el resto de ranuras (1.5 TB en total si se siguen empleando sticks de 64GB cada uno) . La ventaja de la memoria DDR5 es que incorpora corrección de errores (ECC) de serie.

Con respecto al almacenamiento, se decide emplear dos unidades de estado sólido de alta velocidad de 1 TB de la marca SABRENT ([consultar enlace](#)) y 3 unidades de almacenamiento de formato 3.5" y 4 TB de capacidad cada una de la marca Seagate ([consultar enlace](#)). Las unidades de alta velocidad se encontrarán dispuestas en RAID 1, para asegurar tolerancia a fallos, y en ellas se encontrará el sistema operativo y aplicaciones a utilizar. Las unidades mecánicas estarán dispuestas en un RAID 5, de manera que se dispondrá de 8 TB en total y redundancia frente en caso de fallar un disco.

En un primer momento no se contempla la compra de GPUs, dado que no se prevé un procesamiento exhaustivo de los datos ni aplicaciones de inteligencia artificial. En cualquier caso, el chasis permitiría incorporarlas a posteriori de ser necesario.

Cabe destacar que Lenovo ofrece 3 años de garantía en las piezas y la capacidad de contratar un servicio técnico in-situ al siguiente día laborable de 09:00 a 17:00. Esto último puede ser interesante en caso de emergencia, aunque contemos con técnicos propios cualificados para mantener, sustituir y reparar el equipo.

- Para la gestión de inventario y uso diverso por parte de los empleados se deciden emplear tablets [Lenovo Tab P11 Pro de 2º generación](#), dada la

calidad de la pantalla, el hardware puntero y la capacidad de adquirir “combos” con teclado y lápiz, lo cual facilita su uso.

- Para la identificación de los empleados y realizar el control de los horarios de entrada y salida del personal se decide emplear [el siguiente terminal](#). Esto se debe a que permite almacenar multitud de perfiles distintos y genera automáticamente los informes que requerimos, los cuales se pueden extraer mediante USB.
- Para los administradores, técnicos e informáticos en general, se plantea el uso de equipos portátiles ligeros y con capacidades de procesamiento razonables. Entre varias opciones, como Asus Zenbook, HP Envy o Dell XPS se decide emplear [LG Gram modelo 14Z90Q](#) dada su gran portabilidad y buena relación calidad-potencia-precio.
- Se emplea una red cableada LAN mediante Ethernet (típicos conectores RJ-45) para conectar los servidores entre sí, con los puestos de venta y el exterior. Para ello se hará uso de switches CISCO modelo CBS220-24T-4G.
- Para proporcionar conexión a Internet inalámbrico a los diferentes dispositivos de los empleados se utilizará la red anterior en conjunción con puntos de acceso WiFi Ubiquiti U6-LR.
- En lo relativo a seguridad se deciden emplear cámaras de seguridad IP cuyas grabaciones se vuelcan en los servidores anteriormente descritos. Así también, se instalan detectores de presencia a lo largo del supermercado.
- Para cerraduras de las áreas restringidas se decide utilizar el modelo Smart Door Lock M20 de Xiaomi, dado que permite autenticación por código permanente, clave temporal, huella dactilar, Bluetooth (de las tablets y otros dispositivos autorizados) entre otros métodos.
- Como se describe más adelante, se decide utilizar un servicio de respaldo y copias de seguridad en la nube, concretamente el ofertado por Amazon Web Services.

3.1.2. Identificación de los usuarios del sistema

La lista de usuarios del sistema será la siguiente:

- Administradores de servidores. Serán estos profesionales quienes tengan acceso directo a los servidores de la empresa en sí mismos. Contará con permisos sobre el contenido y aplicaciones del sistema, y se encargará de su puesta en marcha, monitorización, mantenimiento y posibles reparaciones o sustituciones.
- Administradores de bases de datos. Estos usuarios se encargarán de asegurar el funcionamiento óptimo de los sistemas de bases de datos de la empresa, pudiendo éstos acceder a sus contenidos y a las opciones de configuración y administración de las mismas.
- Administradores de redes. Serán los encargados del mantenimiento de la infraestructura de red que permite la interconexión y prestación de servicios de los diferentes equipos. Tendrán acceso físico a la infraestructura de red.

- Empleados del supermercado. Podrán tener diferentes responsabilidades en función de su puesto específico dentro de la jerarquía, pero en ningún momento podrán acceder al manejo, control, configuración o administración de servidores, bases de datos, equipos de red o demás elementos informáticos “especializados”. Su empleo de la tecnología se limitará al de los terminales de punto de venta, tablets portátiles, cerraduras inteligentes y visualización de las imágenes de las cámaras de seguridad del local.

3.2. Establecimiento de los requisitos

En este apartado se definen los requisitos mínimos desde el punto de vista del administrador de sistemas.

3.2.1. Obtención, análisis y validación de requisitos

Requisitos de implantación.

- Se debe contar con un servidor que, dada su especificación hardware, pueda ofrecer el rendimiento necesario para satisfacer las necesidades y requerimientos establecidos por la empresa. Su tamaño deberá ser de 1U.
- Las unidades de almacenamiento empleadas para el sistema de información y aplicaciones imprescindibles deben ser NVME de generación 3 o superior, mientras que las unidades de almacenamiento mecánicas para la base de datos y demás archivos deberán ser HDD de un mínimo de 2 TB.
- Las tablets usadas por los empleados deben tener un tamaño mínimo de pantalla de 9” y resolución Full HD. Adicionalmente, deben contar con un mínimo de 6 GB de RAM y 128 GB de almacenamiento. Se valorará muy positivamente la capacidad del dispositivo de poder emparejarse con lápices táctiles.
- Los dispositivos de control de acceso y horarios deben permitir la identificación por huella dactilar y códigos personalizados. Su alimentación debe ser por pilas o baterías, de manera que no dependan directamente de la corriente eléctrica y puedan funcionar en caso de falla de la misma.
- Los cables de red empleados en la instalación deberán ser de categoría 6E o superior, mientras que los puntos de acceso deben poder ofrecer velocidades Gigabit a los dispositivos conectados.
- Los puntos de acceso deben proporcionar cobertura de red inalámbrica en la totalidad del edificio.

Requisitos de rendimiento.

- Son de vital importancia el número de peticiones capaces de ser atendidas por unidad de tiempo y los tiempos de respuesta de las consultas a la base de datos. El servidor deberá ser capaz de administrar 500 peticiones/segundo, de manera que se puedan asumir los momentos picos

de compras y una eventual gestión del sistema de forma simultánea. Los tiempos de respuesta de la base de datos deben ser inferiores a 750 ms cuando se busca un elemento concreto de los disponibles en el almacén.

- El sistema debe mantener sus prestaciones y operar adecuadamente con 10.000 usuarios conectados de forma simultánea.
- El reconocimiento por huella dactilar debe realizarse de manera rápida, en menos de un segundo, y de manera fiable.
- La transferencia de los registros de control de acceso desde los terminales hasta unidades de almacenamiento externo no debe tomar más de 10 segundos.

Requisitos de seguridad.

- Se realizará una copia de seguridad en los servidores de la empresa al finalizar el horario de apertura al público del establecimiento. Esta copia de seguridad será también subida al servicio en la nube.
- La última copia de seguridad de la base de datos del negocio (inventario, contabilidad, fichaje de empleados, etc) de la semana deberá mantenerse almacenarse por un periodo de tiempo no inferior a los 18 meses.
- Las unidades de almacenamiento deben contar con mecanismos de redundancia que permitan la recuperación frente a eventuales fallos hardware. Estas unidades de almacenamiento deben poder ser reemplazadas “en caliente”.
- Los sistemas de apertura de puertas mediante identificación biométrica o código de acceso deberán contar con un retardo de varios segundos en su apertura.
- Cada entrada o salida por una puerta que requiere de autenticación debe ser registrada en un histórico en el que deben guardarse los datos del último mes. Cada usuario que ingrese debe pasar su huella dactilar o ingresar su código, aunque la puerta de acceso esté abierta.
- Los códigos de acceso serán fijos para cada empleado, de una longitud mínima de 8 dígitos, y solo deberán ser empleados tras fallar el reconocimiento biométrico. La excepción a esta norma se presenta en el punto siguiente.
- Se deberá disponer de varios códigos especiales, que de ser introducidos alertarán directamente y de forma silenciosa a la policía. Su uso se justifica en caso de atraco, extorsión o coacción de alguno de los empleados por parte de una tercera persona.
- Se debe contar con unidades de repuesto para los dispositivos que se usan en el sistema. En particular, se deberá disponer de 3 HDD de repuesto, 1 SSD, 2 sticks de memoria RAM y 1 fuente de alimentación. En caso de fallos de componentes menos propensos a errores (y de mayor costo) como procesador o placa base, se deberá pedir al fabricante, recibir e instalar en un plazo máximo de 48 horas.

Requisitos de disponibilidad.

- Se contarán con sistemas SAP para evitar la interrupción de los servicios informáticos en caso de un corte del suministro eléctrico en el local. Bajo un uso promedio de los equipos, estos deberán proporcionar 2 horas de energía.
- Los sistemas de cierre con identificación y de control de accesos utilizarán fuentes de energía como baterías o pilas, independientes de la corriente eléctrica del local.
- El sistema informático debe tener una disponibilidad del 99.99%. La duración de los fallos deberá ser inferior a los 5 minutos y los reinicios del sistema deben tomar menos de 90 segundos.

3.2.2. Especificación de casos de uso

En esta sección se especifican algunas de las situaciones que pueden ocurrir, relacionadas con el sistema informático, y a las que el administrador debe poner una solución o asegurar ciertas condiciones.

- Fallo de un elemento hardware.
 - Escenario: un componente del sistema (discos duros habitualmente) se ha roto o está causando problemas.
 - Postcondición: se reemplaza la unidad defectuosa. En el caso de una unidad de almacenamiento rota se recupera y restablece los datos que contenía el disco antiguo en el nuevo disco.
 - Interfaz: servidor dentro del armario o conjunto de racks donde se encuentra la unidad de almacenamiento que presenta el fallo.
 - Condición de fallo: no se puede reemplazar el disco (no hay repuestos) o no se puede recuperar la información contenida en el mismo.
- Copias de seguridad.
 - Escenario: se comienza a realizar la copia de seguridad de la información del sistema al terminar el horario de atención al público del establecimiento.
 - Postcondición: se realiza la copia de seguridad local y se sube dicha copia al servidor en la nube de forma exitosa.
 - Interfaz: automatizado mediante el propio sistema gestor de la base de datos y la herramienta de Amazon Web Services.
 - Condición de fallo: no se puede realizar la copia local o la subida al servidor externo falla.
- Dispositivos defectuosos.
 - Escenario: un dispositivo no funciona de forma correcta.
 - Postcondición: se sustituye por un nuevo dispositivo.
 - Interfaz: depende del dispositivo a sustituir. Puede tratarse de una cámara, cerradura inteligente, TPV o punto de acceso WiFi.
 - Condición de fallo: no existen unidades a sustituir.
- Consulta de stock.

- Escenario: el empleado realiza una consulta del stock de un producto en el almacén de la tienda.
- Precondición: el producto está registrado en la base de datos y el empleado está autenticado en el sistema.
- Postcondición: se obtiene como respuesta la información del producto consultado.
- Interfaz: las tablets de las que hacen uso los empleados.
- Condición de fallo: el empleado introduce un nombre erróneo de producto, el producto no está registrado en la base de datos o el empleado no está autenticado.
- Ataque al sistema.
 - Escenario: se detecta un uso indebido del sistema informático, una penetración en el mismo o un ataque de otro tipo (como denegación de servicio).
 - Postcondición: se debe mitigar el ataque, y de ser necesario restablecer el sistema y realizar una revisión del sistema de control de accesos.
 - Interfaz: consola de comandos o herramientas de gestión oportunas.
 - Condición de fallo: no se puede restablecer el servicio, no se puede expulsar al atacante del sistema o se sufre una filtración de información.

3.3. Migración de datos y carga inicial

Kobiran ya posee a fecha de redacción de este documento un sistema de información propio, por lo que debe realizarse un proceso de migración de dicha información ya existente al nuevo sistema, de forma que se pueda seguir actuando con las operaciones del propio sistema.

Por tanto, debemos definir un plan de migración, en el que se realice el diseño de un modelo de datos y conjunto de procesos para obtener la información del sistema actual y trasladarla al nuevo sistema que se pretende poner en funcionamiento.

Los datos existentes serán extraídos de la base de datos SQL actual gracias a herramientas de tipo “dumper”. Una vez extraídos los datos, estos serán subidos a un sistema de almacenamiento temporal en la nube, dentro del marco del proveedor Amazon Web Services. Este proceso puede ser automatizado en gran medida haciendo uso de scripts.

Tras tener la copia de los datos existentes, se debe realizar un proceso de filtrado y limpieza, pues la empresa ha decidido aprovechar este momento de cambio de sistema para revisar la base de datos.

En particular, se deberán eliminar entradas de productos ya descatalogados y actualizar algunos precios de otros productos. También, dado que la empresa quiere tener la base de datos lista para el lanzamiento de su tienda online, deberá añadirse una descripción en aquellos productos donde fuera necesario.

Este proceso puede ser automatizado siempre que se disponga de la información necesaria de antemano, la cual tendremos que preguntar a los encargados de la empresa.

El cliente quiere lanzar su tienda online, por lo que se deberán registrar nuevos datos (asociados a información personal digital de los clientes), por lo que se debe realizar una ampliación del modelo de datos.

Gran parte de la información se va a tomar del sistema de tarjetas de fidelización ya existente en las tiendas físicas, siendo la información que falta el correo electrónico, teléfono personal, una contraseña y la conformidad para recibir ofertas vía email.

Por tanto, y aunque la tarea no es trivial, se prevé afrontar esta fase de forma sencilla dado que el modelo inicial de datos está probado por la empresa, y la adición de la nueva información no es una tarea compleja ni requiere de una modificación radical de las estructuras existentes.

Respecto del registro del horario de los trabajadores se deberá realizar un cambio en parte del modelo de datos, de manera que en lugar de almacenarse el código de barras de la tarjeta que se utiliza actualmente se pasee a emplear la huella dactilar. El resto de la información ya existente no debe ser modificada y puede ser extraída mediante los scripts anteriormente mencionados fácilmente.

Tras haber extraído y procesado la información, y estando el nuevo sistema implantado, se realizará una recuperación de las bases de datos a partir de la copia almacenada en la nube.

3.4. Elaboración del modelo de procesos

3.4.1. Características de los modelos de procesos del sistema

Los modelos con los que cuenta el sistema y sus características son los que se describen en los puntos siguientes:

- 1. Fichaje de los empleados.
 - Frecuencia de ejecución: unas 40 peticiones por minuto (para el total de los supermercados)
 - Procesos asociados: control de acceso, administración de tareas, fichaje de los empleados, generador de reportes de fichajes, control de ventas en caja.

- Restricciones de ejecución:
 - Tiempo de ejecución de 500 ms.
 - Máximo de 50 usuarios concurrentes (entre todos los supermercados).
 - Periodo crítico al inicio y término de la jornada laboral.
- 2. Autenticación por huella dactilar.
 - Frecuencia de ejecución: 20 peticiones por minuto (para el total de los supermercados).
 - Procesos asociados: control de acceso, gestión de almacén.
 - Restricciones de ejecución:
 - Tiempo de ejecución máximo de 1 segundo.
 - Se prevé un máximo de 30 usuarios concurrentes.
 - Periodo crítico: al inicio de la jornada laboral (antes de la apertura de la tienda, en la que se da entrada a los nuevos productos al almacén) y en periodos de especial afluencia de gente (como días previos a festividades).
- 3. Generador de reportes de fichaje:
 - Frecuencia de ejecución: 1 vez al día en cada establecimiento al término de la jornada laboral.
 - Procesos asociados: fichaje de los empleados.
 - Debe ejecutarse en menos de 5 minutos.
- 4. Registro de cliente en el sistema.
 - Frecuencia de ejecución: 300 peticiones/min
 - Procesos asociados: control de acceso de clientes, administración de usuarios.
 - Restricciones de ejecución:
 - Tiempo máximo de respuesta de 500 ms.
 - 40 usuarios concurrentes como máximo.
 - Se establece como periodo crítico días laborales en su totalidad y franjas horarias en las que las tiendas físicas están cerradas.
- 5. Autenticación de cliente en el sistema.
 - Frecuencia de ejecución: 400 peticiones/min
 - Procesos asociados: registro de usuarios, administración de usuarios, control de acceso de clientes.
 - Restricciones de ejecución:
 - Tiempo máximo de respuesta de 300 ms.
 - 60 usuarios concurrentes como máximo.
 - Se establece como periodo crítico días laborales en su totalidad y franjas horarias en las que las tiendas físicas están cerradas.
 - Se debe mantener la sesión abierta un máximo de 30 días.
- 6. Registro de un pedido por parte de un cliente.
 - Frecuencia de ejecución: 150 peticiones a la hora.
 - Procesos asociados: autenticación de cliente en el sistema.
 - Restricciones de ejecución:

- Tiempo máximo de respuesta de 500 ms.
- 60 usuarios concurrentes como máximo.
- El proceso es altamente crítico.
- Se espera una mayor demanda al término de la jornada laboral, en días no laborables y la víspera de los mismos.

3.4.2. Localización geográfica de la matriz de procesos

Los servidores que conforman el sistema informático, almacenan los datos necesarios y proporcionan servicio a la cadena de supermercados, se encuentran en la segunda planta del supermercado de mayor tamaño de la capital, ubicado en calle Camino de Ronda.

3.5. Especificación del plan de pruebas

En este apartado se definen las pruebas del sistema en las que se involucra al administrador de sistemas. Este plan consta de 3 fases, definición del alcance de las pruebas, especificación de requisitos del entorno de pruebas y extracción de las pruebas de aceptación para el sistema.

3.5.1. Alcance de las pruebas

En un primer momento se deberán definir las diferentes áreas que deben cubrir las pruebas del sistema. Concretamente, estas serán el entorno tecnológico del sistema de información a implementar, la implantación del sistema en sí mismo, la seguridad en su conjunto y el rendimiento global del sistema.

Para validar y verificar las diferentes secciones del sistema, las diferentes áreas de negocio de la organización requerirán de nuestra supervisión como administradores del sistema.

Así pues, el entorno de pruebas, los requisitos a satisfacer, herramientas a utilizar y personal de la empresa deberán encontrarse debidamente preparados antes de llegar a la fase de construcción del sistema. De esta manera, se podrán realizar las pruebas que sean necesarias y oportunas para garantizar el correcto funcionamiento del sistema a implantar.

3.5.2. Requisitos del entorno de pruebas

A continuación se listan los requisitos que se deberán satisfacer:

- Se debe disponer de acceso a Internet mediante una red inalámbrica de alta velocidad y mediante red cableada.

- Se debe disponer de un dispositivo móvil con control de acceso por huella dactilar y otro dispositivo con pantalla táctil. Puede ser el mismo en ambos casos si satisface ambos requisitos.
- Se debe disponer de un ordenador portátil con sistema operativo Windows 11, con las debidas herramientas de gestión y monitorización instaladas, así como con el sistema gestor de bases de datos instalado y totalmente configurado.
- Se debe disponer de un servidor para alojar las aplicaciones del sistema informático a implantar. Así pues, debe contar con los siguientes elementos software:
 - Mismo sistema operativo que el servidor de producción, Ubuntu Server 22.04.
 - Gestor de bases de datos compatible con la tecnología usada por la organización, e idealmente el mismo.
 - Configuración de seguridad necesaria.
- La base de datos debe contener instancias de prueba suficientes para asegurar el correcto funcionamiento de todas las operaciones a las que se someterá el sistema en producción. Las instancias deben conformar un conjunto de datos lo más verosímil y real posible.
- Los dispositivos deben tener instalados los drivers necesarios para el correcto funcionamiento de los periféricos que deben ser conectados. Para el caso de los TPV se necesitará la pantalla táctil y lector de códigos de barras; para el caso de los portátiles se necesitará de teclado, ratón, impresoras y dispositivos de almacenamiento externo; las tablets no tendrán conectados ningún periférico.

3.5.3. Pruebas de aceptación del sistema

En esta sección se detallan las pruebas que deberán pasarse para dar el visto bueno al sistema. Esta batería de pruebas se define mediante un acuerdo con la organización que emplea el sistema, en este caso, Kobiran.

- Se debe realizar una identificación del personal en las diferentes áreas del sistema (TPV, almacén, terminal de fichaje, p.e) que requieran de autenticación (mediante huella dactilar o código personal).
- Se controla el acceso a las diferentes áreas del sistema mediante un sistema de permisos y realiza un seguimiento de qué usuario accedió a qué área en qué momento.
- Los diferentes equipos informáticos portátiles, terminales de punto de venta, cámaras y demás elementos se encuentran conectados sin problemas a la red global del sistema de información (mediante conexión inalámbrica o cableada, según cada caso).
- No se producen colapsos ni retrasos en los identificadores dactilares, que funcionarán con el nivel de precisión acordado.

- El sistema de fichaje genera los registros de forma automática al término de la jornada laboral en el tiempo acordado.
- Las copias de seguridad se realizan de forma automática al finalizar la jornada laboral y se suben posteriormente al proveedor en la nube (AWS) con la mayor celeridad posible.
- Todos los sistemas se encuentran operativos y proporcionan el nivel de rendimiento prometido y acordado.
- Se ha realizado el mantenimiento y ampliación de la base de datos acordada.
- El sitio web de la tienda se encuentra operativo, con el diseño acordado de antemano, de manera que la visualización correcta de los datos y el proceso de realización de una compra no implique un aprendizaje extra por parte del cliente ni este diste mucho de lo “estandarizado” por el resto de sitios web.

4. Diseño del Sistema de Información (DSI)

El objetivo de esta fase es definir la arquitectura del sistema y del entorno tecnológico que va a usar. Se deben generar todas las especificaciones de construcción, especificación del plan de pruebas, requisitos de implantación, diseño de procedimientos de migración y carga inicial (estos últimos siempre que proceda).

4.1. Requisitos de diseño y construcción

Se dividen a continuación los diferentes requisitos según los departamentos a las que estos afectan:

4.1.1 Módulos del sistema

Administración de servidores:

- El sistema incluirá un módulo para la administración y supervisión de los servidores de la empresa.
- Monitoreo del rendimiento
- Gestión de recursos
- Generación de informes y la gestión de incidencias.

Gestión de empleados:

- Gestionar la información de los empleados, que incluirá datos personales, información laboral, horarios, salarios y registro de asistencia.

Gestión de inventarios:

- El sistema contará con un módulo de gestión de inventarios que permita el seguimiento y control de los productos almacenados.
- Se registran las entradas, salidas y movimientos de inventario, así como las fechas de vencimiento y otros detalles relevantes.
- Se utilizarán técnicas de identificación, como códigos de barra, para facilitar la gestión y seguimientos de los productos.

Administración del parking:

- El sistema incluirá un módulo para gestionar el parking que permitirá el registro de vehículos, control de acceso y asignación de espacios de estacionamiento.

Finanzas y contabilidad

- Debe estar disponible durante las 24 horas.
- Acceso restringido a los administradores y responsables de los departamentos.

- Se deben registrar todos los accesos que se hacen al sistema.
- El tiempo de respuesta debe ser inferior a 2 segundos.

Ventas

- Debe estar disponible durante las 24 horas.
- El sistema debe registrar el número de ventas diarias.
- El sistema debe generar un reporte de todas las ventas diarias, semanales, mensuales y anuales.
- El sistema debe notificar a los administradores los reportes generados.

Compras:

- Debe estar disponible durante 24 horas.
- El sistema debe registrar el número de compras diarias.
- Cada registro de compra tiene que tener una factura asociada con un proveedor registrado.
- Cada compra tiene que estar aprobada.

Almacenamiento:

- Debe estar disponible durante 24 horas.
- El sistema debe llevar un registro de todos los productos.
- El sistema debe proporcionar información de todos los productos.
- Debe registrar todos los accesos que se hacen a los productos.
- El tiempo de respuesta debe ser inferior a 1 segundo.

4.1.2 Servidores de datos y de aplicaciones

En esta sección se va a implementar la Base de datos del sistema donde se involucrará a los administradores de Bases de datos y Administradores de software.

Se almacenará en la base de datos:

- Clientes.
- Proveedores.
- Estados de los diferentes productos.
- Cantidad de los diferentes productos.
- Información de los empleados.
- Control de acceso de los empleados.
- Registro de los vehículos en el parking.

4.1.3. Conectividad en conexiones y red

Conectividad y redes:

- La velocidad de subida y bajada debe ser simétrica y de mínimo 300Mbps

- La velocidad de transferencia de archivos entre dispositivos físicos debe ser mínimo 10Mbps.
- La comunicación con los servidores deberá ser encriptada
- Se configurará un cortafuegos para las comunicaciones entre redes locales y permitir el acceso sólo a dispositivos autorizados.

Dispositivos:

- El tiempo de encendido/reinicio del dispositivo debe ser inferior a 1 minuto.
- Los dispositivos solo podrán conectarse a una red local.
- Los dispositivos estarán configurados para no permitir el acceso a determinadas páginas webs.
- La memoria RAM mínima debe ser de 8GB.
- La tasa de refresco debe ser igual o superior a 60Hz.
- Los dispositivos deberán monitorizar la información de todos sus accesos.

Lectores de huella digital y de tarjetas:

- El tiempo que tardan los lectores en identificar a los usuarios debe ser inferior a 1 segundo.
- Se deberán registrar todos los intentos de accesos que se hacen al lector, tanto los accesos con éxito como los accesos fallidos.
- Los lectores deberán proporcionar una señal visual o acústica como forma de retroalimentación a los usuarios.

4.2. Especificación del entorno tecnológico

Se agrupan los elementos de la infraestructura en hardware, software y comunicaciones.

4.2.1. Hardware

Servidores:

- Chasis [ThinkSystem SR645 V3](#), con instalación de dos procesadores AMD EPYC de 4º generación, con una capacidad de 512 GB de RAM en 8 sticks de 64GB cada uno, pudiendo escalar estos de ser necesarios en el resto de ranuras (1.5 TB en total si se siguen empleando sticks de 64GB cada uno).

Almacenamiento:

- Unidades de estado sólido de alta velocidad de 1 TB de la marca SABRENT y 3 unidades de almacenamiento de formato 3.5" y 4 TB de capacidad cada una de la marca Seagate.

Dispositivos para la gestión de inventarios y para los empleados:

- Tablets [Lenovo Tab P11 Pro de 2º generación](#).

- Portatil [LG Gram modelo 14Z90Q](#).

Gestión de empleados:

- Para la identificación de los empleados y realizar el control de los horarios de entrada y salida del personal se va usar el terminal Aktivstar.

Red e internet

- Conectores RJ-45.
- Switches CISCO modelo CBS220-24T-4G.
- Puntos de acceso WiFi Ubiquiti U6-LR.

Seguridad:

- Cámaras de seguridad IP.
- Detectores de presencia a lo largo del supermercado.
- Cerraduras de las áreas restringidas se decide utilizar el modelo Smart Door Lock M20 de Xiaomi.

4.2.2. Software

- Se usará Windows 11 como sistema operativo para los usuarios finales.
- Microsoft Office 365 como herramienta de ofimática.
- Microsoft SQL Server como servidores.
- Microsoft SQL Server Management Studio herramienta de gestión de los servidores.
- Java 11 lenguaje de programación.
- Junit, Mockito y Selenium (testing) herramienta de testeo.
- IntelliJ Idea editor de código.
- Jira software gestión del proyecto
- Git control de versión.
- Docker

4.2.3. Comunicaciones

- Para las comunicaciones realizadas a través de los equipos para los empleados (capa de presentación) se utilizará el protocolo HTTPS a través del puerto 443.
- Para las comunicaciones realizadas entre los servidores internos se usará el protocolo HTTP a través del puerto 80.
- Para las comunicaciones con la base de datos se usará el protocolo TCP/IP y el puerto 27017.

4.3. Requisitos de operación y seguridad

En cuanto al acceso al sistema y a sus recursos el sistema controlará el acceso y solamente se permitirá a usuarios autorizados. Los grupos de usuarios y sus privilegios se dividen de acuerdo a las funciones que desempeñan y son los siguientes:

Administrador:

- Los usuarios pertenecientes a este grupo podrán acceder a todos los servidores y aplicaciones del sistema con permisos de lectura y escritura.
- Los permisos de los distintos grupos sólo podrán ser cambiados por el administrador.

Desarrollador:

- Los usuarios pertenecientes a este grupo podrán acceder al servidor de la base de datos con permisos de lectura y escritura, a todo el código implementado con permisos de lectura y escritura, y al resto de servidores y aplicaciones con permisos de lectura.

Jefes:

- Los usuarios pertenecientes a este grupo podrán acceder a Jira con permisos de lectura y escritura para asignar las distintas tareas a los empleados. También tendrán acceso de lectura a la base de datos. No tienen acceso a los servidores y aplicaciones propias de los administradores y desarrolladores.

Empleados:

- Los usuarios pertenecientes a este grupo tendrán acceso a los datos de la base de datos con permiso de lectura. También tendrán permisos de lectura en Jira para comprobar las tareas que les son asignadas, teniendo permisos de escritura en aquellas tareas que les hayan sido asignadas. No tienen acceso a los servidores y aplicaciones propias de los administradores y desarrolladores.

El acceso a recursos físicos se realizan a través del lector de huella digital o DNI.

Se configurarán protocolos de bloqueos de acceso a aquellos recursos hardware y software que hayan tenido varios intentos de acceso fallidos.

Se aplicará una autenticación de 2 factores.

Los permisos de acceso podrán ser cambiados solamente por el administrador del sistema.

4.4. Distribución de los datos

Todos los dispositivos de almacenamiento locales se ubicarán en el centro de datos, ubicado en Granada en el edificio central.

La base de datos se situará en los servidores que proporciona Microsoft SQL Server.

Los servidores que proporcionan AWS Backup estarán ubicados en sus propias ubicaciones, con lo cual no habrá que preocuparse de situar físicamente dichos servidores.

El esquema físico de los datos estará compuesto por diferentes tablas almacenados en el servidor de base de datos con la siguiente estructura:

Empleado

```
CREATE TABLE Empleado (  
  IdEmpleado INT PRIMARY KEY,  
  Nombre VARCHAR(100),  
  Apellido VARCHAR(100),  
  Puesto VARCHAR(100),  
  Salario DECIMAL(10, 2),  
  FechaContrato DATE  
);
```

Producto

```
CREATE TABLE Producto (  
  IdProducto INT PRIMARY KEY,  
  Nombre VARCHAR(100),  
  Precio DECIMAL(10, 2),  
  Stock INT,,  
  FechaVencimiento DATE,  
  IdProveedor INT,  
  FOREIGN KEY (IdProveedor) REFERENCES Proveedor(IdProveedor)  
);
```

Proveedor

```
CREATE TABLE Proveedor (  
  IdProveedor INT PRIMARY KEY,  
  Nombre VARCHAR(100),  
  Direccion VARCHAR(100),  
  Telefono VARCHAR(100),  
);
```

4.5. Entorno de pruebas

En este apartado se comentan las siguientes pruebas a realizar en el sistema de información a implantar:

Pruebas unitarias

- Hardware: Réplica del entorno de construcción.
- Software: Instalación, preparación y ajuste de las bibliotecas de testeo utilizadas. Seguimiento de los tests al sistema de gestión de versiones y empleo de un sistema de integración continua, en este caso Selenium.
- Almacenamiento: Réplica del entorno de construcción. No se esperan cambios.
- Accesos: Únicamente los desarrolladores pueden acceder al código y tests desarrollados.
- Integridad datos: Los datos de prueba no contienen información real y pueden ser adaptados, siendo accesibles por los desarrolladores y administradores.
- Recuperación: Uso de AWS backup para mantener una copia de seguridad de los datos y las pruebas realizadas.

Pruebas de implantación del sistema

- Hardware: Se instala el sistema completo en el entorno tecnológico.
- Software: Instalación, preparación y ajuste de las bibliotecas de testeo utilizadas para las pruebas de seguridad, rendimiento, recuperación e integridad entre otras.
- Comunicaciones: Configuración de acceso a los servidores de aplicaciones para que los desarrolladores accedan al sistema.
- Información: Se emplearán datos definidos para este fin, y explicados mediante una leve formación para su correcto uso.
- Almacenamiento: Se establece una conexión de red que aumentará su demanda con mayor tráfico de datos en el sistema. Por otro lado, el almacenamiento reducirá con la inserción de nuevos datos.
- Requisitos: Se aplican los definidos en las pruebas unitarias y previamente.

Pruebas de aceptación

- Hardware: Se aplican las mismas pruebas definidas previamente.
- Software: Se desarrollan las pruebas de aceptación definidas previamente y especificadas mediante casos de uso. Se repiten los procedimientos previos para la instalación de librerías.
- Comunicaciones: Se aplican las mismas pruebas definidas previamente.
- Información: Se aplica el mismo conjunto de pruebas previo, con posibilidad de inserción de algún caso particular.
- Requisitos: Se aplican los mismos requisitos que en pruebas anteriores.

4.6. Requisitos de implantación

Para la implantación es necesario definir una serie de requisitos que se lleven a cabo para la documentación del sistema implantado y la comprensión del mismo. Estos requisitos por lo tanto se encuentran orientados a los usuarios finales. Por

otro lado también se definen los requisitos asociados a la implantación del sistema en la organización.

A continuación se describen los requisitos:

Requisitos de documentación:

- Se deben proporcionar una serie de documentos que ofrezcan la visión general del sistema de información.
- Se deben seguir los estándares de documentación propios de la organización (Sprinter).
- Se deben distinguir manuales de uso, de instalación y de operación del sistema de información.
- La documentación se encuentra almacenada en un repositorio privado y distribuido según departamentos, de forma que solo puedan acceder a los manuales correspondientes los miembros de los diferentes departamentos.

Requisitos de formación de personal:

- Se deben establecer una serie de sesiones de formación del personal relativas al departamento correspondiente de los diferentes conjuntos de empleados.
- Se deben realizar sesiones de forma práctica durante las dos primeras semanas de integración en la empresa (o tras la implantación del sistema) de forma que se aprenda a realizar las diferentes tareas asociadas al empleado según su puesto y permisos.
- Durante el primer mes se debe formar a los encargados de creación, inserción o modificación de tareas (responsables) de forma intensiva con el fin de que se familiaricen y posean una visión global del sistema.

Requisitos de infraestructura:

- Se deben instalar los dispositivos lectores de identificación mediante dispositivo móvil del empleado para garantizar sus accesos a las instalaciones o subsistemas.
- Se debe además configurar los diferentes accesos y sistemas de control y gestión de horarios de los empleados, tanto a su puesto de trabajo como a las áreas a las que se encuentra autorizado.

5. Construcción del Sistema de Información (CSI)

5.1. Preparación del entorno de generación y construcción

Para comenzar con esta tarea tenemos que asegurarnos y preparar los puestos de trabajo, los equipos físicos y los lógicos, los gestores de bases de datos, herramientas de generación de código, bibliotecas de software, ficheros necesarios, etc. En definitiva, hay que preparar el entorno que nos permita construir el sistema de información.

Primero comenzaremos hablando de lo referente a la base de datos. Para levantar todo lo referente a la persistencia de los datos del sistema estableceremos cuáles son las entidades básicas que manejaremos, las cuales son:

- Datos de empleados
- Datos de productos
- Horarios de trabajo
- Logs y registros de acceso

Debido a la naturaleza de la solución que se propone, se ha establecido que el empleo de una base de datos SQL con SQL Server es lo más apropiado. En cada supermercado de la cadena de la empresa existirá un servidor local que será capaz de conectarse a su vez con cada uno de los demás servidores, de manera que habrá una red distribuida de servidores en lo que a la persistencia se refiere. Cada uno de estos servidores contará con 10 terabytes de almacenamiento. En caso de falta de espacio o desbordamiento, esta cantidad se podrá ampliar fácilmente cambiando el disco duro por uno de mayor tamaño.

En segundo lugar, será necesario preparar el entorno para construir los componentes del sistema a desarrollar como tal. Para ello será necesario establecer elementos como las bibliotecas o librerías que se van a utilizar, las herramientas (generadores de código, editores, compiladores, IDEs, etc.) o los puestos de trabajo que se van a establecer durante la construcción.

Para el desarrollo de este sistema se hará una división de equipos tres equipos, de manera que todos los desarrolladores estén compensados en estos equipos, con la posibilidad excepcional de ayuda entre ellos en caso de complicarse alguna tarea y sin buscar que nadie se especialice en nada, pues eso podría suponer un problema en caso de que alguien abandone la empresa y al equipo.

Todo el proyecto se gestionará empleando la plataforma de Jira y todas las facilidades que ofrece para gestionar el software. Los servidores a levantar se van a gestionar con Jenkins para poder mantener de manera sencilla y óptima las últimas

versiones de los códigos que se encuentren en desarrollo. Y todo estará enmarcado dentro de una VPN propia de la empresa para que solo se pueda acceder a los códigos y entornos de trabajo por medio de unas credenciales válidas que proporcionará la empresa.

Se establece que se va a programar empleando el lenguaje de Java 8 siguiendo una estructura de microservicios que se construirán por medio de Maven, de manera que cada Microservicio sea un proyecto Maven, que gestiona la construcción de proyectos.

La siguiente lista muestra diferentes herramientas que serán utilizadas para la construcción:

- Microsoft Office 365
- Microsoft SQL Server
- Microsoft SQL Server Management Studio
- Java 11
- Junit, Mockito y Selenium (testing)
- IntelliJ Idea
- Jira software
- Git
- Docker

Con esto queda preparado el entorno para la construcción del sistema.

5.2. Generación del código de los componentes y procedimientos

Durante esta tarea se va a generar aquellos procedimientos de operación y administración del sistema a desarrollar. Además, también se van a generar los procedimientos de seguridad y control de acceso, los cuales son necesarios para poder ejecutar el sistema cuando por fin se haya implementado y esté en la fase de producción.

Para garantizar la seguridad del trabajo, los empleados/desarrolladores deberán seguir esta serie de procedimientos:

- Tener instalado y configurado la VPN que dará acceso a todos los entornos que ofrece la empresa para poder desarrollar y probar todos los diferentes componentes que se generen.
- Tener instalado y configurado el antivirus de Microsoft. Es nativo de windows y evita la necesidad de tener que instalar otros antivirus que ocupan espacio. Esto va a evitar vulnerabilidades a la hora de realizar conexiones con otras redes o descargas con virus.

- Realizar de manera constante las operaciones de Git de manera que se pueda seguir de la manera más aproximada posible el flujo de trabajo conocido como Git Flow.
- Levantar todos los contenedores docker necesarios en local para poder realizar programar en los equipos locales y no consumir los diferentes recursos y servidores que se utilizarán para el entorno de producción o de desarrollo.

5.3. Ejecución de las pruebas unitarias

Para esta tarea, será necesario el agrupamiento de todos los recursos para poder realizar las pruebas unitarias, en especial de los componentes que se hayan realizado en la parte backend de los servicios desarrollados. Para asegurarnos de que el proyecto cumple unos estándares de calidad, deberá ser necesario probar todos los servicios construidos con una cobertura no menor que un 80%, de manera que la mayor parte del código quede asegurada.

Se creará una base de datos especialmente para el entorno de testing que se empezará en este punto del desarrollo, de manera que se pueda dar persistencia a los datos con los que se hayan realizado las pruebas y que no se modifique en nada la base de datos del entorno de desarrollo.

Los empleados que hayan desarrollado un servicio, idealmente no lo probarán, sino que otro equipo de desarrollo será el encargado de probar el código. Para las pruebas se utilizarán las librerías de Junit 5 y Mockito dentro del contexto de Java y Maven. Si algo no puede ser probado mediante pruebas unitarias, deberá quedar registrado en algún tipo de documentación para notificar al resto de los equipos de trabajo.

5.4. Ejecución de las pruebas de integración

De manera muy similar al punto anterior sobre las pruebas unitarias, los equipos de trabajo se van a encargar de realizar las pruebas de integración en las que se comprobará que todos los elementos unitarios funcionan juntos correctamente probandolos como un todo. Una vez más, los test se llevarán a cabo con la librería de Junit 5 y con Selenium.

Estas pruebas son mucho más complicadas que las unitarias, de manera que los equipos de trabajo que se encarguen de esta tarea si será necesario que estén un poco especializados en la tarea. Por otro lado, necesitarán el apoyo de los desarrolladores que han construido los módulos y los servicios del sistema para que

el equipo de testing pueda aprender como funciona y como se espera que funcione todo en su conjunto.

5.5. Elaboración de los manuales de usuario

En esta tarea se persigue la elaboración y redacción de todos aquellos materiales de documentación que puedan asesorar y guiar a los usuarios finales en cuanto al uso correcto y explotación del sistema desarrollado de acuerdo con los requisitos que han guiado el diseño y construcción del sistema.

Los manuales de usuario que se van a redactar serán los siguientes:

- Aplicación de gestión del almacén
- Aplicación de control de horarios
- Aplicación de control de fichajes
- Aplicación de gestión del parking

5.6. Definición de la formación de usuarios finales

A continuación, debe definirse cuáles son las necesidades en cuanto a la formación que necesitarán los usuarios finales con el propósito de poder sacarle el máximo provecho al nuevo sistema que se ha construido.

Para estos procesos de formación se contará, como es obvio, con los usuarios finales del sistema y, en concreto, de las aplicaciones a utilizar. Por otro lado, también será conveniente la presencia de las personas encargadas del departamento de Recursos Humanos y también de los propios encargados de gestionar estos cursos de formación en el sistema. Parte de estos formadores serán desarrolladores del sistema, pues nadie mejor que ellos conoce el funcionamiento del sistema.

De esta manera, se definirán una serie de cursos que emplearán como guía los manuales de usuario que se han elaborado en el apartado anterior, y, de esta forma, se comenzará con la impartición de los cursos. Se estima que la formación durará aproximadamente 3 semanas y que se utilizará para ello parte del horario laboral de los trabajadores para no provocar muchos inconvenientes. De todas formas, sería conveniente que por su cuenta lean los manuales para avanzar en el trabajo.

5.7. Construcción de los componentes y procedimientos de migración y carga inicial de datos

En lo que a la migración de los datos iniciales se refiere, se va a establecer un entorno de reserva al que se podrá acceder en caso de cambiar la localización física de los datos en cualquiera de los diferentes servidores que se tengan para la persistencia de los datos. Para facilitar esta gestión se van a preparar una serie de herramientas y programas que puedan automatizar tanto el despliegue de las bases de datos en los servidores locales como en las que están distribuidas en la nube. Para esto se utilizará un proveedor cloud que será Amazon Web Services. También se van a preparar aquellos scripts que sean necesarios para este cometido de migración. Se va a establecer un fichero tanto para migrar de Transact SQL a MongoDB como a MySQL, que, aunque ambos están bajo el motor de SQL, tienen sus diferencias.

Los scripts se guardarán de manera segura en los repositorios de la empresa a los que se puede acceder a través de la conexión en la VPN, de manera que solo los trabajadores tendrán acceso a esta información de migración.

La información que es más vital a la hora de hacer la migración será la de los empleados, clientes y la de los productos que están almacenados, de manera que solo será necesario crear dichas entidades con sus correspondientes atributos, que son los siguientes:

- Empleado: Nombre, apellidos, fecha de alta, dni, horario, cargo
- Cliente: Nombre, apellidos, DNI, número de tarjeta, email, hash de la contraseña, conformidad con el envío de publicidad.
- Producto: Id, nombre, descripción, tipo, stock, fecha caducidad, marca

5.8. Aprobación del sistema de información

Llegados a este punto del proceso, lo que se debe realizar es agrupar el conjunto de todos los productos realizados con anterioridad y presentarlos ante el comité de seguimiento y el jefe del proyecto para que estos puedan proceder a su aprobación.

Es esta validación del trabajo realizado la que nos permitirá poder seguir con el desarrollo del sistema de información. En caso de no tener una aprobación, deberíamos rehacer aquello que no convenza al comité.

6. Implantación y Aceptación del Sistema (IAS)

En esta sección se detallarán las tareas previas a realizar al inicio de la fase de producción del sistema de información.

6.1. Establecimiento del plan de implantación

Se identifican los distintos submódulos, analizando posibles dependencias con otros proyectos, que puedan influir en el plan de implantación. Se formará el Equipo de Implantación, acotando los recursos humanos requeridos junto a sus diferentes habilidades y rango de responsabilidad. Conviene contar con representación de todos los escalafones de la empresa, con personalidades variadas.

6.1.1. Definición del plan de implantación

El plan de implantación estará compuesto por las tareas que se listan a continuación:

- Se adiestrará a los miembros de los equipos que conformen la organización, para que sepan cual es su tarea durante la implantación del sistema.
- Una vez que se han planteado los cambios que se deben realizar, se preparará la infraestructura necesaria para poder llevar a cabo dichos cambios.
- Se instalarán los componentes y se realizará la carga inicial de la base de datos de prueba. Los datos de la fase de producción se importarán/generarán una vez que el sistema haya entrado en funcionamiento.
- Se generará el plan de mantenimiento asociado al sistema de información.

Puede ser posible que se necesite de ayuda de miembros de diferentes equipos (presumiblemente relaciones humanas) para informar a los demás sobre qué aspectos de su entorno deberán tener en cuenta para la correcta implantación del sistema.

6.1.2. Especificación del equipo de implantación

El equipo responsable de llevar a cabo la implantación del sistema estará compuesto por el siguiente personal:

- Responsables del CPD. En particular, estos serán el administrador de redes, el administrador de los servidores y el administrador de la base de datos. Serán estos quienes tengan permiso para poder acceder físicamente al CPD en sí mismo.
- Desarrolladores del software. Estos informarán a los administradores responsables del CPD sobre la instalación de herramientas, procesos o

rutinas a realizar para cada submódulo del sistema, necesidades de consumo respecto de los recursos hardware y/o de red, etc.

- Técnicos encargados del mantenimiento. Deberán tener un conocimiento general del sistema y sus componentes para poder preparar acciones a la hora de realizar el mantenimiento del sistema.
- Personal encargado de realizar las pruebas necesarias y oportunas antes de pasar a producción.

6.2. Formación necesaria para la implantación

Los administradores serán formados para la realización de los cambios en el CPD, ya que será necesario para su trabajo en la organización. Se detalla qué componentes se mantienen y cuales son sustituidos por otros nuevos. Se añadirá un nuevo rack al armario del CPD para los servidores de aplicaciones web (de la tienda online), mientras que se sustituirán los racks destinados a la administración de tareas, gestión de horarios y demás tareas burocráticas, así como aquellos destinados a la base de datos. El administrador de servidores será el encargado de esta instalación y su configuración. También tendrán que estimar meticulosamente los recursos a consumir por las aplicaciones para que una vez en producción se adapten a las necesidades de cada uno de los procesos y por tanto, pueda ser el sistema más eficiente, robusto y escalable.

El administrador de redes deberá conocer la arquitectura y topología de la red, planteada para dar servicio a un determinado número de diferentes dispositivos, cada uno de ellos con sus requisitos particulares. Tendrá que conocer qué dispositivos actúan en cada módulo, y en qué lugares deberá realizarse la instalación de red (de diferir con la actual). Estudiará qué componentes y técnicas utilizar para asegurar una red robusta, fiable y fácilmente escalable.

El administrador de base de datos deberá conocer la base de datos anterior, los ficheros que se generaron durante la migración y que serán usados en la carga inicial del sistema. Además, deberá ser conocedor y tener soltura con las herramientas necesarias para el despliegue de la “nueva” base de datos, de que tipo es y características concretas en función de la versión, etc. Esto aplica tanto a la base de datos de producción como a la de pruebas y/o desarrollo.

Además, el conjunto de los administradores tendrán que revisar toda la documentación generada por los desarrolladores. Esto se hace por si fuera necesario tener una reunión con estos para aclarar todas las dudas y sincronizar las ideas relativas al uso de los productos.

Los técnicos encargados del mantenimiento deberán conocer el sistema en su conjunto y las tareas que realiza cada dispositivo. Deberá examinar los procesos de

cada aplicación, para ser capaz de detectar incidentes que provocan anomalías, notificarlos e intentar resolverlos. Su trabajo en la etapa de implantación es comprender el sistema en su conjunto, antes de que comience su trabajo de mantenimiento en sí mismo.

6.3. Incorporación del sistema al entorno de operación.

Para la preparación del entorno se deberá disponer de los dispositivos de control de acceso mediante huellas dactilares, para que los usuarios que los vayan a usar registren sus huellas, códigos personales y se disponga de la información necesaria a posteriori.

Los TPV serán actualizados con el nuevo software y los drivers necesarios para comunicarse con los lectores de códigos de barras, impresoras de tickets, etc.

Será también necesario obtener las licencias software necesarias para los programas que serán instalados, así como para el sistema gestor de la base de datos.

Se deberá instalar Windows 11 en los ordenadores y asegurarse de que las tablets tengan la versión del sistema operativo Android compatible más reciente (Android 13 a fecha de redacción de este documento). Tanto en los ordenadores como en los dispositivos móviles deberán quedar registrados los distintos tipos de usuarios (recogidos en los requisitos de operación y seguridad), incorporando las debidas restricciones de acceso a las herramientas instaladas.

Para poder realizar las copias de seguridad en la nube, deberá configurarse el perfil de usuario de AWS correcto con la frecuencia de realización de los “backups”. También es importante configurar las conexiones de red con los routers, permitiendo el acceso a internet desde todos los dispositivos, tanto móviles como ordenadores.

6.4. Carga de datos al entorno de operación.

Se deberá realizar una migración de datos desde la base de datos que tuviera el antiguo sistema de Kobiran, pasando por la nube, hasta el nuevo sistema. Se mantiene el mismo tipo de base de datos, basada en Oracle SQL.

La migración de datos será parcial, en tanto que se realiza un proceso de limpieza de entradas obsoletas e inútiles. Sin embargo, también es un proceso de ampliación, en tanto que se deben rellenar algunos campos nuevos que tendrá la base de datos a implantar.

Se proporcionará una cantidad suficiente de datos para poder realizar correctamente todas las pruebas. También se deberán proporcionar nuevos datos de prueba en aquellas columnas de las tablas existentes, y colecciones nuevas de

la base de datos, que se hayan incorporado en los requisitos y que no se contemplaban en la base de datos anterior.

6.5. Pruebas de implantación del sistema

6.5.1. Preparación de las pruebas

Para la preparación de las pruebas se deberá generar el entorno de trabajo utilizado por los desarrolladores. Esto se hará en las plataformas de integración continua CircleCI y Semaphore CI.

Gracias a estas herramientas y a su entrega continua se podrán obtener de forma rápida y automática las herramientas necesarias para la realización de las pruebas de implantación.

6.5.2. Realización de las pruebas

Preparado el entorno de pruebas, se procede a la realización de las mismas. Estas deberán ser realizadas por el equipo que ya se había concretado, formado por personas con un perfil profesional determinado, expertas en este ámbito. Se deberán realizar todas las pruebas que ya estaban planeadas, como aquellas que hayan podido surgir a posteriori.

Se hace uso de las dos plataformas mencionadas anteriormente bajo la premisa de que cada una de ellas ejecutará una parte del conjunto de pruebas, paralelizando y agilizando el proceso de testeo en su conjunto.

Realizadas las pruebas, se proporcionará una plantilla a cada una de las personas encargadas de la realización de las pruebas. En dicha plantilla, se tendrá un campo de observaciones para cada una de las pruebas, en el que se deberá indicar los posibles problemas que hayan podido surgir y cuya solución no se ha hallado durante la prueba en sí misma.

6.5.3. Evaluación de las pruebas

Realizada la batería de pruebas, los encargados de su realización deberán entregar el informe al responsable. Este deberá comparar los resultados obtenidos con los esperados. Si alguna prueba ha presentado problemas, se elaborará un informe. Este se remitirá al desarrollador encargado de la funcionalidad cuya prueba haya fallado, para que provea una solución a la mayor celeridad posible.

Una vez comunicados los problemas encontrados, y aplicados los parches desarrollados para solucionarlos, se decidirá si re-ejecutar toda la batería de test o

solo parte de la misma. También se tendrá en cuenta posibles pruebas, ignoradas hasta el momento, pero que son necesarias para garantizar el funcionamiento del sistema. De existir, deberán recogerse en un nuevo plan de pruebas.

6.6. Preparación del mantenimiento del sistema

6.6.1. Establecimiento de la infraestructura

En el marco de esta tarea se asignará un responsable del mantenimiento. Este será el encargado de comprobar que el entorno propuesto está realmente preparado para soportar la ejecución de las diferentes tareas que se deban realizar durante el mantenimiento del sistema.

Así pues, deberemos comprobar las herramientas que se necesitarán en el sistema y asegurarnos de que están instaladas, configuradas y listas para ser usadas. En particular, se consideran las siguientes herramientas imprescindibles:

- Herramientas de monitorización del rendimiento del sistema.
- Herramientas de monitorización de los módulos y máquinas del sistema.
- Herramientas de comunicación entre los empleados de los supermercados y entre los técnicos y administradores.
- Herramientas de registro de peticiones de mantenimiento, que englobará las tareas de solicitud, evaluación, realización y notificación.
- Herramientas de detección de riesgos, fallos o problemas en el sistema (en su totalidad o en alguno de los componentes del mismo)

6.6.2. Formalización del plan de mantenimiento

El propio responsable del mantenimiento, en contra de lo que se pueda pensar, debe recibir formación sobre el sistema sobre el cual deberá realizar el mantenimiento. Esta formación será impartida durante la fase de implantación del sistema.

El responsable podrá solicitar más información si considera que la formación o la documentación recibida es insuficiente para comprender el sistema (en su totalidad, y para cada módulo) y poder operar y mantenerlo durante la vida útil del sistema.

Finalmente, se establecen los siguientes tipos de mantenimiento para el sistema:

- *Mantenimiento preventivo.* Para todo el sistema mediante un sistema de registro de peticiones de mantenimiento. Se tendrá especial cuidado para el módulo de ventas (tanto pedidos de los clientes, como a proveedores desde la tienda) y recursos humanos (gestión de asuntos relacionados con los empleados) ya que no son utilizados por personal técnico formado.

- *Mantenimiento predictivo.* Para la parte física (especialmente hardware de los servidores) mediante un sistema de monitorización, de manera que podamos prevenir posibles errores futuros del sistema, o remediarlos a la mayor prontitud posibles si no se pueden evitar de antemano.

6.7. Presentación y aprobación del sistema

6.7.1 Convocatoria de la presentación del sistema

Se preparará una presentación ante el consejero delegado de Kobiran y su equipo de trabajo, donde se comenten los módulos del sistema, configuraciones, procesos, datos a almacenar y procesar, etc. Será este consejero delegado y equipo quienes deberán aprobar el sistema que le presentamos.

En esta fase, se deben redactar y presentar una serie de documentos, entre los que destacamos los siguientes:

- Una presentación donde se aborden todos los temas relativos al sistema de información, la cual debe ser completa, clara y concisa. Es conveniente presentar al consejero delegado y su equipo de trabajo un resumen de dicha presentación, para que conozca a grandes rasgos los puntos que se van a tratar y puedan preparar preguntas, dudas, consultas o sugerencias de antemano.
- Informe de evaluación, con un gran nivel de detalle sobre las diferentes pruebas realizadas, de forma que se pueda comprobar el correcto funcionamiento del sistema pormenorizadamente.
- Plan de mantenimiento, en el que figuran todos los procesos y cuestiones planteadas.

6.7.2. Aprobación del sistema

Tras haber realizado la presentación ante el comité de dirección de Kobiran, anotadas las sugerencias y resueltas las dudas o consultas, y si estos lo estiman, se procederá a la firma por la cual se aprueba el sistema de información propuesto.

Tras haber redactado formalmente el documento de aprobación, se asume que el consejo de dirección entiende perfectamente lo expuesto y no podrá solicitar cambios fuera de lo firmado.

6.8. Paso a producción

6.8.1. Preparación del entorno de producción

En el marco de esta fase se deberán realizar las siguientes tareas:

- Comprobar la correcta configuración de los sistemas de control de accesos y seguridad del sistema.
- Comprobar que los diferentes módulos funcionan correctamente y se integran como se había testado previamente y cómo se esperaba. Se comenzará por los módulos con menor grado de interacción con clientes y empleados, hasta los módulos principales (gestión de usuarios, control de ventas, y gestión de empleados).
- Se debe comprobar la disponibilidad del sistema (servidor web principalmente), su sistema gestor de bases de datos y la integridad de los datos almacenados.

6.8.2. Activación del sistema en producción

En esta última fase del desarrollo del sistema se procede a la activación del propio sistema de información. Este nuevo sistema empleará la base de datos con las modificaciones especificadas en apartados anteriores. Se establece el sistema como activo, por lo que se procede a dar de baja el anterior sistema que estuviera en funcionamiento.

Posteriormente, se realizarán las sesiones de formación a empleados. Con esto se pretende reducir la inclinación de la curva de aprendizaje para los empleados de la empresa que hagan uso del nuevo sistema (y otros posibles clientes). Pretendemos que el cambio se realice de forma breve, para mantener la productividad tan alta como se pueda.

Finalmente, se realiza la asignación de permisos para los usuarios que presentan a los diferentes integrantes de la organización, se activa el sistema de control de accesos y el sistema de mantenimiento.

7. Mantenimiento del Sistema de Información (MSI)

7.1. Registro de la petición

Primero se establecerán las áreas donde se pueden solicitar un mantenimiento de forma que se pueda hacer un mejor seguimiento de las peticiones:

1. Mantenimiento de seguridad: se refiere a las acciones que se realizan para proteger el sistema contra posibles amenazas de seguridad. Por ejemplo, el mantenimiento de seguridad podría incluir la aplicación de parches de seguridad, la configuración de cortafuegos o la realización de auditorías de seguridad.
2. Mantenimiento de hardware: se refiere a las acciones que se realizan para mantener en buen estado de funcionamiento el hardware utilizado en el sistema. Esto podría incluir la limpieza regular de componentes, la reparación o sustitución de piezas dañadas o la actualización de hardware obsoleto.
3. Mantenimiento de software: se refiere a las acciones que se realizan para mantener el software utilizado en el sistema en buen estado de funcionamiento. Esto podría incluir la actualización regular de software, la corrección de errores o la eliminación de software obsoleto.
4. Mantenimiento de bases de datos: se refiere a las acciones que se realizan para mantener en buen estado de funcionamiento las bases de datos utilizadas en el sistema. Esto podría incluir la limpieza regular de la base de datos, la optimización del rendimiento de la base de datos o la corrección de errores en la base de datos.

En segundo lugar, dentro de estas categorías se podrá solicitar los siguientes tipos de mantenimiento:

1. Mantenimiento preventivo: acciones planificadas que se realizan para prevenir problemas futuros en el sistema. Por ejemplo, el mantenimiento preventivo podría incluir la limpieza regular de hardware, la actualización de software obsoleto o la realización de pruebas de rendimiento.
2. Mantenimiento adaptativo: acciones que se realizan para adaptar el sistema a cambios en el entorno o en las necesidades de los usuarios. Esto puede incluir la configuración de nuevos dispositivos, la actualización de software, o la integración de nuevos componentes.
3. Mantenimiento perfectivo: acciones que se realizan para mejorar la calidad interna del sistema, sin cambiar su funcionalidad. Esto puede incluir la reestructuración del código, la optimización del rendimiento, o la implementación de nuevos algoritmos.

4. **Mantenimiento correctivo:** en un sistema de información se refiere a las acciones que se realizan para corregir errores o fallos que se producen en el sistema. Estos errores pueden ser identificados por los usuarios o por el personal encargado del mantenimiento del sistema, y su corrección puede implicar la modificación de código, la reparación o sustitución de hardware, o la actualización de software.

IMPORTANTE: Cuando se realiza el mantenimiento de un sistema de información, es importante tener en cuenta el tipo de mantenimiento que se va a llevar a cabo. Dependiendo del tipo de mantenimiento, se deberá estudiar qué subsistemas del sistema pueden verse comprometidos. Esto implica realizar una evaluación de los distintos subsistemas y componentes que forman parte del sistema, para determinar si los cambios que se van a realizar en uno de ellos afectarán a otros subsistemas.

Es muy importante tener en cuenta que cualquier cambio que se realice en un subsistema del sistema puede tener un impacto en el rendimiento del producto y en sus prestaciones. Por ejemplo, un cambio en el subsistema de base de datos puede afectar a la capacidad del sistema para procesar grandes cantidades de datos, mientras que un cambio en el subsistema de red puede afectar a la capacidad del sistema para comunicarse con otros sistemas.

Es por ello que, antes de llevar a cabo cualquier cambio en el sistema, se deben realizar pruebas para comprobar la viabilidad del cambio y su impacto en el rendimiento y las prestaciones del sistema. Además, es importante contar con un plan de contingencia en caso de que se produzcan problemas o errores durante el mantenimiento.

En tercer lugar, escogeremos un ciclo de vida para determinar los pasos a seguir en nuestro ciclo de vida de mantenimiento de Software.

El ciclo de vida que seguiremos para el mantenimiento será el estándar IEEE 1219 el cual define un conjunto de fases que se deben seguir en el proceso de mantenimiento de software, aunque también lo aplicaremos para tareas de mantenimiento hardware ya que se puede aplicar correctamente. Estas fases son las siguientes:

1. **Análisis:** En esta fase se lleva a cabo una evaluación del software para determinar cuál es su estado actual, identificar posibles fallos y determinar qué tareas de mantenimiento son necesarias.
2. **Diseño:** En esta fase se lleva a cabo la planificación de las tareas de mantenimiento necesarias, se definen los objetivos del mantenimiento y se establecen los recursos necesarios para llevar a cabo las tareas.
3. **Implementación:** En esta fase se llevan a cabo las tareas de mantenimiento planificadas, incluyendo la corrección de errores, la optimización del software,

la incorporación de nuevas funcionalidades y la eliminación de características obsoletas.

4. **Pruebas:** En esta fase se realizan pruebas para asegurarse de que las tareas de mantenimiento se han llevado a cabo correctamente y que el software funciona de manera adecuada.
5. **Documentación:** En esta fase se elabora la documentación necesaria para el software actualizado, incluyendo manuales de usuario y de mantenimiento, así como cualquier otra documentación necesaria para su correcta utilización.
6. **Entrega:** En esta fase se entrega el software actualizado al cliente o usuario final, asegurándose de que se han cumplido los objetivos del mantenimiento y de que el software funciona de manera adecuada.
7. **Evaluación:** En esta fase se evalúa el proceso de mantenimiento para determinar su efectividad, identificar posibles problemas y planificar mejoras para futuras tareas de mantenimiento.

7.1.1. Registro de la petición

En esta fase haremos una colección de solicitudes de mantenimiento de los distintos usuarios que hagan una petición de cualquiera de los tipos descritos anteriormente.

En todas las solicitudes de mantenimiento además de las características del mantenimiento solicitado, es importante incluir información personal del usuario que realiza la solicitud, como su nombre, apellido y número de identificación, para poder establecer una comunicación eficiente y llevar un registro claro de la solicitud.

También es importante incluir la fecha de la solicitud, para poder establecer una prioridad en función de la urgencia del mantenimiento solicitado y llevar un seguimiento de las solicitudes registradas.

Las fases recogidas en este proceso serán las siguientes:

1. **Entrega de la solicitud de mantenimiento:** En esta fase, el usuario que detecta un problema o una necesidad de mantenimiento, debe entregar una solicitud a través de un formulario o sistema online que proporcione la organización.
2. **Recogida por el comité de mantenimiento:** En esta fase, el comité de mantenimiento debe recibir y recopilar todas las solicitudes de mantenimiento, para su posterior análisis y evaluación.
3. **Registro de la solicitud:** En esta fase, se debe registrar la solicitud de mantenimiento en una colección o base de datos, incluyendo información relevante como la fecha de la solicitud, el tipo de mantenimiento solicitado, el usuario que la ha solicitado y cualquier otra información adicional que se considere relevante.

7.1.2. Asignación de la petición

Una vez tengamos el plan de mantenimiento y el catálogo de peticiones es hora de decidir si se acepta o rechaza la petición y realizar una asignación para la petición.

Dependiendo del ámbito los asignados pueden ser los siguientes:

- **Desarrolladores:** Los desarrolladores pueden ser asignados para llevar a cabo tareas de mantenimiento evolutivo o perfectivo, como añadir nuevas funcionalidades o mejorar el rendimiento del sistema.
- **Administradores de seguridad:** Los administradores de seguridad pueden ser asignados para tareas de mantenimiento preventivo o adaptativo, como actualizar los sistemas de seguridad o corregir vulnerabilidades.
- **Gestores de bases de datos:** Los gestores de bases de datos pueden ser asignados para tareas de mantenimiento adaptativo o correctivo, como actualizar o reparar la base de datos.
- **Especialistas en hardware:** personal encargado de la gestión y mantenimiento de los dispositivos físicos utilizados por el sistema, como servidores, ordenadores, impresoras, entre otros.
- **Especialistas en software:** personal encargado de la gestión y mantenimiento de los programas y aplicaciones utilizados por el sistema, como sistemas operativos, aplicaciones de software específicas, entre otros.
- **Administradores de redes:** Los administradores de redes pueden ser asignados para tareas de mantenimiento adaptativo o preventivo, como actualizar los sistemas de red o solucionar problemas de conectividad.
- **Personal de soporte técnico:** personal encargado de brindar soporte técnico a los usuarios del sistema ante cualquier problema técnico que puedan enfrentar.
- **Expertos en seguridad informática:** personal encargado de garantizar la seguridad de la información y los datos almacenados y procesados por el sistema, así como de prevenir y mitigar posibles amenazas informáticas.
- **Analistas de datos:** personal encargado de analizar los datos generados por el sistema con el objetivo de identificar posibles problemas o áreas de mejora, y proponer soluciones.
- **Especialistas en integración de sistemas:** personal encargado de integrar el sistema de información con otros sistemas o aplicaciones utilizados por la empresa para garantizar una correcta interoperabilidad y evitar problemas de incompatibilidad.
- **Personal de gestión de proyectos:** personal encargado de planificar, coordinar y supervisar las actividades relacionadas con el mantenimiento y mejora del sistema de información, asegurando que se cumplan los plazos, objetivos y presupuestos establecidos.

- Personal operativo: El personal operativo puede ser asignado para tareas de mantenimiento correctivo o preventivo, como reparar equipos o llevar a cabo labores de mantenimiento de rutina.
- Gestores de mantenimiento: Los gestores de mantenimiento pueden ser responsables de coordinar y supervisar todas las tareas de mantenimiento, asegurándose de que se llevan a cabo de manera eficiente y en el tiempo previsto.

Es importante que la asignación de tareas se haga en función de las habilidades y capacidades de cada miembro del equipo donde se ha enviado la petición y hay que asegurarse que se establezca una comunicación clara y efectiva para asegurar que todos los miembros estén al tanto de las tareas que les corresponden y de los plazos previstos para llevarlas a cabo.

Se hará una evaluación de las capacidades (como por ejemplo preguntar directamente) de este equipo para determinar si podrán llevar a cabo o no la petición y en caso negativo redactar un informe del por qué no.

7.2. Análisis de la petición

Se debe establecer un plan de acción detallado para llevar a cabo el cambio propuesto, incluyendo la asignación de recursos necesarios, los plazos de ejecución y los costos asociados al cambio. También se debe definir la estrategia de implementación para asegurar que el cambio se integre sin problemas en el sistema de información y no afecte negativamente su funcionamiento.

Es importante que se realice un análisis completo de la petición para asegurar que se están abordando todas las necesidades del usuario y que no se están dejando áreas importantes sin cubrir.

7.2.1. Verificación y Estudio de la Petición

Antes de iniciar el estudio de la petición, se verifica que la información registrada es correcta. Para determinar su validez hay que tener en cuenta el tipo de mantenimiento:

- Si se trata de un mantenimiento correctivo, se debe reproducir el problema.
- En el caso de un mantenimiento evolutivo, hay que comprobar que la petición es razonable.

También se estudiará adicionalmente cuando es adaptativo y perfectivo.

Una vez examinada la petición comienza su estudio, que será diferente en función del tipo de mantenimiento establecido:

1. En el mantenimiento correctivo de un sistema de información, se evalúa la gravedad del problema para determinar si la solución es a corto, medio o largo plazo. Si es un problema crítico, se aborda de inmediato para restaurar el nivel de servicio, pero luego se revisa para evaluar cualquier efecto secundario y establecer una solución permanente. Si no es crítico, se clasifica para tiempos posteriores.
2. En el mantenimiento evolutivo, se determina el alcance de la modificación de los sistemas de información inicialmente afectados. También se evalúa la complejidad de la modificación, así como los recursos necesarios para llevarla a cabo, como el tiempo y el personal necesario. Es importante definir claramente el alcance del cambio y las funcionalidades adicionales que se van a incorporar para asegurar que el sistema de información no sufra efectos secundarios no deseados.
3. En el caso del mantenimiento adaptativo, se realiza un análisis detallado de los entornos en los que opera el sistema de información y se determinan las modificaciones necesarias en hardware, software de base, gestores de base de datos y comunicaciones para garantizar el correcto funcionamiento del sistema. También se evalúa el impacto de las modificaciones en la arquitectura general del sistema de información y se establecen las medidas necesarias para garantizar la integridad de los datos y la seguridad de la información.
4. Finalmente, en el mantenimiento perfectivo se lleva a cabo un análisis detallado del código fuente del sistema de información para identificar las áreas que pueden ser optimizadas o reestructuradas para mejorar su rendimiento, eficiencia y calidad interna. También se pueden identificar posibles problemas de diseño y se pueden aplicar mejores prácticas de programación para optimizar el código y reducir el tiempo de ejecución.

En términos generales debemos asegurarnos de que los cambios no sean críticos y no tengan un fuerte impacto en áreas importantes como la seguridad, la eficiencia, la disponibilidad, la integridad, etc del sistema y que no repercuta negativamente de forma económica a la empresa.

7.2.2. Estudio de la propuesta de la solución

En el proceso de Estudio de la Propuesta de Solución para cada petición recogida en el sistema de información del supermercado, se asigna una prioridad y se analiza si existe relación con otras peticiones o si ya está en curso. Se evalúan los sistemas de información involucrados para determinar el impacto que la modificación puede causar.

Dependiendo si el mantenimiento es evolutivo, correctivo, adaptativo o bien es perfectivo se toman diferentes acciones:

Para el mantenimiento evolutivo, se estudia cómo atender la petición considerando la política de versiones vigente. Si implica incorporar o eliminar elementos, se evalúa la necesidad de realizar actividades del proceso de Análisis del Sistema de Información antes de identificar los elementos afectados

Para el mantenimiento correctivo, las peticiones no se consideran cerradas hasta que se verifique que la solución propuesta no comprometa el sistema. Se aplican soluciones a corto o medio plazo y se realizan pruebas pertinentes para garantizar la integridad y operatividad del sistema.

Para el mantenimiento adaptativo y perfectivo se tomarán las mismas medidas que el mantenimiento correctivo aunque en las ocasiones que requieran un gran cambio e implique incorporar o eliminar elementos, se aplicarán también medidas del mantenimiento evolutivo.

En ambos casos, se realiza una estimación preliminar del esfuerzo requerido utilizando los indicadores establecidos en el acuerdo de nivel de servicio para cada sistema de información.

Gracias a esto conseguimos un estudio del impacto y la aceptación o denegación de la solución en nuestro catálogo de soluciones junto a la propuesta de la solución.

7.3. Preparación de la implementación de la Modificación

Una vez finalizado el análisis previo de la petición y aprobada su utilización, se entra en la fase de detectar de manera descriptiva todos los recursos dañados por el cambio a través de una investigación exhaustiva de efecto. Este estudio tiene como objetivo principal establecer con precisión qué parte del sistema de información se verá afectada y en qué medida, brindando una comprensión clara y documentada de los elementos que deben ser modificados, tanto a nivel de software como de hardware.

El resultado del análisis realizado proporciona datos cuantitativos que se utilizan como base para aplicar los indicadores establecidos. Estos indicadores permiten establecer un plan de acción con el objetivo de cumplir el plazo máximo de entrega una vez se haya establecido el valor de los indicadores correctamente.

7.3.1. Identificación de Elementos Afectados

Se lleva a cabo un análisis exhaustivo del impacto de la petición para comprender el alcance real de la modificación, considerando el número, características y relaciones existentes entre los elementos afectados. Esto permite establecer una secuencia y

planificación adecuada para el desarrollo de los cambios, evaluando los recursos necesarios para llevarlos a cabo.

En el caso de un mantenimiento evolutivo que involucra la incorporación o eliminación de elementos, el alcance real de la modificación se determina después de realizar el proceso de Análisis del Sistema de Información, como se mencionó anteriormente. A partir de los resultados obtenidos en el estudio realizado, se identifican cada sistema de información afectado y se crean argumentos de búsqueda para determinar qué elementos están implicados en el proceso de cambio y en qué medida. Esto proporciona una base sólida para gestionar y ejecutar eficientemente el proceso de modificación.

Durante este estudio exhaustivo, se registrará de manera precisa y adecuada los recursos de la infraestructura tecnológica, incluyendo hardware, programas base, comunicaciones, entre otros.

Asimismo, se identificará y documentará los recursos asociados a los productos de software involucrados en cada solicitud. Esto puede abarcar desde modelos y pantallas hasta informes, módulos, programas fuente, programas objeto, JCL, archivos de datos y manuales de usuario y de explotación. Se establecerán referencias cruzadas entre estos recursos para facilitar su seguimiento y comprensión. Esto significa que se documentarán las relaciones y dependencias entre los diferentes elementos, proporcionando una visión clara de cómo interactúan y se afectan mutuamente.

Este enfoque exhaustivo garantiza que se tengan en cuenta todos los componentes y recursos relevantes para la modificación propuesta. Además, facilita la planificación precisa y la implementación ordenada de los cambios, al brindar una visión completa de los recursos tecnológicos y de software involucrados en cada solicitud.

7.3.2. Establecimiento de un plan de acción

En el proceso de establecimiento de un plan de acción, se identifican las tareas y actividades necesarias en los diferentes procesos de desarrollo, como el Análisis de Viabilidad del Sistema, Estudio del Sistema de Información, Diseño del Sistema de Información, Creación del Sistema de Información y Fijación y Asentimiento del Sistema. Estas tareas se determinan en función de las características, complejidad y alcance de la demanda estudiada, así como del proyecto de mantenimiento establecido para los sistemas de información involucrados.

En otras palabras, en esta etapa se establece un plan detallado que incluye las tareas específicas a realizar en cada proceso de desarrollo, considerando las

particularidades de la demanda y los objetivos del proyecto de mantenimiento de los sistemas de información afectados.

7.3.2. Especificación del plan de pruebas de regresión

Las pruebas de regresión son un tipo de pruebas que se realizan en el marco del proceso MSI 3.3, con el propósito de evitar el impacto negativo o los errores adicionales en otros elementos no modificados del sistema. El objetivo principal de estas pruebas es verificar que los cambios realizados en los elementos afectados no generen efectos no deseados en esos mismos componentes ni en otros del sistema.

Para lograr este objetivo, es necesario especificar casos de prueba que reflejen las interrelaciones existentes entre los diversos elementos identificados durante la labor de Identificación de Recursos Dañados (MSI 3.1). Estos casos de prueba deben diseñarse de manera que cubran todas las funcionalidades y escenarios relevantes, asegurando así que se verifiquen adecuadamente las interacciones entre los componentes del sistema.

Al ejecutar las pruebas de regresión, se busca confirmar que los cambios implementados no afecten negativamente el funcionamiento previo del sistema y que los componentes no modificados continúen operando correctamente. Esto ayuda a garantizar la integridad y estabilidad general del sistema después de la implementación de los cambios.

En nuestro caso para el sistema de información de nuestro supermercado, tendríamos pruebas de regresión como las siguientes:

- Caso de prueba de actualización de stock: Verificar que, después de realizar una compra de productos, los niveles de stock se actualicen correctamente en el sistema sin afectar otros procesos relacionados, como la generación de informes de inventario.
- Caso de prueba de generación de informes de inventario: Verificar que los informes de inventario generados después de la modificación muestran los datos correctos y sean consistentes con los cambios realizados en el registro de productos y niveles de stock.
- Caso de prueba de búsqueda de productos: Verificar que la función de búsqueda de productos siga funcionando correctamente después de la modificación, sin introducir errores adicionales o afectar la recuperación de información de otros módulos del sistema, como el punto de venta.
- Caso de prueba de integración con el sistema de compras: Verificar que la modificación en el módulo de gestión de inventario no afecte la integración con el sistema de compras, asegurando que los pedidos de reposición se realicen correctamente y los productos se agreguen al inventario sin problemas.

- Caso de prueba de cálculo de precios: Verificar que los precios de los productos se calculen correctamente después de la modificación, considerando cualquier cambio en las reglas de precios o descuentos aplicables.
- Caso de prueba de generación de informes financieros: Verificar que los informes financieros generados después de la modificación, como los estados de ganancias y pérdidas o los balances, muestren datos precisos y no se vean afectados negativamente por los cambios realizados en el módulo de gestión de inventario.
- Caso de prueba de funcionalidad de alertas de stock: Verificar que las alertas de stock, que avisan cuando un producto está por debajo del nivel mínimo, sigan funcionando correctamente después de la modificación y que se generen de manera adecuada según los cambios en los niveles de stock.
- Caso de prueba de interoperabilidad con sistemas externos: Verificar que la modificación en el módulo de gestión de inventario no afecte la interoperabilidad con sistemas externos, como proveedores o sistemas de logística, asegurando que los datos se intercambien correctamente y no se introduzcan errores en los procesos de compra o entrega de productos.

Estas pruebas de regresión se centran en verificar que los cambios realizados en un elemento del sistema, como el módulo de gestión de inventario, no introduzcan comportamientos no deseados o errores en otros elementos no modificados, como la generación de informes, búsqueda de productos o integración con otros módulos.

7.4. Seguimiento y Evaluación de los Cambios hasta la Aceptación

El seguimiento de los cambios se realiza según el plan de acción establecido, verificando que solo se han modificado los elementos afectados y se han realizado las pruebas correspondientes, incluyendo pruebas de integración y del sistema. Se evalúa el resultado y se aprueba la petición después de las pruebas de regresión, asegurando que todo funcione correctamente. Al cerrar la petición, se puede incluir información relevante en el catálogo de mantenimiento para análisis futuros.

7.4.1. Seguimiento de los cambios

A partir del plan de pruebas de regresión se hace un seguimiento de los cambios que se han provocado en el sistema de forma que se haya modificado únicamente lo que se especificó de forma correcta, por ejemplo podríamos hacer el siguiente seguimiento de los cambios en nuestro sistema de información de nuestro supermercado:

1. Verificar la generación de informes: Se comprueba que los informes asociados al cambio están actualizados y se generan correctamente, asegurando que la información presentada sea precisa y confiable.
2. Controlar la modificación establecida: Se comprueba que solo se han realizado las modificaciones definidas en el plan de acción, evitando cambios no autorizados o innecesarios.
3. Actualización de productos: Se verifica que los productos afectados por la petición, como programas, archivos de datos o manuales, han sido actualizados correctamente según los requisitos del cambio.
4. Control de desarrollos paralelos: Se lleva un seguimiento de los diferentes desarrollos que se estén realizando simultáneamente en un mismo componente, garantizando la coordinación y evitando conflictos o inconsistencias.
5. Realizar la traza de los cambios: Se registra y documenta todos los cambios realizados en los procesos a lo largo de la petición, asegurando una trazabilidad adecuada.
6. Verificar las pruebas realizadas: Se asegura que se han llevado a cabo de manera satisfactoria las pruebas unitarias, de integración y del sistema que se consideraron necesarias para validar los cambios implementados.

El seguimiento de estos aspectos contribuye a garantizar la correcta implementación de los cambios y a asegurar la integridad y calidad del sistema de información.

7.4.2. Aprobación y Cierre de la Petición

En esta fase la petición de mantenimiento se aprueba formalmente según los resultados obtenidos. Se actualiza el catálogo de peticiones con el cierre de la petición tratada. Además, se registra información cuantitativa sobre el tiempo empleado en el análisis, estudio del impacto, resolución del cambio y recursos utilizados. Esto permite evaluar la eficacia de las técnicas y procedimientos de mantenimiento.