UNIVERSIDAD
DE GRANADA

Prácticas de la asignatura Administración de Sistemas y Seguridad

Máster en Ingeniería Informática

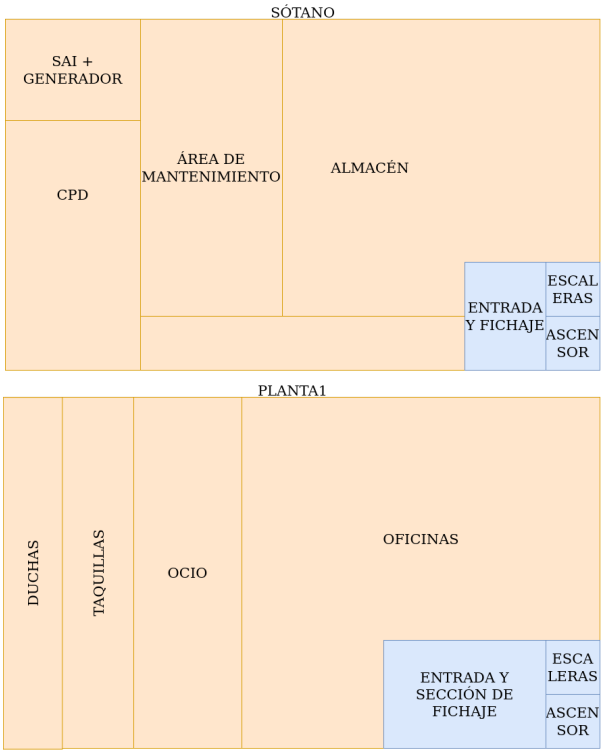
Curso 2019-2020

Carlos Enríquez López
Antonio Martos Rodríguez
María Matilde Cabrera González
Lidia Sánchez Mérida

Índice

Descripción de la organización.

Nuestra organización se presenta como un fábrica de coches autónomos con un conjunto de instalaciones y una amplia plantilla de 1.000 trabajadores. Para desarrollar su trabajo la corporación dispone de un edificio que consta de seis plantas en total más un sótano. A continuación se visualiza el mapa del inmueble representando los dos primeros pisos correspondientes al sótano y a la planta baja.



En el sótano se sitúan el centro de procesamiento de datos donde se almacena la información relacionada con los empleados, las investigaciones de campo, los prototipos y productos desarrollados, proveedores de componentes físicos y software, clientes, entre otros datos.

Por otra parte, en esta misma planta también se encuentra un almacén en el que se guardan componentes tanto tecnológicos como relativos a los prototipos de los vehículos en desarrollo. Asimismo, en esta planta también se encuentran las instalaciones eléctricas con sus respectivos generadores y conexiones pertinentes para abastecer el edificio completo de electricidad.

La primera planta está destinada a las diversas funcionalidades relacionadas con el personal de la organización, y por ende, se sitúan las oficinas de los diferentes departamentos que existen en la empresa así como las instalaciones personales y de ocio.

En las dos siguientes plantas se encuentran ambas instalaciones orientadas a la fabricación de los automóviles de la compañía. Asimismo, en las dos siguientes se encuentran los dos

campos de testeo para verificar y realizar las pruebas pertinentes de los prototipos que se encuentran en desarrollo.

Por último disponemos de una planta orientada a investigación en la que se encuentra el equipo material necesario para realizar los estudios correspondientes a los aspectos influyentes en la construcción de los coches autónomos.

Al tratarse de un sector innovador la organización lleva en bolsa año y medio y recibe de sus inversores inyecciones de capital del orden de unos 10 millones de dólares mensuales. Esto le permite seguir investigando en el área y ofrecer productos a baja rentabilidad.

Misión

Ser una empresa reconocida mundialmente en la fabricación de vehículos autónomos, satisfaciendo todas las necesidades de nuestros clientes con la ayuda de nuestro personal altamente cualificado.

Visión

Llegar a ser la empresa líder en el campo de vehículos autónomos. Ser la primera opción a valorar para nuestros clientes.

Descripción del sistema.

El sistema a desarrollar consta de tres módulos principales:

1. Control de horarios.
   En este subsistema se mantiene un registro de los horarios de los trabajadores. El objetivo consiste en controlar las jornadas de los diferentes miembros de la plantilla para, a su vez, permitir el acceso a los distintos recursos y zonas del edificio durante la realización de sus tareas. Los empleados deberán de utilizarlo tanto al comenzar como al finalizar su jornada laboral. Para ello, se estudiarán diferentes alternativas de modo que se integre un dispositivo sencillo de uso exclusivo dentro del edificio.
2. Control de acceso.
   Este segundo módulo tiene como objetivo supervisar los accesos a las distintas áreas del edificio. Para ello se crearán diferentes grupos de usuarios en el sistema con diversos privilegios con los cuales realizar la distinción sobre qué trabajadores pueden acceder a qué zonas.
3. Gestión de tareas.
   Por último, integramos un tercer subsistema con el que poder crear y administrar las tareas. De nuevo, como en el caso anterior, se crearán diferentes grupos de usuarios para limitar las distintas operaciones que se pueden realizar. El objetivo es que los supervisores y jefes de sección sean los únicos que creen y/o modifiquen las tareas asignadas a los trabajadores. Para ello introducen la información asociada como la descripción, el estado inicial, los trabajadores asignados, etc. Mientras que

estos solo podrán realizar acciones tales como adjuntar un comentario, cambiar el estado en el que se encuentra la tarea, entre otras.

1. Planificación del sistema de información (PSI):

Para la implantación del sistema previamente descrito en la empresa el primer paso a realizar es la planificación del sistema. Este proceso incluye una larga lista de actividades como estudios, análisis, diseño o identificación de requisitos que deben ser completadas por parte de la empresa.

De todas ellas, la actividad que abarca una mayor implicación de administración de sistemas y que será llevada a cabo por este equipo para la empresa es la Definición de la arquitectura tecnológica.

1.1. Definición de la arquitectura tecnológica

Antes de poder definir la arquitectura es necesario estudiar las necesidades de la organización y contratar las distintas alternativas que se ofrecen para escoger la más conveniente según la organización.

1.1.1. Identificación de las necesidades de Infraestructura Tecnológica:

Los elementos necesarios para posibilitar la correcta administración y soporte del sistema propuesto anteriormente son los siguientes:

Componentes hardware:

- Un servidor de para alojar las aplicaciones de administración de tareas, fichaje y control de acceso. Un servidor de datos para almacenar los datos de asistencia y privilegios de los empleados y las tareas asignadas.
    - Las alternativas principales para solucionar esta necesidad son:
        - Subcontratar un proveedor cloud para alojar los servidores en la nube.
        - Levantar ambos servidores de manera física en las instalaciones de la organización.
- Terminales tipo tablet para la realización de las actividades de registro de tareas y de fichaje. Serán necesarias como mínimo una por cada instalación de acceso restringido del edificio.
    - Deben permitir el acoplamiento con un dispositivo de identificación biométrico o contar con uno ya incorporado.
        - En tablets Android e IOS no es posible usar su dispositivo de identificación biométrico por defecto, el lector de huellas, ya que el hardware no permite el acceso al mismo.
    - Las alternativas principales para su implementación son:
        - Tablets industriales portátiles con puertos suficientes para acoplar un dispositivo de identificación biométrico y permitir carga simultánea.
        - Terminales TPV fijos que permitan acoplamiento de dispositivos de identificación biométrica.
- Dispositivos de identificación biométrico:
    - De este tipo de aparatos se requerirán:

        - Entre 1 y 10 en la entrada del edificio principal para registrar los fichajes de los empleados.
        - Tantos como sean necesarios para en control de acceso a instalaciones restringidas para algunos usuario, presumiblemente uno por cada puerta de acceso.
        - Uno por cada terminal tipo tablet o TPV para uso de los empleados en su actividad diaria y tareas de registro de las mismas.
    - Las alternativas propuestas en cuanto a la funcionalidad de estos componentes son:
        - Dispositivos simples en todos los casos que requieren acoplamiento a un componente con software para su manejo.
        - Dispositivos simples para las terminales de los empleados y de fichaje y dispositivos específicos para control de acceso, que cuenten con perno incluido. Requerimientos posteriores de comunicación pueden conllevar la necesidad de que incluir conectividad vía WiFI (p.e: Terminal RX1).
    - Los distintos tipos de dispositivos que podemos encontrar en el mercado y que son aptos para las tareas mencionadas son:
        - Lectores de huellas dactilares. Existen lectores simples o incrustados en sistemas de acceso listo para su uso.
        - Escáneres de iris con los cuales podemos encontrar las misma variaciones que con los lectores de huellas.
- Estaciones de trabajo para la administración del sistema de información.
    - Ordenadores de sobremesa.
    - Portátiles.
- Un switch para administrar el acceso a la red de cada planta del edificio.

Comunicaciones:
Para la comunicación entre dispositivos se pueden optar por varias alternativas:

- Una red LAN desplegada en el edificio para conectar los servidores (si son físicos se conectará directamente con ellos y si se ubican en la nube se conectará con un servidor local que ejerza como proxy) con todos los terminales que hagan uso de datos o aplicaciones de la red.
    - De esta manera se requiere que los terminales incorporan un puerto de Ethernet RJ-45.
- Un red LAN que conecta con todos los switches del edificio y se extienda hasta una serie de puntos de acceso inalámbricos que ofrecen conexión WiFi para los terminales.

Disponibilidad y servicios críticos:
La disponibilidad de todos los servicios debe ser total durante toda la jornada laboral pues serán usados por los trabajadores y que estén caídos reduciría su desempeño.

Servicios de terceros:

- Servicio *cloud* para almacenar las copias de seguridad del sistema de modo que se garantice el acceso a la información respaldada independientemente del error que pueda sufrir este y/o sus componentes. Las tres alternativas son las siguientes:
    - AWS Backup. Dispone de dos tipos de almacenamiento de las copias de seguridad, servicios de restauración de información y transferencias de datos desde la copia de seguridad guardada.
    - IBM Backup. Almacenamiento de las copias de seguridad en la nube con servicios adicionales de gestión, protección de datos y búsqueda en los mismos.
    - Dropbox Business. Prove almacenamiento de datos en la nube, historial de versiones y recuperación de archivos eliminados de 120 días.

El servicio con mayor grado de criticalidad que podemos encontrar en el sistema será el de control de acceso. Si este fallara en primer lugar, la seguridad del sistema estaría expuesta, supondría un cese de la actividad de la planta hasta que el problema se solucionara e incluso podrían quedar trabajadores atrapados.

Por lo tanto, además del acceso biométrico se propone la posibilidad de acceder con llaves maestras. Se acompañará de monitorización de las entradas y salidas (con y sin llave) para comprobar que no se produce ninguna violación de la seguridad.

1.1.2. Selección de la arquitectura tecnológica:

De acuerdo al contexto de la organización y al sistema de información, la infraestructura escogida para dar soporte a las necesidades previamente mencionadas será la siguiente:

Componentes hardware:

- Servidores:
    - Se ha optado por levantar los servidores físicos en las instalaciones de la organización ya que evitamos el sobrecoste a largo plazo de contratar un proveedor en beneficio de un primera inversión más fuerte en hardware que se amortizará con el tiempo.
- Terminales para actividades de registro de tareas:
    - La decisión ha sido, ante la alternativa de los TPV, la de incorporar tablets industriales con el SO Android y varios puertos de conexión ya que
        - Con las tablets logramos un mayor control sobre el sistema y las app gracias a la flexibilidad de Android.
        - De cara al futuro se podrán incluir nuevas aplicaciones en los dispositivos con poco esfuerzo.
        - Implantación más fluida ya que son dispositivos ya conocidos entre los empleados.
        - Cuentan con conexión WiFi por defecto.
- Dispositivos de identificación biométrica:
    - El tipo de dispositivo escogido finalmente ha sido el lector de huellas dactilares ya que aunque son menos precisos que los lectores de iris:
        - En el mercado existe más variedad.
        - Es más barato que las alternativa y realiza la misma función.

        - Es más sencillo de implementar y están más extendidos en la industria.
    - De cara a su funcionalidad se implantarán dos variaciones de lectores:
        - Lectores simples para incorporar a las tablet industriales ya que:
            - Cumplén con la función requerida de identificación segura en menos de un segundo.
            - Son de fácil instalación y configuración.
            - Ofrecen muchos posibles usos en el futuro. Tienen un coste muy contenido en comparación con otros dispositivos.
        - Lectores de huellas dactilares específicos para control de acceso gracias a que:
            - Son más fáciles de instalar en puertas que una combinación de lector y tablet y además ya cuentan con un perno para la apertura o cierre de la puerta..
            - Son una alternativa más económica que comprar varios dispositivos para el mismo propósito.
            - Aunque son menos configurables podemos comunicarlos a través de WiFi o cableado LAN.
- Estaciones de trabajo para los administradores.
    - Se ha optado por adquirir un portátil para cada uno de los administradores con el objetivo de que puedan desplazarse libremente por el edificio disponiendo de un medio tecnológico para realizar sus respectivas tareas.

Comunicaciones:

- En lo relativo al despliegue de red que se utilizará será el mixto entre cableado e inalámbrico mencionado anteriormente donde el cableado red cubrirá la comunicación en cada planta que se extenderá con punto de acceso inalámbricos. Los terminales de control de acceso contarán con enlaces cableados mientras que el resto usarán WiFi. En cualquier caso se deberá contar con una red alta velocidad de transferencia. Las principales opciones en cuanto a la red a desplegar son:
    - La red cableada a desarrollar será de menor tamaño y se podrá expandir al añadir puntos de acceso.
    - Se asegura la disponibilidad del control de acceso siempre que haya red y de la manera adecuada y se permite aumentar el número de dispositivos bajo la red solo aumentando en número de puntos de acceso inalámbricos, sin tener que aumentar el cableado.

Disponibilidad y servicios críticos:

- Finalmente de cara a los servicios críticos la alternativa más segura es acompañar al servicio de control de acceso de una llave maestra física que permita la apertura de las barreras sin necesidad de conexión y una fuerte monitorización de los accesos.

Servicios de terceros:

- Para almacenar las copias de respaldo del sistema de forma remota la organización se ha decantado por contratar el servicio AWS Backup puesto que es el más económico y el que más servicios ofrece.

2. Desarrollo de sistemas de información:

En esta sección, una de las más importantes en el ciclo de vida de un sistema, se describirán todas las actividades y tareas que se deben llevar a cabo para desarrollar un sistema desde el punto de vista de la administración de de sistemas.

2.1. Estudio de la viabilidad del sistema (EVS)

En el estudio de viabilidad se analizará el conjunto concreto de las necesidades para llegar a una solución a corto plazo y decidir, en base a esta, si el proyecto sigue adelante o se abandona.

Las actividades que se desarrollan para este estudio son muy variadas, pero de cara a la administración de sistemas se tendrán en cuenta las siguientes:

2.1.1. Establecimiento del alcance del sistema

En cuanto al alcance del sistema se tomará como referencia los requisitos aportados por la empresa en la descripción de su sistema ya que no es una tarea de la administración.

De cara a los usuarios y desde el punto de vista de la administración se ha realizado el siguiente catálogo con los principales usuarios del sistema una vez esté implantado.

- Catálogo de usuarios:
    - Administrador de servidores.
    - Administrador de la base de datos.
    - Administrador de redes.
    - Empleados (su nivel y privilegios dependerá del papel que realicen en su trabajo).

2.1.2. Estudio de la situación actual

La situación actual del sistema de la organización desde la perspectiva de la administración de sistemas y en según el sistema a desarrollar es el siguiente:

- Elementos físicos de los sistemas actuales:
    - CPD para servidores y datos ubicado en el sótano del edificio y mantenido por la empresa.
    - Red LAN de baja extensión ya instalada en las zonas básicas del edificio.
- Usuarios participantes en el sistema actual:
    - Administrador de servidores.
    - Administrador de la base de datos.
    - Administrador de redes.

La información relativa a la lógica de otros sistema no ha sido proporcionada por parte de la empresa.

2.1.3. Definición de requisitos del sistema

En esta sección se definen los requisitos generales que debe abarcar el sistema desde el punto de vista de la administración para cumplir con una correcta implantación del sistema.

Identificación de las directrices de seguridad y gestión de cambios.

- Políticas de seguridad:
    - Los accesos a todas las estancias restringidas estarán controlados por un dispositivo biométrico de reconocimiento de huella dactilar. Alternativamente se podrá usar una llave física maestra que permita el acceso.
    - Existirá más de una llave maestra para que un fallo no comprometa todas las instalaciones. Las llaves estará en posesión del administrador del sistema que será el único que podrá hacer uso de las mismas.
    - Al CPD y a los armarios de redes solo tendrán acceso los administradores del sistema.
    - El CPD contará con conexión remota únicamente accesible por los administradores del sistema.
    - El CPD contará con las medidas físicas de vigilancia que se desempeñaban antes de la instalación del sistema sin ninguna añadida.
    - Los accesos a los recintos de trabajo por parte de los empleados se realizarán de la manera ya especificada, mediante huella dactilar asociada al perfil de empleado de cada trabajador.
    - Cualquier acceso a cualquier recinto será monitorizado y almacenado en un histórico en el servidor junto con los datos de fecha, hora, persona y recinto.
- Directrices de gestión de cambios:
    - Todos los cambios en la organización que involucren la administración del sistema estudiado deben ser primero evaluados. Para ello se debe entregar un informe a los administradores del sistema los cuales estudiarán el caso concreto, la viabilidad y el beneficio y lo aprobarán si lo creen conveniente. Cualquier cambio aprobado será llevado a cabo por los mismo administradores y no por terceros.

Los requisitos mencionados anteriormente son los identificados por el departamento de administración de sistemas como necesarios para la correcta implantación del sistema y deberán añadirse al catálogo de requisitos generales para tenerse en cuenta en la decisión final sobre la viabilidad del proyecto.

2.1.4. Descripción valoración y selección de las alternativas de solución

Finalmente,de acuerdo a la arquitectura tecnológica propuesta y los requisitos identificados anteriormente se proponen los siguientes elementos del sistema:

- Matriz Procesos / Localización geográfica.
    - Las nuevas aplicaciones con las que contará el sistema se desplegarán en un servidor en el CPD de la empresa, ubicado en el sótano del edificio.
- Matriz Datos / Localización geográfica.

    - Los datos almacenados y manejados por las aplicaciones del sistema se guardarán en volúmenes guardados en discos SSD.
- Entorno tecnológico y comunicaciones.
    - La alternativa de entorno tecnológico a evaluar en el estudio de viabilidad será la descrita anteriormente en el punto 1.1.2 pues ya ha sido evaluada su idoneidad.
- Estrategia de implantación global del sistema.
  Ante el entorno tecnológico planteado y los requisitos descritos para el sistema se propone la siguiente estrategia de implantación para la evaluación de su viabilidad.
    - Instalación en un armario del CPD de tres nuevos blades, uno para cada nueva aplicación que incluirá el sistema (control de acceso, administración de tareas y fichaje).
    - Instalación de otro armario del CPD de los discos necesarios para almacenar los datos de dichas aplicaciones y conectar los armarios. Con instalaciones en armarios separados se mejora la organización y se minimizan errores en la administración del sistema.
    - Instalación de un switch de acceso red en cada planta para la administración del acceso a red.
    - Extensión de la red LAN existente para cubrir las necesidades de instalación de los puntos de acceso inalámbricos y de los terminales de control de acceso biométrico.
    - Instalación de nuevos punto de acceso inalámbricos. Al menos uno por cada área de acceso restringido o por cada 100m2 aproximadamente. Cifras más concretas se darán cuando se realice un análisis del sistema.
    - Instalación de los terminales de control de acceso con perno (junto con las cerraduras de llave maestra) en las puertas de entradas y salidas de áreas de acceso restringido.
    - Adhesión de todos los lectores de huellas simples a los terminales tipo tablet de uso para empleados.
    - Distribución de todos los terminales tipo tablet a todas las instalaciones donde sean requeridos. Habilitación de un puerto de carga por cada terminal tipo tablet en un emplazamiento cercano a su lugar de uso común.
    - Registro en el sistema de todos los dispositivos que tiene permitido conectarse a la red de la organización.

Dada la situación económica de la empresa y las inyecciones de dinero asiduas que recibe la organización se concluye que tiene los recursos necesarios para adquirir el equipamiento mencionado e invertir en el desarrollo de este nuevo sistema.

3. Análisis del sistema de información

En esta sección se hará una especificación más detallada que la llevada a cabo hasta ahora para el sistema de información a implantar. De nuevo se llevarán a cabo la definición de las actividades donde la administración de sistemas esté implicada.

3.1. Definición del sistema

La definición del sistema implica la especificación de todos los elementos del entorno tecnológico así como de las características de los usuarios implicados en él.

3.1.2. Identificación del entorno tecnológico

Siguiendo la línea de la arquitectura tecnológica seleccionada en el punto 1.1.2 se procede a las especificación de la misma en sus diferentes niveles. Todos los elementos seleccionados se han escogido de cara al cumplimiento de los requisitos analizados en la sección 3.2.1.

Componentes hardware:

- Servidores:

  Hardware escogido: El servidor escogido para almacenar las aplicaciones será el Smart Value Power Edge R6515 para racks de DELL. Cuenta con el procesador AMD EPYC 7302P 3GHz de 16 núcleos y 64 GB de RAM. Suficiente para soportar las aplicaciones a incluir en el sistema hasta cuando más demanda sobre ellas se espere.

  Se adquirirán discos SSD HPE SSD 400GB SAS III para almacenar las bases de datos del sistema, ya que este tipo de discos destacan por su velocidad de lectura y escritura. Asimismo, se comprarán el mismo número de discos SSD para configurar sus correspondientes discos RAID y así asegurar la redundancia y evitar posibles pérdidas de datos.

- Terminales para actividades de registro de tareas:
  - Terminal escogido: Huawei Mediapad T5, 3GB RAM, 32GB almacenamiento interno.

- Dispositivos de identificación biométrica:
  Los lectores de huellas acoplables a los terminales:
  - Dispositivo escogido: Hamster Pro.

  Lector de huellas para control de acceso:
  - Dispositivo escogido: NN99. Cuenta con funcionalidades extendidas como reconocimiento facial y teclado para posible uso futuro ante cambios en el sistema.

- Estaciones de trabajo para los administradores:

    - Los portátiles corresponden al modelo MacBook Pro de 16”, procesador de 8 núcleos, un espacio de almacenamiento de hasta 8TB SSD, 64GB de memoria RAM, entre otras características.

Comunicaciones:

- Red cableada de LAN con conexión de cable de par trenzado y conectores RJ-45 a ser extendida en cada planta (Unos 200 metros de cable en total.)
- Switches seleccionados: Cisco SF220 de 48 puertos como previsión ante posible expansión futura del sistema.
- Puntos de acceso seleccionados: CISCO Catalyst 9130.

Disponibilidad y sistemas críticos:

- Cerradura común anti-bumping con conexión al perno electrónico para la apertura.
- Botón de apertura de emergencia en el lado interior del control de acceso.
- Sistema de monitorización de entradas/salidas por histórico.

Servicios de terceros:

- Programación, realización, almacenamiento y gestión de copias de seguridad mediante el servicio AWS Backup con almacenamiento en frío para minimizar costes ya que no se realizarán demasiados accesos a las copias de respaldo.

3.1.3. Identificación de usuarios

La lista de usuarios tanto participantes como finales del sistema junto con sus permisos es la siguiente.

- Administrador de servidores.
    - Acceso a todas las instalaciones del complejo y a armarios de red. Permiso sobre el contenido y administración de las aplicaciones del sistema.
- Administrador de la base de datos.
    - Acceso al CPD y al contenido y administración de las bases de datos de las aplicaciones del sistema.
- Administrador de redes.
    - Acceso a todas las instalaciones del complejo y a los armarios de red.
- Empleados.
    - Sus privilegios pueden variar en función de su puesto y otros factores su matriz de privilegios se almacena en el sistema con los datos concretos. En ningún caso contarán con acceso al CPD o a los armarios de red. El acceso a las aplicaciones vendrá únicamente dado para un uso a nivel de usuario mediante sus credenciales de acceso y las funcionalidades a las que puedan acceder dependerán de su puesto.

3.2. Establecimiento de los requisitos

En esta sección se recogen los requisitos relativos al área de administración de sistemas del proyecto a implantar.

3.2.1. Obtención, análisis y validación de los requisitos

Los requisitos necesarios para el correcto funcionamiento del sistema desde el punto de vista de la administración de sistemas son:

Requisitos de implantación:

- Obtención de un servidor que cumpla con los estándares de tamaño de unidades rack para alojar las aplicaciones del sistema.
- Obtención disco SSD con conexión SAS III para alojamiento de datos de rápido acceso de la base de datos de huellas dactilares..
- Las tablets deberán ser portátiles, con sistema operativo Android Nougat (7), al menos un puerto USB y un puerto de carga.
- Por cada tablet a implantar se debe ubicar cerca un enchufe libre junto con un cargador apropiado.
- Dispositivos simples de reconocimiento de huella dactilar con conexión USB y SDK para Android disponible y de libre uso.
- Dispositivo de control de acceso con huella dactilar con puerto de red RJ-45.
- Kit de perno electrónico con alternativa manual compatible con los dispositivos de control de acceso con huella dactilar.
- Extensión de la red LAN de cable de par trenzado a lo largo de todas las instalaciones de la organización. Necesidad de conexiones RJ-45.
- Instalación de switches en cada planta para control y administración de la red LAN de la organización.
- Despliegue de puntos de acceso inalámbricos en la red de la organización que ofrezcan cobertura en todas las instalaciones.

Requisitos de rendimiento:

- El servidor debe poder soportar una carga de hasta 300 peticiones/segundo de manera continua durante 1 hora.
- El tiempo de respuesta de disco al pedir una huella dactilar debe ser menor a 100ms.
- El tiempo de reconocimiento de huella del lector de huellas debe ser menos que 500ms.

Requisitos de Seguridad:

- Se debe realizar una copia de seguridad diaria para prevenir los ataque con ransomware o sucedáneos.
- Semanalmente y de manera automática se ejecuta la creación del reporte de fichajes de los empleados.
- Los dispositivos de control de acceso deben contar con sistema de retardo, apertura automática ante pérdida de corriente eléctrica en los pernos y botón de emergencia para salida de la instalación de acceso restringido.
- Cada entrada o salida realizada debe ser registrada en un histórico en el que deben guardarse los datos del último año completo. Cada usuario que ingrese debe pasar su huella dactilar aunque la puerta de acceso esté abierta.

Requisitos de disponibilidad:

- El servidor debe contar con un sistema de discos en RAID para asegurar que el sistema siempre puede estar en funcionamiento.
- Los discos del servidor deben posibilitar cambios en caliente (hot swap) para no tener que parar en sistema ante el fallo de uno de ellos.
- Se debe contar con unidades de repuesto para todos los dispositivos que se usan en el sistema.

Los requisitos anteriores son los establecidos por la organización y considerados como prácticas necesaria para el buen funcionamiento del sistema desde el punto de la administración. El resto de requisitos relativos a otras áreas no han sido considerados. Se concluye por tanto, que la revisión de los requisitos ha concluido con éxito y estos son válidos consistentes y completos.

3.2.2. Especificación de Casos de uso

A continuación se describen los casos de uso que pueden darse en la organización y que son competencia de la administración de sistemas.

Casos de uso:

- Cambio de disco en caliente.
  Escenario: Detección de un disco defectuoso/Cambio de disco por fin de vida útil.
  Postcondición: El disco a reemplazar a sido sustituido por uno nuevo y el sistema puede establecer la consistencia del mismo para su correcto funcionamiento.
  Interfaz de usuario: Rack de discos y disco cuya especificación permita el cambio en caliente.
  Condición de fallo: No existan discos de repuesto disponibles que permitan el cambio en caliente.
- Realización de copia de seguridad.
  Escenario: Llegada de la madrugada de un día laborable/Situación de emergencia que requiera realizar una copia de respaldo.
  Postcondición: En uno o varios discos aislados del sistema y protegidos así como en almacenamiento en la nube debe estar guardada la información de la bases de datos del sistema.
  Condición de fallo: No hay nadie que pueda detonar el inicio del proceso de realización de copia de respaldo en caso de emergencia.
- Acceso a un área restringida mediante huella dactilar.
  Escenario: Un empleado necesita acceso a un área restringida para realizar su trabajo.
  Postcondición: La puerta de las instalaciones deseadas se abre de manera correcta.
  Interfaz de usuario: Lector de huellas dactilares acoplado a puerta de acceso.
  Condición de fallo: El usuario no tiene los permisos requeridos para acceder al área que desea.
- Acceso a un área restringida mediante uso de llave maestra.
  Escenario: Un empleado necesita acceso a un área restringida para realizar su trabajo.
  Postcondición: La puerta de las instalaciones deseadas se abre de manera correcta.

Interfaz de usuario: Cerradura de llave maestra para acceso a instalaciones.
Condición de fallo: No se cuenta con la llave maestra necesaria.

- Sustitución de dispositivos defectuosos.
  Escenario: Un dispositivo del sistema no funciona de manera correcta.
  Postcondición: El dispositivo es sustituido por uno nuevo que si cumple con las tareas de la manera adecuada.
  Interfaz de usuario: Dependiente del dispositivo a sustituir.
  Condición de fallo: No Existen unidades de repuesto del dispositivo a sustituir.

De estos casos de uso se pueden extraer los requisitos anteriormente redactados junto con sus escenarios y otras características derivadas de los mismos como las relativas a seguridad y rendimiento.

3.3. Migración de datos y Carga inicial

En función del modelo de datos anterior especificado por el grupo de desarrollo del sistema se definen las siguiente necesidades de migración y carga inicial de datos.

Ya que el sistema a implementar es nuevo, la única información previa existente es la de los empleados. No obstante, esta se encuentra almacenada de antemano en una base de datos en el centro de procesamiento de datos de la organización. La única necesidad es la de añadir los campos ‘Horario’ y ‘Permisos’ a la tabla de empleados de la base de datos. Por lo tanto, la única actividad necesaria es la de la carga inicial de datos.

Carga inicial de datos:
Las tablas a rellenar en la carga inicial de datos son: Horario, Tarea, Fichaje y EmpleadoTieneTarea.
Los datos a introducir son triviales ya que los horarios y las tareas son ya existentes aunque no estén introducidos en el sistema y deberán ser introducidos por los propios empleados y jefes de departamentos mediante las aplicaciones que ofrece el sistema. Los fichajes también se registran de manera automática por el sistema.

Por lo tanto queda solo introducir los horarios de los trabajadores en el sistema. Para ello no se requiere el uso de ninguna herramienta o software ya que deben ser copiados los horarios reales de los trabajadores. Se hará mediante el uso de un script que recoja los datos de los documentos excel donde estén reflejados los horarios y los introduzcan en la base de datos.

El orden de carga de las tablas será Horarios, Tareas, la relación EmpleadoTieneTarea y por último los fichajes una vez el sistema comience su funcionamiento.

El método de confirmación de que los procesos han sido realizados de manera exitosa será mediante contraste por medio de los empleados de los datos registrados y verificando que son correctos.

3.4. Elaboración de los modelos de procesos.

Dados los procesos existentes en el sistema a continuación se obtiene las características propias de cada proceso junto con su Matriz de Procesos / Localización Geográfica.

3.4.1. Características de los modelos de procesos del sistema.

Los modelos de procesos de sistema proporcionados junto con sus características principales son los siguientes:

Autenticación de huella dactilar:

- Frecuencia de ejecución: 30 peticiones/min
- Procesos asociados: Registro de fichajes, administración de tareas, control de acceso.
- Restricciones de ejecución:
    - Tiempo máximo de respuesta: 200ms.
    - Número máximo de usuarios concurrentes: 50.
    - Periodo crítico: Dias laborables al inicio, descanso y fin de la jornada.

Registro de fichajes:

- Frecuencia de ejecución: 6 peticiones/min
- Procesos asociados: Autenticación de huella dactilar, generador de reportes de fichajes.
- Restricciones de ejecución:
    - Tiempo máximo de respuesta: 200ms.
    - Número máximo de usuarios concurrentes: 40.
    - Periodo crítico: Dias laborables al inicio, descanso y fin de la jornada.

Generador de reportes de fichajes:

- Frecuencia de ejecución: 1000 peticiones/semana
- Procesos asociados: Registro de fichajes.
- Restricciones de ejecución:
    - Tiempo máximo de respuesta: 1 día
    - Franja de ejecución: Domingos a las 23:00.
    - Periodo crítico:

Administración de tareas:

- Frecuencia de ejecución: 10 peticiones/min.
- Procesos asociados: Autenticación de huella dactilar.
- Restricciones de ejecución:
    - Tiempo máximo de respuesta: 500ms.
    - Número máximo de usuarios concurrentes: 100.
    - Periodo crítico: Dias laborables al inicio, descanso y fin de la jornada.

Control de acceso:

- Frecuencia de ejecución: 10 peticiones/min
- Procesos asociados: Autenticación de huella dactilar.
- Restricciones de ejecución:
    - Tiempo máximo de respuesta: 200ms.
    - Número máximo de usuarios concurrentes: 100.

- Periodo crítico: Dias laborables al inicio, descanso y fin de la jornada.

3.4.2. Matriz de Procesos / Localización Geográfica.

La localización geográfica de los procesos del sistema es la misma para todos. En nuestro caso, como la organización cuenta con un CPD, los procesos se alojarán y se les dará cobertura en el servidor montado en dicho centro de datos específicamente para esta finalidad.

3.5. Especificación del plan de pruebas.

A continuación se definirá el plan de pruebas para la parte del sistema implicada en la administración de sistema. 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.

Las pruebas para el área de administración de sistemas se limitarán a cubrir el correcto funcionamiento del entorno tecnológico, su implantación, su seguridad y su rendimiento. No obstante otras áreas requerirán del equipo de administración de sistema para llevar a cabo de manera adecuada su fase de pruebas.
Los recursos necesarios para la fase de pruebas deberán estar listos antes del inicio de la la fase de construcción del sistema.

3.5.2. Requisitos del entorno de pruebas.

Los requisitos para poder llevar a cabo las pruebas del sistema, tanto las relacionadas con la administración como las del resto de áreas, son los siguientes:

- Punto de acceso inalámbrico de prueba para comprobar las necesidades de cobertura.
- Lector de huellas simple para pruebas de autenticación.
- Lector de huellas de control de acceso con correspondiente kit de perno para realización de pruebas de seguridad en cuanto a apertura y cierre de instalaciones.
- Discos SSD para realizar las pruebas de configuración de discos RAID y los tests del rendimiento de los subsistemas.
- Servidor para alojar las aplicaciones que debe contar al menos con:
    - Sistema operativo igual al usado en producción.
    - Monitor para calcular rendimiento y poder estimar el necesario en producción.
    - Gestor de bases de datos como el ya usado por la empresa.
    - SDK y librerías usados por los dispositivos de lectura de huellas dactilares.
- Réplicas de los sistema de la organización ya implantados con los que se interactúa, en nuestro caso únicamente la base de datos de empleados.
- Copia parcial de ficheros de horarios de los empleados para pruebas de datos y carga inicial.
- Red LAN de pequeño tamaño que imite la de producción para pruebas de integración.

3.5.3. Pruebas de aceptación del sistema.

Las condiciones de aceptación de las pruebas propuestas por el equipo de administración de sistemas son las siguientes:

- Los datos de los empleados sus horarios y tareas asociadas sean los correctos.
- Sólo sea posible el acceso a áreas restringidas mediante huella dactilar o llave maestra.
- El sistema de control de acceso permite el acceso de manera adecuada dependiendo de los permiso del empleado.
- El sistema de control de acceso deje abiertas las puertas si no hay luz.
- Un empleado pueda acceder a una instalación usando el sistema de control en menos de 1 seg.
- Un empleado pueda fichar al entrar o salir del edificio en menos de 1 seg.
- La información en cualquier disco duro esté duplicada en otro disco.
- Se realice de manera diaria un copia correcta de los datos importantes del sistema.
- Todos los terminales instalados pueden acceder a la red y las aplicaciones desplegadas en el servidor.

El cumplimiento de todas ellas confirmará un buena instalación del entorno tecnológico y una buena administración del mismo.

4. Diseño del sistema de información

El objetivo de esta etapa consiste, primeramente, en definir la arquitectura asociada al sistema de modo que completemos el catálogo de requisitos general con las restricciones asociadas a sus componentes, las características del entorno donde se implantará el sistema así como los requerimientos de seguridad, control de acceso, administración y los procedimientos de operación.

4.1. Requisitos de diseño

En primer lugar vamos a identificar los requisitos asociados con la arquitectura tecnológica especificada anteriormente puesto que influye considerablemente en el diseño del sistema. Para ello comenzamos con los requerimientos relacionados con el rendimiento que debe proporcionar cada uno de los elementos que la componen.

- Servidores de datos y de aplicaciones.
    - Los servidores tanto de las aplicaciones como de los datos deberán encontrarse disponibles, al menos, durante la jornada laboral para que la plantilla pueda utilizar las aplicaciones alojadas.
    - El tiempo asociado a la latencia máxima que pueden experimentar los servidores de aplicaciones no podrá ser superior a 30 milisegundos.
    - Los servidores de aplicaciones deben de poder escalarse automáticamente en función del número de peticiones y la carga de trabajo.
    - Solo el grupo de administradores podrá acceder y/o modificar justificadamente los servidores de aplicaciones y de datos.
    - La base de datos debe ser única y se encuentra distribuida en varias máquinas pertenecientes a los servidores de datos situados en el CPD.
    - Solo el grupo de administradores de bases de datos podrán acceder y/o modificar las instancias de la misma.
    - La información y operaciones de la base de datos a las que pueda acceder cada trabajador dependerá del rol de usuario asociado en el sistema.
    - En operaciones que impliquen la modificación de la estructura de datos o de la información almacenada en la base de datos se deberá comprobar la integridad y la consistencia del sistema de almacenamiento resultante.
    - Crear índices para todas las tablas de la base de datos con el objetivo de minimizar los tiempos de respuesta en las consultas más frecuentes, como la obtención o adición de nuevos datos.
    - Configurar discos RAID para mantener, al menos, una copia de todos los discos en los que se almacenen los datos del sistema.
    - Programar la realización de copias de seguridad de los subsistemas y sus respectivos datos periódicamente.
    - Como lenguaje para la base de datos utilizaremos *MySQL* puesto que los datos disponen de una estructura definida y son fácilmente asociables mediante modelos entidad-relación.
    - El gestor de bases de datos será *MariaDB* puesto que es totalmente compatible con el lenguaje *SQL* y presenta más ventajas que el gestor

MySQL, como la escalabilidad y velocidad cuando las bases de datos tienen un tamaño considerable.
- Se configurarán tantos nodos como servidores de datos disponibles con el objetivo de distribuir el sistema de almacenamiento en diversos *hosts*.
- En cada nodo se ejecutarán dos instancias, una máster y otra esclava que se actualizará conforme le lleguen los datos a la máster.
- Si alguno de los servidores es atacado este se apagará automáticamente hasta que un administrador lo desbloquee.
- Si alguno de los servidores alcanza temperaturas extremas se apagará automáticamente para no sufrir daños.
- Solo se podrá acceder y realizar peticiones a los servidores desde la red local del edificio.

- Módulos del sistema. En el caso de nuestro proyecto el sistema cuenta con tres módulos diferenciados: un primer subsistema asociado al control de horarios de los empleados, un segundo relativo al control de acceso a las diferentes áreas del edificio y por último, un tercero que facilita la gestión de las tareas por parte de los trabajadores. El principal requisito reside en que cada uno de ellos será almacenado en un servidor *blade,* tal y como se comentó anteriormente, para mantener separados los tres subsistemas de modo que si surge un fallo en un servidor no afecta al sistema completo. A continuación se detallan los requisitos particulares a cada uno de los subsistemas.
    - Módulo de control de horarios.
        - Este módulo debe de estar disponible durante, al menos, la jornada laboral establecida en la organización
        - Cada trabajador solo podrá acceder a los datos de su propio registro con permisos solo de lectura. Solo los administradores podrán acceder a los registros de toda la plantilla pero también en modo lectura.
        - La tasa de errores deberá ser inferior al 1% del total de registros de horarios.
        - El sistema registrará los intentos de identificación y control de horarios satisfactorios y fallidos.
        - El sistema debe proporcionar una realimentación al usuario en sus operaciones principales, como es la de fichar al comenzar y finalizar su jornada laboral.
        - El sistema solo tomará como datos de entrada los proporcionados por los lectores de huellas para el control de horarios.
        - El sistema verificará el estado de los lectores de huellas enfocados al control de horarios y notificará a los administradores acerca de un mal uso o/y funcionamiento.
        - El sistema deberá notificar los casos en los que se realicen tres intentos de identificación fallidos en un corto espacio de tiempo proporcionando el lugar donde ocurrió, el número de intentos y el espacio temporal entre ellos.

        - El tiempo de respuesta entre la identificación del usuario y su validación y registro de la hora en la que lo ha realizado no puede ser superior a 3 segundos.
        - Los lectores de huellas deben ser compatibles con el sistema operativo Android para poder instalarlos en las tablets de la empresa.
        - El lenguaje de programación será Android puesto que el sistema se implantará en una tablet.
    - Módulo de control de acceso.
        - Este módulo deberá estar disponible las 24 horas con el objetivo de controlar, en todo momento, los accesos a las diferentes áreas del edificio.
        - El sistema registrará los intentos de acceso satisfactorios y fallidos.
        - El sistema deberá de reportar los casos en los que un trabajador intente acceder a una área restringida más de dos veces. Para ello aportará sus respectivos datos, la zona en cuestión, el número de intentos y el tiempo invertido.
        - El sistema verificará el estado de los lectores de huellas situados en las puertas de cada zona y notificará a los administradores acerca de un mal uso o/y funcionamiento.
        - La tasa de errores deberá ser inferior al 1% del total de registros de accesos.
        - El tiempo de respuesta desde que el usuario se identifica hasta que se abre la puerta a la zona particular no puede superar los 2 segundos.
        - Solo los administradores podrán acceder a los datos relativos al acceso de las zonas del edificio en modo lectura.
        - El lenguaje de programación será Android puesto que el sistema se implantará en una tablet.
    - Módulo de gestión de tareas.
        - Este módulo se encontrará disponible solo durante la jornada laboral.
        - Cada trabajador solo podrá acceder a sus tareas asignadas en modo lectura, excepto el jefe de cada departamento que podrá acceder solo a las tareas de los trabajadores a su cargo tanto en modo lectura como edición.
        - Los trabajadores solo podrán acceder a sus correspondientes tareas tras haberse identificado correctamente y haber fichado al comenzar su jornada laboral.
        - El sistema almacenará un registro acerca de las modificaciones realizadas en las tareas guardando, para ello, el autor, la tarea en cuestión, el trabajador asignado a ella y los campos que ha cambiado.
        - Este sistema deberá comprobar la consistencia e integridad de los datos de cada tarea antes de realizar una operación sensible, como dar por finalizada una actividad.
        - El tiempo de respuesta ante cualquier operación no puede ser superior a 1 segundo.

    - El módulo notificará a los administradores si se produce un mal uso y/o funcionamiento del mismo.
    - El lenguaje de programación será Android puesto que el sistema se implantará en una tablet.
    - Se incluirán mecanismos para guardar el estado de una operación en caso de que se quede incompleta.

- Conexiones y redes. Los requisitos administrativos de los medios de comunicación entre los componentes del sistema son los siguientes.
    - Todas las transferencias de datos y comunicaciones entre los servidores de datos y de aplicación deberán estar encriptadas utilizando algoritmos como RSA o AES.
    - Se configurará un cortafuegos para cada uno de los puntos de acceso a la red local para monitorizar el tráfico y detectar anomalías en el flujo de paquetes.

- Tablets. Los requisitos asociados a estos dispositivos se detallan a continuación.
    - Solo se podrá acceder a cada dispositivo a través de la huella dactilar.
    - Las tablets solo podrán conectarse a la red local del edificio.
    - Solo los administradores podrán instalar aplicaciones.
    - Se prohibirá el acceso a ciertas páginas webs como redes sociales, videojuegos online, plataformas de contenido audiovisual, páginas con contenido sensible, entre otras.
    - Todas las tablets tendrán activa la localización para comprobar su posición en todo momento y controlar que los usuarios se las lleven fuera del edificio.
    - Los dispositivos dispondrán de un cortafuegos configurado para filtrar el tráfico así como un sistema de antivirus que lo proteja frente a posibles amenazas.
    - Serán capaces de notificar su estado actual y reportar excepciones a los administradores cuando se produzca un mal uso y/o funcionamiento.

- Lectores de huella. Los requisitos relacionados con su rendimiento o modo de funcionamiento se describen a continuación.
    - Tanto los incorporados en puertas como en las tablets deberán de identificar al usuario en menos de 3 segundos.
    - Deben ser compatibles con el sistema operativo Android para su gestión desde el sistema.
    - Proporcionarán una retroalimentación acústica o/y vibratoria dependiendo de si el usuario ha sido identificado correctamente o no, con el objetivo de hacerle conocer el resultado de dicha operación.

Una vez han sido establecidos los requisitos y restricciones en torno a los elementos que componen la arquitectura tecnológica, procedemos a detallar las cualidades del entorno en el que se incluirá el sistema.

4.2. Entorno Tecnológico

En esta etapa se definen los recursos necesarios para dar soporte al nuevo sistema de información, incluyendo una planificación de la evolución de los mismos en un futuro. El objetivo consiste en adquirir componentes y servicios cuya duración sea máxima.

Comenzamos analizando las necesidades de almacenamiento del sistema en cuestión. Para implementar y configurar los nodos en los servidores de datos vamos a montar un cluster utilizando la herramienta *MySQL Cluster*. A través de ella podremos definir las direcciones de los servidores de datos que almacenarán la información y los servidores de aplicaciones que serán los que accedan a dichos datos.

Si bien se trata de una base de datos distribuida cabe destacar que en ella se almacenarán los datos respectivos a los tres subsistemas identificados. Como todos ellos demandan un gran número de peticiones de lectura y escritura, especialmente los de control de horarios y accesos, se utilizarán discos SSD para almacenar los datos que generen. La razón de ello reside en la rapidez de este tipo de tecnología frente a los discos duros convencionales. No obstante, para agilizar las lecturas de las actividades se almacenarán en memoria las tareas del día de todos los trabajadores. De este modo, se vacía la memoria y se cargan las tareas del día al comienzo de la jornada laboral de cada trabajador. Así conseguimos agilizar la operación más frecuente de este módulo: las consultas.

En segundo lugar procedemos a estudiar los requisitos de procesamiento para el sistema de información. Como ninguno de los tres subsistemas realiza tareas computacionalmente costosas, prevemos que las prestaciones de los procesadores AMD de los servidores serán suficientes para el buen funcionamiento del sistema de información. Para que su uso sea eficiente energéticamente se incluirá en cada uno de los servidores un balanceador de carga que sea capaz de activar y desactivar núcleos en función de la demanda del sistema.
En cuanto a las estaciones de trabajo también consideramos que los portátiles adquiridos cubrirán los requisitos de administración necesarios para gestionar los sistemas de forma adecuada, por lo que esperamos que estos equipos se adapten a la evolución de la administración del sistema.

Por último, relativo a los esquemas de comunicación cabe destacar que la topología de la red local (LAN) será de malla de modo que todos los nodos se encuentren conectados entre sí con el objetivo de agilizar las comunicaciones entre ellos puesto que permite el envío de un mensaje por diferentes caminos. Asimismo, esta estructura ofrece cierta robustez puesto que el fallo en un nodo no provoca la caída de la red al completo.
Esta red consta de una línea de comunicación formada por dos enlaces redundantes de 100MB con la posibilidad de aumentar este ancho de banda hasta los 600 MB. También dispondrá de las principales medidas de seguridad como la inclusión y configuración de firewalls y encriptación de datos extremo a extremo.
El sistema operativo de red elegido será el OS/2 Warp Server Advanced puesto que es multiplataforma, permite la conexión con todos los servidores con el uso de una única contraseña, dispone de numerosas aplicaciones de administración como de distribución e

inventario de software y hardware, así como monitorización del rendimiento de la red, ficheros y estaciones conectadas a esta.
Los switches adquiridos serán capaces de adaptarse a los requisitos futuros del sistema puesto que disponen de un número considerable de puertos como para añadir más equipos conectados a la red en caso de que, en un futuro, fuese necesario.

4.3. Requisitos de operación y seguridad

En esta etapa se pretenden especificar los requisitos asociados con las medidas de seguridad, tanto asociadas a los datos como al sistema, que se van a implantar así como las relacionadas con las diferentes operaciones que el propio sistema puede realizar.

- Control de acceso al sistema y sus recursos.
    - Se definirán cuatro grupos de usuarios en función de los recursos a los que pueda acceder, las operaciones habilitadas en función de su rol y los permisos asociados al mismo.
        - Desarrolladores. Este grupo de usuarios tendrá acceso al gestor de la base de datos con permisos de adición, modificación y eliminación de la estructura del sistema. De igual forma también dispondrá del código fuente de los tres módulos, diseños, análisis, catálogo de requisitos, planificación del desarrollo, pruebas y sus resultados.
        - Administrador. Este colectivo tendrá acceso tanto a los servidores de datos como a los de aplicación. En el primer caso podrán acceder a toda la información almacenada pero solo con permisos de lectura, para evitar modificaciones no deseadas.
          En el caso de los subsistemas podrán acceder a sus recursos y herramientas proporcionadas para la monitorización, gestión y administración de los mismos. Asimismo dispondrán de acceso a los *logs* de los subsistemas y a la administración de los usuarios que hacen uso de estos, posibilitando el registro, la gestión y eliminación de sus cuentas.
        - Gestores. Este grupo de usuarios se corresponden con los respectivos jefes de departamento que tendrán acceso tanto a su información como a los datos asociados con los miembros a su cargo. Podrán añadir, modificar y eliminar tareas sin finalizar pero no realizar estas operaciones sobre datos que haya proporcionado el trabajador, como por ejemplo comentarios, estado de finalización, entre otros.
          En relación a los sistemas, este colectivo deberá hacer uso de los los sistemas de control de horario para fichar al comienzo y al acabar su jornada laboral además de identificarse para entrar a las áreas habilitadas del edificio.
        - Trabajadores. Por último en este grupo se encontrarán los miembros de la plantilla que solo tendrán acceso a sus propios datos, también en modo lectura, y que podrán interactuar con sus tareas asignadas sin la posibilidad de añadir, editar y eliminarlas. Asimismo, deberán hacer uso de los sistemas de control de horarios y acceso a las zonas del edificio al igual que el grupo anterior.

- Los controles de acceso a los recursos físicos, como la sala del CPD, se llevan a cabo mediante el subsistema de control de acceso utilizando, para la identificación, lectores de huella.
- Para realizar un mayor control de los recursos físicos se instalarán cámaras de vigilancia en pasillos y áreas del edificio que contengan materiales de alto valor, como la zona de I+D.
- Se incluirán herramientas de seguridad, como *firewalls* y antivirus, con el objetivo de evitar accesos no autorizados en el sistema y recursos virtuales.
- Se hará uso de programas especializados en el bloqueo temporal del acceso a los recursos software, físicos y sistemas en caso de detectar intentos fallidos de accesos no autorizados.

- Integridad y privacidad de los datos.
  - Cada usuario podrá acceder solamente a la información autorizada en función de su rol asignado en el sistema.
  - Los datos de carácter sensible serán cifrados mediante el algoritmo RSA.
  - Las transferencias de datos de cualquier naturaleza serán encriptadas
  - Los datos asociados a los registros de horarios o de acceso a las áreas del edificio no se podrán modificar bajo ningún concepto. Igualmente, la información personal asociada a un trabajador solo podrá ser modificada bajo su autorización.
  - Cada registro de la base de datos deberá de contar con un identificador único que lo diferencie del resto.
  - Se añadirán las comprobaciones necesarias para verificar la existencia de un registro que es referenciado por otro.
  - La operación de borrado deberá implementar una actualización en cascada de modo que si se elimina un registro también se borren sus referencias.
  - Se garantiza la completitud de los datos incluyendo medidas para obligar a rellenar los campos necesarios para considerar que el registro contiene información completa, como por ejemplo los datos personales básicos de los trabajadores.
  - Para garantizar la precisión de los datos se realizarán comprobaciones mensuales de los datos almacenados con el objetivo de verificar que son válidos y realizar las correcciones oportunas.
  - Se analizarán las fuentes de las que provienen los datos antes de ser almacenados como registros en la base de datos.
  - Se llevarán a cabo pruebas de auditoría periódicas para analizar la evolución y modificaciones que se han realizado sobre los datos indicando quién lo ha realizado, qué es lo que ha cambiado, cuándo y su respectivo motivo.

- Copias de seguridad y recuperación de datos.
  - Se realizará una copia de seguridad del sistema completo la primera vez que se lance este proceso. El objetivo es disponer de una copia de la información más relevante del sistema inicial, como los datos actuales, ficheros de configuración y administración.

    - El resto de copias de seguridad que se realicen periódicamente solo guardarán los cambios realizados en los datos.
    - Se lanzarán tres copias de seguridad simultáneas durante los fines de semana para respaldar los nuevos datos de los tres subsistemas.
    - Las copias de seguridad en la nube serán cifradas para proteger los datos en caso de accesos no autorizados.
    - Las copias de seguridad serán comprimidas al máximo, dependiendo del servicio cloud, de modo que ocupen el menor espacio posible.
    - Todos los servidores de datos dispondrán de discos RAID para almacenar una copia actualizada de los datos. Este sistema nos permitirá tanto recuperar información como garantizar el funcionamiento de los servidores de datos en caso de que surgiese un fallo en el disco principal.

- Recuperación frente a catástrofes.
    - Uso del servicio AWS Backup para la programación, realización, administración y almacenamiento de las copias de seguridad del sistema.

4.4. Datos del sistema

En este apartado se detallarán todos los aspectos relacionados con la estructura física de los datos, las herramientas a usar para su administración segura, la distribución del almacenamiento de los mismos así como la inicialización de la información necesaria para que el sistema pueda ser puesto en funcionamiento.

En primer lugar procedemos a especificar el modelo de datos por el cual detallamos la estructura física en la que se va a organizar y almacenar toda la información del sistema. Este esquema se encuentra compuesto por siete nodos en los que se almacenan los datos asociados particulares a las entidades involucradas en el sistema así como las relaciones existentes entre las mismas, tanto en forma de claves externas como en tablas independientes en el caso en el que la relación contemple un uno-muchos como es el caso de las tareas, que pueden tener varios empleados asignados.

Tabla “**HORARIO**”.

- *ID*. Identificador único, de asignación automática e incremental para identificar cada jornada laboral de forma unívoca. *Tipo*: entero. Clave primaria.
- *HoraEntrada*. Hora de comienzo de la jornada laboral. *Tipo*: time.
- *HoraSalida*. Hora de finalización de la jornada laboral. *Tipo*: time.
- *TiempoDescanso*. Tiempo de descanso total que se toma el empleado dentro de la jornada laboral completa. *Tipo*: timedelta.

Tabla “**EMPLEADO**”.

- *Nombre*. Nombre del empleado de la organización. *Tipo*: varchar(60).
- *DNI*. Número identificativo del empleado de la organización. *Tipo*: varchar(9). Clave primaria. Índice.
- *Departamento*. Nombre del departamento de la empresa en el que está destinado. *Tipo*: varchar(100).

- *Puesto*. Cargo que ocupa el empleado dentro de la organización. *Tipo*: varchar(100). Índice.
- *Permisos*. Permisos con los que accede al sistema dependiendo del rol asociado a su usuario. *Tipo*: varchar(100).
- *Horarios*. Jornada laboral asociada al empleado. *Tipo*: entero. Clave foránea a la tabla "HORARIO".

Tabla "**ESTADO"**.
- *ID*. Identificador único, de asignación automática e incremental para identificar un estado. *Tipo*: entero. Clave primaria.
- *Nombre*. Nombre representativo del estado. *Tipo*: varchar(20).
- *Descripción*. Descripción de la situación que plantea el estado. *Tipo*: varchar(100).

Tabla "**DEPARTAMENTO**".
- *ID*. Identificador único, de asignación automática e incremental para identificar un departamento. *Tipo*: entero. Clave primaria.
- *Nombre*. Nombre del departamento. *Tipo*: varchar(20). Índice.
- *Descripción*. Descripción del objetivo del departamento, el funcionamiento, las funciones que desempeñan, entre otros. *Tipo*: varchar(200).
- *Miembros*. Número de trabajadores que pertenecen al departamento. *Tipo*: entero.

Tabla "**TAREA**".
- *ID*. Identificador único, de asignación automática e incremental para identificar una tarea. *Tipo*: entero. Clave primaria.
- *Título*. Título de la tarea con el que expresar la idea general de la funcionalidad a llevar a cabo. *Tipo*: varchar(50). Índice.
- *Departamento*. Identificador del departamento al que se asocia la tarea. *Tipo*: entero. Clave foránea a la tabla "DEPARTAMENTO".
- *Descripción*. Descripción de las funcionalidades y restricciones a ejecutar para poder cumplir la tarea. *Tipo*: varchar(500).
- *DuraciónPrevista*. Duración estimada para completar la tarea. *Tipo*: datetime.
- *DuraciónFinal*. Tiempo invertido final en realizar la tarea. *Tipo*: datetime.
- *Estado*. Estado descriptivo del desempeño del trabajador en la tarea. *Tipo*: entero. Clave foránea a la tabla "ESTADO".
- *Comentario*. Texto que puede añadir el trabajador para realizar algún tipo de observación con el objetivo de que sea visualizado por el supervisor. *Tipo*: varchar(200).

Tabla "**TAREA_EMPLEADOS**".
- *ID*. Identificador único, de asignación numérica e incremental para identificar cada relación entre una tarea y sus empleados asociados.
- *Empleado*. Identificador del empleado que está asignado a una tarea. *Tipo*: entero. Clave foránea a la tabla EMPLEADO.
- *Tarea*. Identificador de la tarea de la que se definen los empleados asociados a ella. *Tipo*: entero. Clave foránea a la tabla TAREAS.

Tabla “**CONTROL_HORARIOS**”.

- *ID*. Identificador único, de asignación automática e incremental para identificar cada registro de horario. *Tipo*: entero. Clave primaria.
- *Empleado*. Identificador del empleado que ha realizado el registro de horario. *Tipo*: entero. Clave foránea a la tabla EMPLEADO. Índice.
- *Entrada*. Fecha y hora a la que el empleado ha realizado el registro del horario de su jornada laboral. *Tipo*: datetime.
- *Salida*. Fecha y hora a la que el empleado ha realizado el registro de salida y finalización de su jornada laboral. *Tipo*: datetime.

Tabla “**CONTROL_ACCESO**”.

- *ID*. Identificador único, de asignación automática e incremental para identificar cada registro de acceso a un área del edificio. *Tipo*: entero. Clave primaria.
- *Empleado*. Identificador del empleado que ha realizado el acceso. *Tipo*: entero. Clave foránea a la tabla EMPLEADO. Índice.
- *Entrada*. Fecha y hora en la que el empleado ha realizado el intento de acceso a un área del edificio. *Tipo*: datetime.
- *Area*. Zona en la que se ha realizado el registro de acceso. *Tipo*: varchar(20).
- *Estado*. Este campo registra si el intento de acceso ha sido satisfactorio o fallido. *Tipo*: booleano.

Como se comentó anteriormente, las estructuras de datos anteriormente descritas junto con su información asociada serán almacenadas en los discos SSD de los servidores de datos. Para ello haremos uso del motor de almacenamiento de MySQL denominado *Federated*, el cual facilita la creación de una misma base de datos **distribuida y homogénea** de manera que se almacene en varias máquinas pero que todos los nodos tengan en común un único gestor de bases de datos. Este, tal y como comentamos anteriormente, será *MariaDB* en el modo compatible con el lenguaje SQL.
En relación al tipo de almacenamiento hemos escogido la técnica basada en *fragmentación,* de filas y columnas, puesto que es la que permite dividir una tabla para almacenar cada segmento en un nodo. De este modo si cae uno, no se pierden todos los datos y además distribuimos el espacio que ocupa la información entre los servidores de datos.
Para el respaldo de los nodos se configurarán discos RAID 1 de modo que cada disco de los servidores de datos tengan su disco espejo en el que se almacenan de manera síncrona todos los datos duplicados. Además de ser el más barato es también el más eficaz y recomendado para bases de datos por su redundancia de datos completa.
El sistema RAID será controlado por *software* de modo que no se necesite hardware adicional para conectar los discos y sea fácilmente ampliable y configurable.

Una vez disponemos del modelo físico de datos y su organización para distribuirlos en disco, procedemos a detallar los procesos por los cuales llevar a cabo la **inicialización de la información** necesaria para el primer funcionamiento del sistema. Cabe destacar la diferencia entre los datos necesarios para la puesta en marcha de los distintos módulos y los **datos de prueba** asociados a efectuar la fase de validación de los mismos. En sendos casos, como nuestro sistema es novedoso dentro de la empresa no existe información que podamos reutilizar. Es por ello por lo que deberemos generarlos mediante procesos

automatizados cuyas fuentes de datos dependerán del subsistema al que se encuentren asociados así como del objetivo para que vayan a ser usados.

En primer lugar describiremos el proceso asociado a los datos necesarios para comenzar con el funcionamiento real del sistema. La primera tarea consiste en insertar la información asociada a los empleados y a la propia organización, como sus datos personales, horarios, departamentos existentes y los estados en los que puede estar una tarea. Los datos asociados a los trabajadores se pueden recoger mediante un formulario común de forma que cada empleado lo rellene personalmente. Para cada campo se añaden las restricciones propias de los tipos de datos que se esperan, el rango de valores posibles en aquellos casos en los que se pueda especificar, entre otros. Este primer formulario se encontrará disponible dentro de los servidores de aplicación para que toda la organización pueda acceder a él.
Tras la recopilación de la información se realizará el procesamiento de estos datos en busca de posibles inconsistencias. Para ello se desarrollarán una serie de *scripts* con los que componer los diversos procesos de análisis textual y numérico con el fin de realizar las comprobaciones anteriores además de otras asociadas a la sintaxis, semántica, etc. En el caso de que se descubra algún tipo de error, el usuario deberá realizar los cambios correspondientes para comenzar de nuevo el análisis. Si se supera el límite de intentos, se bloqueará el proceso y se notificará al responsable del mismo para el estudio de la situación.

Además de un procesamiento automático, el responsable de este proceso también deberá verificar personalmente los datos introducidos por los trabajadores para garantizar su veracidad y completitud. Una vez se hayan aprobado sendos análisis, se procede a ejecutar el procedimiento de inserción de la información en la base de datos. Este también es automático y consiste en añadir los datos preprocesados a la tabla correspondiente. Para ello cada tipo de dato se guarda previamente en una estructura de datos diferente con el fin de facilitar la inserción de los datos en el sistema de almacenamiento.
Para recopilar la información asociada tanto a la empresa como a los horarios de los trabajadores se llevará a cabo un procedimiento similar al anterior. La diferencia es que, en este caso, serán los directivos de la organización los que introduzcan los datos mediante un formulario diferente al anterior. Asimismo, tras el análisis automático serán ellos los responsables de verificar personalmente la información introducida antes de su almacenamiento.

En relación al acceso y modificación de los datos iniciales, la información personal de los trabajadores podrá ser consultada por los directivos de la organización y por los propios trabajadores en modo lectura. Estos datos solo podrán ser modificados por los mismos empleados bajo autorización y supervisión, tras lo cual se analizará de nuevo la información al completo aplicando el procedimiento anterior. Mientras que los horarios almacenados de los empleados los podrá consultar tanto los directivos, jefes de departamento así como el propio trabajador asociado. Del mismo modo ocurre con la información relativa a los departamentos y los posibles estados de las tareas. Ambos tipos de datos solo podrán ser modificados por los directivos de la empresa también bajo autorización, supervisión y aplicando de nuevo el análisis correspondiente.

Para finalizar cabe destacar que tanto los datos asociados con las tareas, registro de horarios y acceso serán generados conforme se vayan utilizando los sistemas por lo que no es necesario producir este tipo de información para comenzar el funcionamiento del sistema.

En principio el almacenamiento de la información asociada a los empleados y sus correspondientes horarios será constante, a menos que se realicen contrataciones de personal. En este caso los horarios muy probablemente seguirán siendo los mismos, mientras que en la tabla de empleados habría que añadir un registro por cada nuevo trabajador, lo cual tampoco supone una necesidad de almacenamiento considerable.

El segundo conjunto de información que se debe generar es conocido como los **datos de prueba**. Estos tienen la misma estructura que los anteriores de modo que solamente se producirán aquellos relacionados con los empleados, sus horarios, los departamentos de la empresa y los distintos estados en los que puede encontrarse una tarea. A diferencia del procedimiento anterior, este será generado de forma automática aplicando unas directrices diferentes. El objetivo es generar, en primer lugar, un conjunto de datos inusuales que pongan a prueba la tolerancia de fallos del sistema. De este modo se podrá analizar su comportamiento cuando reciba datos que no cumplan las condiciones esperadas. Generalmente este tipo de información suelen producir problemas comunes referentes a los tipos de datos y al espacio que ocupan, como por ejemplo *overflow*.
Sin embargo, también se suele utilizar información considerada como habitual y dentro de las características esperables para explorar las diversas ramas de cada una de las funcionalidades del sistema. De nuevo, se utilizarán programas automatizados para generarlos de modo que se consideren las estructuras físicas de datos especificadas anteriormente.

4.5. Entornos de construcción y de pruebas

El cometido de los administradores en esta fase consiste en proporcionar las herramientas necesarias para comenzar la implementación y el testeo del sistema. Para ello deben considerar el diseño previamente definido y el entorno en el que se encontrará el mismo. Comenzamos definiendo los recursos para el desarrollo del sistema para luego detallar los de validación.

4.5.1. Entorno de construcción

Se habilitará una oficina particular para los desarrolladores en la que dispondrán de sus respectivos portátiles. Se ha creído conveniente adquirir el mismo modelo seleccionado para las estaciones de trabajo de los administradores puesto que cuentan con recursos *hardware* suficientes para facilitar el desarrollo del sistema.

En cuanto a los recursos *software* los propios equipos ya cuentan con un sistema operativo compatible con la mayoría de herramientas de desarrollo y construcción por lo que no será necesario incorporar un segundo sistema. Dependiendo de los lenguajes de programación que se vayan a utilizar para codificar el sistema se deberán adquirir las correspondientes

licencias e instalar las librerías de los mismos, sus correspondientes IDE y/o editores de texto que les facilite la codificación. Del mismo modo se deberá proceder con las bibliotecas o *software* de terceros que se vayan a incorporar al sistema de forma que todo se encuentre disponible en los equipos de los desarrolladores antes de comenzar la codificación.
Con el objetivo de llevar un control de versiones y situar el código de los subsistemas en una plataforma *cloud* que sea visible para todos los desarrolladores, se instalarán los clientes necesarios para mantener repositorios privados de la empresa de modo que solo sus miembros puedan visualizar los progresos de los módulos.
Por último se instalará y configurará la herramienta *AWS Backup* que utiliza la empresa para la realización y administración de copias de seguridad de los equipos de los desarrolladores hasta que finalicen sus trabajos.

En relación a las comunicaciones se deberá de configurar en todos los equipos el acceso a la red local de la empresa para que dispongan de conexión a Internet. Para ello harán uso del router inalámbrico instalado en la planta en la que se encuentre su oficina.
Se les proporcionará acceso al servidor de datos en el que se encuentre instalado el SGBD para que puedan implementar los procedimientos almacenados de inserción, modificación y borrado de modo que estas operaciones solo se implementen una vez pero se utilicen tantas como se necesiten.

Para finalizar detallaremos a continuación los requisitos de operación y seguridad enfocados al entorno de construcción.

- Control de acceso al sistema y sus recursos.
    - Cada equipo dispondrá de los credenciales que aporte su usuario y solo se podrá acceder a él proporcionando estos datos. Por lo que cada programador solo podrá acceder a su portátil.
    - Los propios desarrolladores podrán configurar su equipo para que ellos mismos sean los administradores del mismo.
    - Se instalarán herramientas de seguridad en cada equipo como *firewalls*, antivirus, entre otros para protegerlos de intrusiones y ataques.

- Integridad y privacidad de los datos.
    - Cada desarrollador tendrá acceso solo a los datos de su propio equipo.
    - Para tener acceso a la información de la base de datos deberán de firmar un acuerdo de confidencialidad por el cual se le prohíbe hacer un uso indebido de los datos así como publicarlos, entre otras acciones.
    - Solo podrán consultar la información de la base de datos pero no aplicar ninguna operación que suponga su modificación.
    - Podrán acceder a la estructura de las tablas de la base de datos pero sin añadir, modificar o eliminar campos.
    - Tras cada procedimiento almacenado de inserción, modificación y borrado en la base de datos deberán de añadir uno adicional para comprobar que la operación se ha realizado correctamente. En caso contrario se deberá volver al estado anterior.

- Copias de seguridad y recuperación de datos.

- Se programarán copias de seguridad periódicas de los datos más relevantes de cada equipo así como su configuración.
- Se configurarán en todos los equipos la generación de puntos de restauración para devolver el equipo a un estado anterior en caso de que se hayan perdido datos o surja algún problema con el equipo.
- En cada jornada laboral todos los desarrolladores deberán subir el código actualizado de los módulos a la plataforma *cloud* para así evitar perder el trabajo realizado,

- Recuperación frente a catástrofes.
    - Las copias de seguridad se realizarán utilizando el servicio *AWS Backup* para poder recuperarlas en caso de que sea necesario.
    - Se podrán clonar los repositorios en los que se mantiene el código fuente de los módulos desde la plataforma *cloud* en la que se alojan.

4.5.2. Entorno de pruebas

Dependiendo de los tipos de tests que se vayan a realizar los recursos del entorno de validación serán diferentes. Por ende vamos a especificarlos en función de los diferentes tipos de validaciones que se llevarán a cabo.

- Pruebas unitarias y de integración.
    - Hardware. Los recursos hardware seguirán siendo los mismos que los especificados en el entorno de construcción.
    - Software. Se necesitará la adquisición de las licencias correspondientes y la instalación, si fuese necesaria, de las bibliotecas que se vayan a usar para implementar los tests. Asimismo, se subirán al repositorio los tests unitarios y de integración desarrollados y se incluirán herramientas de Integración Continua para que automáticamente los ejecuten y analicen los resultados.
    - Comunicaciones. Del mismo modo que ocurría con los recursos hardware, los de comunicaciones tampoco se ven alterados.
    - Planificación de las capacidades necesarias. No se esperan cambios en las capacidades de almacenamiento y red puesto que para la primera tanto las pruebas como sus resultados se encontrarán disponibles en la herramienta de CI escogida. Y para el segundo caso se prevé que las necesidades de conexión de red se mantengan constantes.
    - Planificación de la información necesaria. Los datos que se deberán proveer para la realización de los tests son los datos de prueba, explicados anteriormente, así como los casos de uso que indican las operaciones a testear.
    - Requisitos de operación, seguridad y procedimientos de recuperación.
        - Control de acceso al sistema y sus recursos.
            - Los desarrolladores podrán acceder al código fuente del sistema en modo lectura y escritura, mientras que los directivos de la organización solo en modo lectura.
        - Integridad y privacidad de los datos.
            - Solo los desarrolladores y los directivos de la organización podrán acceder a los datos de prueba generados.

        - Los datos de prueba no contendrán información personal veraz ni asociada a los empleados ni a la organización.
        - Los datos de prueba podrán ser modificados por los desarrolladores para adaptarlos a las pruebas.
        - Solo los desarrolladores y directivos de la organización podrán acceder a los resultados de la validación del sistema.
    - Copias de seguridad y recuperación de datos.
        - Se realizará una primera copia de seguridad para almacenar en la nube los datos de prueba generados al comienzo del proceso.
        - Las sucesivas copias de seguridad solo actualizarán los datos que hayan sido modificados.
        - Se realizarán copias de seguridad para mantener los datos de prueba actualizados en la nube con el objetivo de poder reutilizarlos en sucesivos tests.
    - Recuperación y restauración.
        - Uso del servicio AWS Backup para mantener copias de seguridad de los datos de prueba.
        - Posibilidad de recuperar versiones anteriores de los subsistemas gracias a la plataforma cloud elegida para almacenar y administrar los códigos fuentes.

- Pruebas de implantación.
    - Hardware. En esta fase se instalará el sistema completo en los servidores de aplicaciones para integrarlo con su entorno tecnológico.
    - Software. Será necesaria la adquisición de licencias, y en su caso la instalación, de programas y/o librerías orientados a desarrollar los tests de implantación, entre los cuales se incluyen pruebas de seguridad, rendimiento, de operación, recuperación, gestión de copias de seguridad, entre otros.
      Asimismo, se deberán instalar los recursos necesarios en los servidores de aplicaciones para posteriormente instalar el propio sistema. Además, será necesaria la configuración y puesta a punto de la base de datos.
    - Comunicaciones. Se deberá configurar el acceso a los servidores de aplicaciones para que los desarrolladores puedan acceder al sistema y ejecutar los tests desarrollados.
    - Planificación de las capacidades necesarias. En relación a la capacidad de almacenamiento se prevé que vaya disminuyendo conforme el sistema comience a registrar los horarios, accesos y tareas. Sin embargo los discos SSD destinados a su almacenamiento serán suficientes por el momento. La necesidad de conexión de red aumentará conforme se produzca un mayor tráfico de datos entre el sistema y los servidores donde se aloja la base de datos pero con los recursos expuestos anteriormente prevemos que serán suficientes.
    - Planificación de la información necesaria. Los datos de prueba y los casos de uso serán, de nuevo, la información a proporcionar para realizar estas pruebas.

- Requisitos de operación, seguridad y procedimientos de recuperación. Se aplican los mismos requisitos que en las pruebas anteriores.

- Pruebas de aceptación.
  - Hardware. Se emplea el mismo que en las pruebas anteriores.
  - Software. Se desarrollarán las pruebas de aceptación necesarias para verificar que el sistema cumple con los requisitos especificados y que todos los casos de uso definidos se encuentran incluidos en él. Para ello, de nuevo, se adquirirán las licencias de las librerías necesarias para implementar los tests.
  - Comunicaciones. Se emplea el mismo esquema que en las pruebas anteriores.
  - Planificación de las capacidades necesarias. Son las mismas que las especificadas anteriormente.
  - Planificación de la información necesaria. Serán necesarios los datos de prueba, los casos de uso y los requisitos del sistema para comprobar que este los satisface.
  - Requisitos de operación, seguridad y procedimientos de recuperación. Se aplican los mismos requisitos que en las pruebas anteriores.

4.6. Requisitos de implantación

En esta última fase del diseño se detallarán los requisitos asociados a la documentación del sistema, especialmente orientada a los usuarios finales, así como los requisitos de implantación del mismo en la propia organización.

- Documentación de usuario. Consta de un conjunto de documentos en los que se proporciona una visión general del sistema. Para su redacción se utilizarán los estándares básicos de documentación de los manuales de usuario. Estos incluyen información como a quién va dirigida esta documentación, el modo de instalación y configuración así como diversos manuales de iniciación y explicación de las operaciones del mismo, entre otros.

  La documentación será almacenada en un repositorio privado y común a la organización y a los desarrolladores de modo que estos puedan realizar su correspondiente mantenimiento durante el plazo acordado en el contrato. A través de la plataforma *cloud* en la que se aloje el repositorio se podrá llevar a cabo un control de versiones así como de las propuestas de mejora. Solo podrán realizar modificaciones los desarrolladores y directivos de la organización, el resto del personal accederá con permisos de lectura.

- Requisitos de implantación.
  - Nueva infraestructura. Los recursos hardware del sistema son los que se han explicado en la infraestructura tecnológica. En particular, será necesario instalar lectores de huella en las áreas en las que se desee controlar el acceso. Asimismo, se deberá de proveer una tablet con su lector de huella a cada trabajador para llevar a cabo el control de horarios y la gestión de tareas.

En relación a los recursos software será necesaria la instalación de la aplicación asociada al subsistema de gestión de tareas en las tablets de los trabajadores para poder llevar a cabo la creación y administración de las tareas. Asimismo, se deberá configurar el acceso al subsistema encargado del control de horarios para que los trabajadores puedan fichar identificándose con el lector de huellas de su tablet.

- Formación. Para los subsistemas de control de horarios y de acceso no será necesario ningún tipo de formación puesto que para utilizarlos basta con identificarse mediante el lector de huellas, ya sea del área al que se pretende entrar o de la tablet adjunta a cada empleado. Si bien el módulo encargado de las tareas no es complejo, se organizarán diferentes periodos de tiempo en función de las actividades que puede llevar a cabo cada tipo de trabajador.
    - Para los empleados que solo pueden gestionar sus tareas se llevarán a cabo talleres teórico-prácticos durante dos horas diariamente hasta completar una semana. En ellos aprenderán a visualizar sus tareas y las operaciones básicas de gestión como marcar una tarea como completada, escribir observaciones, cambiar el estado de la tarea, entre otras.
    - Para los miembros con capacidad de creación, modificación y eliminación de tareas, se plantean talleres también teórico-prácticos de dos horas diarias durante dos semanas. En ellos se impartirá el mismo contenido que en los otros talleres además de la formación necesaria para dar de alta nuevas tareas, asignarlas a miembros de la organización, modificar sus características, eliminarlas entre otras.

5. Construcción del Sistema de Información (CSI)

5.1. Preparación del Entorno de Generación y Construcción

Se debe asegurar la disponibilidad de todos los medios y facilidades para la construcción del sistema de información. Se deben preparar los puestos de trabajo, equipos físicos y lógicos, gestores de bases de datos, biblioteca de programas, herramientas de generación de código, bases de datos o ficheros de prueba, entre otros.

5.1.1. Implantación de la Base de Datos Física o Ficheros

En esta tarea se implementará la Base de Datos diseñada anteriormente. Esta tarea se realizará junto a los administradores de Bases de Datos.

Se almacenará en la base de datos:

- Huellas dactilares.
- Empleados.
- Estados posibles de las tareas.
- Departamentos del edificio.
- Tareas y su asignación a los empleados.
- Control de los horarios de los empleados.
- Control de acceso de los empleados.

Se utilizará una base de datos SQL distribuida y homogénea con MariaDB. Se generarán las tablas diseñadas y los usuarios que podrán acceder a ellas junto a sus permisos. Se debe conocer el espacio de almacenamiento que se usará en los dispositivos de almacenamiento SSD y inicializar la base de datos cargando los datos necesarios.

5.1.2. Preparación del Entorno de Construcción

En este apartado se asegurará la disponibilidad de todas las herramientas necesarias para poder llevar a cabo la construcción del sistema de información:

- Preparar puestos de trabajo.
- Equipos físicos y lógicos.
- Gestores de Bases de Datos.
- Bibliotecas de programas.
- Herramientas de generación de código.
- Bases de Datos de prueba.

Los desarrolladores trabajarán con sus portátiles por lo que será muy útil el uso de alguna herramienta para instalar automáticamente todas las herramientas necesarias, como programas, bibliotecas, lenguajes de programación, editores de texto, gestores de bases de datos, etc con sus respectivas versiones. Para ello se puede usar alguna herramienta como Ansible, con la que los trabajadores tendrían un playbook almacenado en el repositorio privado de la empresa. De esta forma los trabajadores pueden automatizar la instalación al

comienzo de su jornada laboral y al no ser accesible por todo el mundo, se estaría protegiendo de dar a conocer a los atacantes los programas que están utilizando los desarrolladores junto a sus versiones. Habrá un playbook para cada tipo de desarrollador. Por ejemplo, para los encargados de realizar tests, existirá un playbook con el que se descargarán herramientas para ese propósito y se inicializará una Base de Datos con datos de prueba. En esta automatización también se instalará y configurará la herramienta AWS Backup para administrar las copias de seguridad.

Los ordenadores de los desarrolladores se podrán conectar a la red local de la empresa mediante un router inalámbrico instalado en la planta de su oficina. Solo podrán acceder estos ordenadores, haciendo uso de algún control como puede ser el filtrado por MAC.

5.2. Generación del Código de los Procedimientos de Operación y Seguridad.

En esta tarea se abordará la generación de los procedimientos de operación y administración del sistema de información, así como los procedimientos de seguridad y control de acceso , necesarios para ejecutar el sistema una vez que se haya implantado y esté en producción.

Los desarrolladores deberán de seguir unos procedimientos de seguridad. Estos procedimientos estarán bien establecidos y documentados para que los desarrolladores puedan entenderlos perfectamente y además puedan volver a ser revisados tantas veces sea necesario.

En estos procedimientos se incluirán aspectos como:

- Tener credenciales fuertes en su ordenador de trabajo
- Tener firewall y antivirus instalado y activado
- Tener configurado el antivirus para que haga una inspección del sistema de archivos al acabar la jornada laboral
- Utilizar únicamente sus propios ordenadores
- Crear copias de seguridad con AWS Backup.
- Subir el código generado al repositorio al finalizar el día.

Además de estos procedimientos, cada cierto tiempo se realizarán cursos sobre seguridad básicos en los que los trabajadores aprenderán a tener unas pautas de seguridad básicas. Estos cursos serán visualizados por los desarrolladores de manera online. También se realizarán pequeños cursos a medida que se vayan descubriendo nuevas estrategias para combatir riesgos nuevos.

5.3. Preparación del Entorno de Pruebas

Se prepararán todos los recursos necesarios para poder trabajar en la realización de las pruebas de cada uno de los componentes del sistema de información.

Se asegurará la disponibilidad del entorno

- Los desarrolladores deberán de ejecutar el playbook correspondiente localizado en el repositorio privado al comenzar su jornada laboral de forma que se instalen todos los programas y versiones necesarias para poder realizar su trabajo.

Datos necesarios para ejecutar las pruebas

- Los datos de prueba se encontrarán cargados en la base de datos de prueba de forma que los desarrolladores puedan acceder a estos datos para realizar los tests.
- Una vez instaladas todas las herramientas se ejecutarán tests dedicados a comprobar la disponibilidad de la base de datos de prueba. De forma que se asegure que la Base de Datos sea accesible y están cargados los datos de prueba correctamente.

Preparar bibliotecas

- Las bibliotecas necesarias serán instaladas automáticamente al instalar todas las herramientas necesarias con Ansible.

Procedimientos manuales o automáticos.

- La instalación de aplicaciones y bibliotecas se hará automáticamente al ejecutar manualmente el playbook de Ansible.
-

Pruebas Unitarias

Los desarrolladores tendrán que ejecutar el playbook correspondiente de forma que tengan disponibles todas las herramientas para poder realizar los tests unitarios localmente para comprobar que todo funciona correctamente antes de subir el nuevo código al repositorio, donde automáticamente se ejecutarán de nuevo los tests para verificar que todo funciona como se esperaba.

Se crearán varios grupos entre los desarrolladores, creando un grupo por cada uno de los distintos subsistemas existentes. Cada grupo se centrará únicamente en el desarrollo de las pruebas unitarias pertenecientes a ese subsistema.

Pruebas de Integración

En este apartado los desarrolladores deberán realizar tests de integración, comprobando la correcta comunicación entre los subsistemas. El playbook a ejecutar debe contener, además del código para instalar todas las herramientas y bibliotecas necesarias, código para levantar una versión de prueba de cada subsistema de forma que el desarrollador pueda comprobar si la comunicación entre subsistemas es correcta a partir de los tests que se desarrollen.

Los desarrolladores que se encarguen de las pruebas de integración, desarrollarán cerca de los demás desarrolladores para tener un mejor conocimiento de las comunicaciones que existen entre los diferentes subsistemas y poder resolver las dudas que se puedan producir de una forma más eficaz.

Pruebas del Sistema

En el entorno de pruebas del sistema deberá existir las herramientas necesarias para testear el sistema software completo, con todos los subsistemas integrados.

En este tipo de pruebas, el playbook debería de desplegar una versión del software completo que utilizase datos de prueba. También instalaría más herramientas específicas para estos tipos de prueba como pueden ser herramientas para realizar pruebas de carga, prueba de estrés, etc.

5.4. Preparación del Entorno de Migración y Carga Inicial de Datos

Se dispondrá el entorno en el que se construirán los componentes y procedimientos de migración y carga inicial de datos.

Migración

Hay que preparar un entorno de migración para poder actuar en caso de tener que cambiar la localización física de los datos. Se tendrá que preparar scripts de automatización para desplegar la Base de Datos tanto en el CPD de la empresa como en Cloud. Se deberá de preparar la automatización del despliegue de la Base de Datos en servicios Cloud de varios proveedores, como pueden ser AWS, Azure y Google Cloud. Además también se deben tener preparados varios scripts para poder pasar toda la información almacenada a varios gestores de bases de datos diferentes, como puede ser MariaDB, que es el que se utilizará normalmente, MongoDB, PostgreSQL, o algún otro. Además de tener scripts de aprovisionamiento para aprovisionar al servidor de los gestores de Bases de Datos y las bibliotecas que necesiten. Además se deberá cargar toda la información que se ha almacenado hasta el momento.

Para realizar todas estas tareas los desarrolladores tendrán que crear varios playbook de Ansible para poder obtener automáticamente todas las herramientas y bibliotecas necesarias. Estos playbook estarán almacenados en el repositorio privado de la empresa. De esta forma, cuando los trabajadores vayan a comenzar a trabajar sólo deberán ejecutar el playbook para tener sus máquinas listas para trabajar con las herramientas y bibliotecas necesarias.

Carga Inicial

En un principio la empresa solo tiene los datos de los empleados. Por lo que habría que crear las demás tablas (HORARIO, ESTADO, DEPARTAMENTO, TAREA, TAREA_EMPLEADOS, CONTROL_HORARIOS, CONTROL_ACCESO) , que tendrían que ser rellenadas por los jefes de departamentos. En la carga inicial de los sistemas solo se incluirá la información de los empleados y la empresa. Los empleados rellenarán un formulario con sus datos. Se comprobará que los datos introducidos son correctos y se insertarán en el sistema.

6. Implantación y Aceptación del Sistema (IAS):

En esta sección se indicarán las actividades previas al inicio de la producción.

6.1. Establecimiento del plan de implantación

Se identifican los distintos subsistemas, analizando posibles dependencias con otros proyectos, que puedan condicionar el plan de implantación. Se constituirá el Equipo de Implantación, determinando los recursos humanos necesarios junto a sus perfiles y niveles de responsabilidad.

6.1.1. Definición del plan de implantación

Se realizará un plan de implantación en el que se seguirá un determinado orden. En primer lugar, se formará a los miembros de los diferentes equipos para que entiendan perfectamente su labor en la tarea de la implantación. Ocasionalmente se deberán de ayudar los miembros de diferentes equipos para informar a los demás sobre qué aspectos de su entorno deben de tener en cuenta. Una vez que se han planteado correctamente los cambios necesarios, se prepara toda la infraestructura para poder realizarlos. Después se instalan los componentes y se realiza una carga inicial de datos en la Base de Datos de prueba, puesto que los datos en producción se generarán una vez el sistema esté en marcha. Finalmente se formará el plan de mantenimiento.

6.1.2 Especificación del equipo de implantación

El equipo de implantación estará formado por:

- Encargados del CPD: Serán el administrador de servidores y el administrador de la Base de Datos, que son los únicos que tienen permiso para poder acceder al CPD.
- Desarrolladores del software: En la etapa de implantación solamente deberán de informar a los encargados del CPD sobre la instalación de los componentes para que los instalen, informar al responsable de mantenimiento de los procesos que se realizan en cada subsistema y de especificar los recursos de red que necesitan para trabajar al encargado de red.
- Desarrolladores de pruebas: Se encargarán de realizar las pruebas antes de pasar a producción.
- Encargados de red: Tendrá que ver que se cumplen todos los requisitos necesarios para satisfacer las necesidades de todos los equipos.
- Encargados de mantenimiento: Deberán de conocer el sistema antes del paso a producción para tener conocimiento de su funcionamiento antes de llegar a la tarea de mantenimiento.

6.2. Formación necesaria para la implantación

El administrador de servidores y el administrador de la base de datos serán formados para realizar los nuevos cambios en el CPD, puesto que son los únicos que tienen acceso a él. Se explicará detalladamente los nuevos componentes necesarios. Se instalará un nuevo

armario en el CPD para las aplicaciones de control de acceso, administración de tareas y fichaje. También se instalará otro armario para almacenar los datos de las aplicaciones. Deberán estimar correctamente los recursos aproximados que consumirán las aplicaciones una vez se encuentren en producción para seleccionar los componentes que mejor se adapten a las necesidades de procesamiento y memoria de forma que las aplicaciones siempre estén disponibles y sean fácilmente escalables.

El administrador de servidores deberá estudiar la documentación del software de cada subsistema creada por los desarrolladores para poder instalar las aplicaciones en el CPD. Conocerán las herramientas necesarias de cada aplicación. El administrador de la Base de Datos deberá conocer las herramientas necesarias para el despliegue de la Base de Datos y de la Base de Datos que se utilizará para las pruebas. Ambos administradores, además de estudiar toda la documentación creada por los desarrolladores, tendrán una semana en la que se reunirán junto a los desarrolladores para resolver posibles dudas y facilitar que los administradores comprendan todo a la perfección.

El administrador de redes deberá conocer el número de trabajadores que trabajará en cada subsistema y los lugares en los que trabajaran de forma que pueda estudiar los componentes hardware más adecuados para crear una red estable y que cumpla las necesidades de red de cada área, además de hacer la red escalable para poder ampliar la red sin problema en caso de que fuese necesario algún día.

El responsable de mantenimiento deberá tener un conocimiento general de las tareas que realizan cada uno de los subsistemas. Estudiará los procesos generales que realiza cada aplicación de forma que si algún día ocurriese cualquier incidente, sepa a que equipo debe dirigirse para comentar los problemas que han ocurrido para que se encarguen de solucionarlo. Tendrá unas semanas para conocer los diferentes subsistemas y reunirse con los demás empleados para que le ayuden con el aprendizaje. La finalidad del responsable de mantenimiento en esta etapa de implantación es que comprenda perfectamente el sistema antes de que comience su labor de mantenimiento.

6.3. Incorporación del sistema al entorno de operación.

6.3.1. Preparación de la instalación.

Se deberán obtener las terminales tipo tablets con sistema operativo android que utilizarán los empleados a la hora de gestionar las tareas. También se deberán obtener los lectores de huella dactilar que se incorporarán en las tablets y los que se utilizarán para el control de acceso. También será necesario 3 nuevos blades en el CPD para las aplicaciones y otro para la Base de Datos. Se deberá obtener un router para la planta en la que se encuentran la oficina en la que estarán los desarrolladores.

Se creará un documento en el que se vayan apuntando las incidencias que surjan durante la preparación, registrando la gravedad del problema, la causa y la solución que se debe realizar. Con este documento de incidencias se tratará de no olvidar acabar con todos los detalles durante la preparación, de forma que se minimice los problemas posteriormente.

6.3.2. Realización de la instalación.

Se obtendrán todas las herramientas necesarias para la instalación del control de acceso, el registro de horarios, la gestión de tareas y la Base de Datos. Se instalarán todos los sensores de huella dactilar en todas las áreas restringidas y en la entrada para el registro de horarios. Se crearán las nuevas tablas en la Base de Datos y los grupos de usuarios definidos anteriormente (4.3 Requisitos de operación y seguridad), en los que se establecerán los permisos que tendrán en función de los recursos a los que puedan acceder. Estos grupos serán los de 'Desarrolladores', 'Administrador', 'Gestores', 'Trabajadores'. Se debe configurar la automatización de la generación de copias de seguridad con el servicio AWS Backup, de modo que se realice y almacene una copia de cada subsistema los fines de semana, guardando tanto los datos actuales, como los ficheros de configuración y administración. También se instalará y configurará el sistema de discos en RAID en el CPD. Se instalarán las cámaras de vigilancia en las zonas establecidas.

6.4. Carga de datos al entorno de operación

El sistema en un principio solo tiene los datos de los empleados, que ya están en la Base de Datos. Por lo que en un principio no se aportarían más datos en la Base de Datos puesto que estos datos se comenzarán a generarse a la hora de usar realmente el sistema. Sin embargo, en la Base de Datos de prueba se cargarán datos para poder realizar las pruebas unitarias, de integración y del sistema. Estos datos no contendrán información real, para proteger la confidencialidad.

6.5. Pruebas de implantación del sistema

6.5.1. Preparación de las pruebas de implantación

La preparación de las pruebas de implantación comienza con la generación del entorno de pruebas. Para ello se deben ejecutar los playbook de Ansible generados por los desarrolladores de las pruebas unitarias, de integración y del sistema. De esta forma se instalarán automáticamente todas las herramientas necesarias para realizar las pruebas. También se asegurarán de que los datos están correctamente cargados en la Base de Datos de prueba antes de realizar las pruebas.

6.5.2. Realización de las pruebas de implantación

Una vez realizado el provisionamiento, se ejecutarán todas las pruebas unitarias, de integración y del sistema creadas. Se recopilarán todos los resultados para obtener el comportamiento del sistema frente a estas pruebas.

6.5.3. Evaluación del resultado de las pruebas de implantación

Se estudiarán los resultados que se han obtenido en la fase de realización de las pruebas de implantación, conociendo si todas las pruebas se han realizado correctamente. En caso de que se hayan obtenido errores a la hora de realizar los tests se deberán de anotar en un

lugar accesible para todo el personal para que tengan conocimiento del error que existe en el momento. Estos errores deberán de estar bien comentados, teniendo la información necesaria sobre cómo de grave es, los subsistemas que se ven afectados, el tipo de tareas que no se pueden realizar por consecuencia de estos errores, y en caso de que exista conocimiento sobre ello almacenar también la información asociada a la causa que lo provoca y la solución que se debe dar. Estos errores deberán de tener una clasificación de gravedad del error para que los desarrolladores tengan un orden de prioridad a la hora de solucionarlos.

6.6. Preparación del mantenimiento del sistema

6.6.1. Establecimiento de la infraestructura para el mantenimiento

El responsable de mantenimiento deberá comprobar si el entorno está preparado adecuadamente para la tarea de mantenimiento. Deberá conocer si existen actualmente herramientas en la organización para la gestión de mantenimiento y comprobar si son adecuadas. Si no lo son deberá de investigar cuáles son las que se deberían adquirir. Tienen que existir herramientas para:

- Registrar peticiones de mantenimiento, evaluarlas, controlarlas, realizar cambios y asegurar que se implementan correctamente.
- Comunicación con los demás empleados.
- Herramientas de monitorización de máquinas.
- Herramientas de alerta al detectar cualquier peligro como por ejemplo, detección de temperatura demasiada elevada el un componente del CPD.

6.6.2. Formalización del plan de mantenimiento

El responsable de mantenimiento formará parte del Equipo de Implantación de forma que conozca el sistema antes que haya pasado a producción. Deberá conocer las necesidades de los usuarios que usan el sistema. Cada equipo mostrará su parte al responsable de mantenimiento para facilitar que entienda cada subsistema desde un mejor punto de vista.

El responsable deberá comentar a cada equipo si la información que le han proporcionado es suficiente para que él pueda valorar el estado del sistema para su futuro mantenimiento. De forma que sepa perfectamente si los productos están completos, actualizados y son consistentes y precisos.

Para el subsistema de registro de horarios, se realizará un mantenimiento correctivo, en el que se corregirán los errores conforme vayan apareciendo, como puede ser la necesidad de sustituir un lector de huellas que ha dejado de funcionar.

Para el subsistema de control de acceso, se realizará tanto un mantenimiento correctivo como preventivo. Mantenimiento correctivo porque si un empleado no tiene permiso para realizar una tarea que verdaderamente debería poder realizar se tiene que corregir una vez aparezca la situación. Mientras que el mantenimiento preventivo se encarga de comprobar cada cierto tiempo que los permisos que están establecidos para cada grupo de empleados es el correcto para que puedan realizar sus tareas, especialmente por seguridad.

Para el subsistema de gestión de tareas, se realizará un mantenimiento correctivo, de forma que se solucionen los problemas una vez los empleados o sus superiores detecten algún error en él.

En cuanto al CPD se debe realizar todos los mantenimientos posibles:

- Correctivo: Corregir cualquier error que se produzca en el momento en el que aparece, como puede ser que haya que sustituir un componente, se encuentre alguna vulnerabilidad, se necesite aumentar el almacenamiento, etc.
- Preventivo: Se deben realizar pruebas regulares para comprobar el estado general, realizando pruebas de vulnerabilidades, comprobando el estado de los componentes, etc.
- Predictivo: Se debe monitorizar constantemente el CPD, obteniendo todos los valores posibles sobre su funcionamiento, temperatura, estado, etc. De esta forma se pretende evitar que suceda alguna consecuencia o estar totalmente preparados cuando vaya a suceder.

6.7. Presentación y aprobación del sistema.

El Comité de Dirección debe formalizar la aprobación del sistema, por lo que se lleva a cabo una presentación general del sistema y se espera la confirmación de su aprobación.

6.7.1. Convocatoria de la presentación del sistema.

En este paso se realiza una convocatoria para la presentación del sistema al Comité de Dirección y se espera la confirmación por parte del Comité de Dirección. Se debe preparar una presentación en la que se vea bien reflejado el estado del sistema. Entre los apartados que se tomarán habrá un informe detallado con la evaluación obtenida de las pruebas realizadas y el plan de mantenimiento, mostrando todos los procesos que se realizaron y que se han probado correctamente.

6.7.2. Aprobación del sistema.

Se presenta el sistema al Comité de Dirección según el plan previsto y se aprueba formalmente el sistema.

6.8. Paso a producción.

6.8.1. Preparación del entorno de producción.

En este punto se comprobará que la instalación del sistema en producción es correcta. Se debe haber comprobado ya que las sistemas de control de acceso, gestión de tareas y registro de horarios funciona a la perfección en el entorno de pruebas, por lo que solo será necesario asegurarse de que la Base de Datos de producción está preparada para funcionar.

6.8.2. Activación del sistema de producción.

Se levantará el sistema utilizando la Base de Datos del entorno de producción, la cual en un principio solo contará con los datos de los empleados y se comenzarán a registrar la información que generará el uso de los subsistemas nuevos, como las tareas a realizar y a asociarlas a los empleados encargados de la tarea y los permisos de acceso que tienen.

Una vez que el sistema en producción está activado, comenzaría el proceso de Mantenimiento.

7. Mantenimiento de Sistemas de Información (MSI)

7.1 Registro de la Petición

Se proveé un sistema estandarizado para el registro de las peticiones de mantenimiento, común a los usuarios del sistema y al equipo de mantenimiento, en el que se contemplan:

- Error de procesamiento (salidas incorrectas de un programa).
- Error de rendimiento (tiempo de respuesta demasiado alto).
- Error de programación (inconsistencias en el diseño).
- Error de documentación (inconsistencias entre la funcionalidad de un programa y el manual de usuario).
- Error de conectividad (fallos en las conexiones de red).
- Mejora (modificaciones y eliminaciones necesarias en un producto software para cubrir la expansión o cambio en las necesidades del usuario).

Se define error cuando esté fuera de los requisitos establecidos para el sistema de información. Si está dentro de los límites establecidos pero no es suficiente para los criterios del usuario, se considera mejora.

Dependiendo del tipo de mantenimiento solicitado se hará un estudio de los subsistemas a los que competen dicho mantenimiento, comprobando su viabilidad de acuerdo a las prestaciones de mantenimiento establecidas para los diferentes subsistemas.

Algunos de los estándares para el mantenimiento del software son IEEE 1219 e ISO/IEC 14764. Vamos a emplear este último,ISO/IEC 14764.

Es un estándar internacional que presenta los requerimientos para el proceso de mantenimiento del software, proporciona una guía que es aplicable a la planificación, ejecución, control, revisión y evaluación de los procesos de mantenimiento por medio de un plan.

Dicho plan es usado para guiar el mantenimiento, explica su necesidad, contiene la documentación y responsabilidades de todos los involucrados, incluye qué recursos hay disponibles para el mantenimiento, dónde se hace y unos requisitos para establecer una guía.

Los requisitos son la descripción del sistema, identificación del estado inicial del software, descripción del soporte. Definidos en la construcción e implementación de este mismo proyecto.

El mantenimiento se hará en el sitio donde esté situado el sistema afectado en cuestión y el que sea posible, en la sala de mantenimiento dispuesta para esta tarea, situada en el sótano del edificio.

7.1.1 Registro de la Petición

Se creará un catálogo con las diferentes peticiones de los usuarios, con éste, el comité o responsable de mantenimiento que se podrá hacer cargo de las diferentes solicitudes.

El procedimiento exacto se podría hacer de la siguiente manera: Entrega de la solicitud de mantenimiento en administración, desde ahí se le da registro de entrada para tener constancia y se le entrega al comité de mantenimiento para que lo incluya al catálogo.

En toda solicitud se deberá registrar el nombre y firma de la persona que lo solicita, cuando se reciba en el departamento de mantenimiento deberá tener nombre y firma del experto que la recibe, fecha y hora de recepción y se entregará un recibí.

Se diferencian dos tipos de peticiones según el anterior estándar para el registro de las peticiones de mantenimiento: mejoras o incidencias.

En este apartado, para las peticiones de mejora, se debe especificar los requisitos a completar. Para las peticiones de mantenimiento por un fallo, habrá que incluir una descripción completa de las circunstancias específicas que llevaron al fallo, adjuntando todos los datos que sean precisos.

7.1.2 Asignación de la Petición

Con la información anterior podemos identificar los sistemas de información que inicialmente estarían afectados en la petición de mantenimiento. Con estos datos, el comité de mantenimiento estudia si el plan de mantenimiento cubre la petición registrada en el catálogo, si es así se le asigna el posterior análisis a un experto del campo correspondiente, nuestro equipo de mantenimiento contendrá:

- Arquitectos del sistema.
- Especialistas en cada área tecnológica.
- Especialistas en integración y test.

Aunque se especifica con exactitud posteriormente, en este punto se asigna la petición a un experto que a partir de este momento será el controlador del mantenimiento para la petición en concreto, recibirá la solicitud de mantenimiento y asumirá la responsabilidad de su gestión y seguimiento.

Según proceda se acepta o rechaza la petición, si es aceptada se nombra a un responsable que procederá al estudio minucioso de la petición y se hará cargo de la misma.

7.2 Análisis de la Petición

Una vez aceptada la petición de mantenimiento, el controlador de mantenimiento para la petición, hará un diagnóstico y análisis del alcance del mismo en lo referente a los sistemas y subsistemas afectados, valorará hasta qué punto es aceptable que los sistemas de información sean modificados dependiendo del ciclo de vida estimados para los mismos. En caso de no ser aceptable el impacto de la reparación, se procederá a desviar la petición

hacia el proceso de Estudio de Viabilidad del Sistema (EVS), del cual se hará cargo el comité de mantenimiento.

7.2.1 Verificación y Estudio de la Petición

El comité de mantenimiento verificará cada petición de mantenimiento para determinar su validez. Si es correctivo se debe reproducir el problema constatando el error. Si es evolutivo hay que comprobar que la petición es factible.

Una vez realizada la verificación procederemos al estudio de la petición que dependerá si el mantenimiento es correctivo o evolutivo:

- Estudio de la petición para el mantenimiento correctivo: Ha de determinarse si el fallo es crítico o no. En caso de ser un problema crítico se propondrá una solución inmediata a corto plazo para restaurar el servicio afectado lo más pronto posible. Posteriormente habrá que establecer una solución definitiva valorando los subsistemas implicados y teniendo en cuenta los posibles efectos secundarios en los mismos. En caso de no ser un problema crítico la petición será clasificada con el fin de determinar cuál será la solución más adecuada.

- Estudio de la petición para un mantenimiento evolutivo: En este caso se determina si se trata de una modificación de los sistemas de información inicialmente afectados o se trata de una incorporación de nuevas funcionalidades necesarias para el buen funcionamiento de la empresa.

Se determina sistema crítico si un fallo del mismo afecta a posibles pérdidas económicas significativas, daño físico o afecta a la vida humana, así como a cuyo fallo de funcionamiento del sistema puede provocar lagunas en las actividades de la empresa y por consiguiente afecta a la confiabilidad del sistema, la cual agrupa los siguientes apartados:

- Disponibilidad. Si el sistema no proporciona servicios que son requeridos.
- Fiabilidad. Si el sistema no proporciona los servicios que han sido especificados.
- Seguridad. Si el sistema deja de funcionar por un fallo catastrófico.
- Protección. Si el sistema se ha visto comprometido por intrusiones accidentales o premeditadas.

7.2.2 Estudio de la Propuesta de Solución

Para cada petición recogida en el catálogo, se asigna una prioridad inicial, se analiza si tiene relación con otras peticiones, si estas están en curso, se evalúa la repercusión de la petición en las peticiones en curso. Se analiza los sistemas de información implicados, valorando sus características y la cantidad de cambios sufridos desde su funcionamiento, el impacto que la modificación puede ocasionar al entorno tecnológico y el nivel de servicio del mismo. Dependiendo si el mantenimiento es evolutivo o correctivo tenemos:

- Evolutivo: Se estudiará cómo atender las peticiones teniendo en cuenta la política de versiones vigente en ese momento en la empresa (se mantiene un control de versiones en plataforma *cloud*). Si se trata de una incorporación o eliminación, se

determina la necesidad de llevar a cabo el Análisis de los Subsistemas de Información, de modo previo a la identificación de los elementos afectados.

De la misma manera, se podría tomar una solución si:

- El ciclo de vida estimado para los sistemas de información afectados haga que su cambio sea inminente y no sea necesario abordar el problema.
- La existencia en el mercado de opciones más idóneas que hagan que sea menos costoso cambiar el sistema de información.
- Que las implicaciones en el entorno tecnológico, produzca un alcance de la modificación sean demasiado extensos.

- Correctivo: Si se trata de una solución de emergencia, hay que comprobar que dicha solución no compromete a cualquier subsistema, es decir, se mantiene la integridad y operatividad del sistema. Por ello reanudaremos y comprobaremos todas las actividades restantes que no incluyen las del mantenimiento en sí para no vernos en un problema de mayor envergadura.

En cualquier caso se hará un estudio del esfuerzo requerido para el mantenimiento para cada sistema de información, según la tecnología aplicada, naturaleza y tamaño del subsistema de información y los tipos de lenguajes utilizados, base de datos, etc. Por último si es necesario se propone una alternativa a la solución, determinando una fecha límite y un coste aproximado en función de la estimación realizada anteriormente. Junto con el usuario se aceptará o rechazará la solución.

7.3 Preparación de la Implementación de la Modificación

Se identificará de forma detallada cada uno de los elementos afectados por el cambio mediante el análisis de impacto. Dicho análisis tiene como objetivo determinar qué parte del sistema de información se ve afectada y en qué media (tanto software como hardware). Esto permite fijar un plan de acción con el fin de cumplir un plazo máximo para la entrega. Posteriormente se activan los correspondientes procesos de desarrollo para llevar a cabo la implementación de la solución. Al mismo tiempo, se especifican las pruebas de regresión con el fin de evitar el efecto onda en el sistema, una vez realizados los cambios.

7.3.1 Identificación de Elementos Afectados

Se realiza un análisis donde quedarán reflejados los elementos de la infraestructura tecnológica (nombrados en el punto Identificación del entorno tecnológico, de este mismo proyecto) y los elementos asociados a los productos software implicados en cada petición, así como la asociación de elementos a cada petición, esto permite el control de la gestión del cambio sobre un mismo elemento.

Para una eficaz identificación de software implicado, anteriormente se han definido:

- Uso de técnicas estándares para descomponer el software en entidades funcionales.
- Uso de estándares de documentación del software.
- Diseño paso a paso en cada nivel de descomposición del software.
- Uso de código estructurado.

- Definición a priori de todas las interfaces y estructuras de datos antes del diseño.
- Uso de métricas de productos y procesos.

7.3.2 Establecimiento del Plan de Acción

Para determinar el plan de acción, se identificarán las actividades y tareas siguientes:

- Estudio de viabilidad.
- Análisis del sistema.
- Diseño del sistema de información.
- Construcción del sistema de información.
- Implementación y aceptación del sistema de información que sea preciso realizar

Cuando ya tengamos delimitado el alcance el plan de acción, se utilizarán los indicadores establecidos para evaluar el conjunto de componentes afectados, realizando los reajustes oportunos. Se determinará:

- El coste asociado.
- Plazos estimados.
- Composición del equipo de trabajo inicial necesario. Se establece como mínimo:
    - Controlador del mantenimiento, recibirá la solicitud de mantenimiento y asumirá la responsabilidad de su gestión y seguimiento.
    - Supervisor del sistema software, conoce la aplicación a mantener e informa de la afectación de la misma conforme se apliquen los cambios (tendremos un especialista por área tecnológica en el equipo de mantenimiento).
    - Desarrollador de mantenimiento, realizará los cambios en la aplicación.
- Puntos de control que permiten hacer un seguimiento del plan de trabajo.

7.3.3 Especificación del Plan de Pruebas de Regresión

Se trata de una pruebas para eliminar el “efecto onda”, esto son los cambios de comportamiento o errores provocados por una petición. Para que esto no suceda hay que comprobar los efectos secundarios en el componente modificado y en otros asociados. En concreto se van a realizar las pruebas de regresión para evitar:

- Efectos secundarios sobre el código:
    - Cambios en el diseño que suponen muchos cambios en el código.
    - Eliminación o modificación de un subprograma.
    - Eliminación o modificación de una etiqueta.
    - Eliminación o modificación de un identificador.
    - Cambios para mejorar el rendimiento.
    - Modificación de la apertura/cierre de ficheros.
    - Modificación de operaciones lógicas.
- Efectos secundarios sobre los datos:
    - Redefinición de constantes locales o globales.
    - Modificación de los formatos de registros o archivos.
    - Cambio en el tamaño de una matriz u otras estructuras similares.
    - Modificación de la definición de variables globales.
    - Reinicialización de indicadores de control o punteros.

    - Cambios en los argumentos de los subprogramas. Es importante una correcta documentación de los datos.
- Efectos secundarios sobre la documentación:
    - Modificar el formato de las entradas interactivas.
    - Nuevos mensajes de error no documentados.
    - Tablas o índices no actualizados.
    - Texto no actualizado correctamente.

Tendremos como salida el Plan de Pruebas de Regresión que recoge las relaciones existentes entre los distintos componentes identificados en la tarea 7.3.1 (Identificación de Elementos Afectados), para comprobar en consecuencia los elementos que pueden verse afectados.

7.4 Seguimiento y Evaluación de los Cambios hasta la Aceptación

Hay que comprobar que todo lo que se ha modificado o pudiera verse afectado, funciona correctamente. Para posteriores análisis se puede incluir la información oportuna al catálogo.

7.4.1 Seguimiento de los Cambios

Se hará el seguimiento del plan de acción de acuerdo con los puntos de control propuestos en la actividad anterior.

Se realizará el seguimiento de los cambios en cada sistema de información que se vea afectado, siguiendo las actividades conformadas en los procesos de Análisis, Diseño, Construcción e Implantación.

Se establece el siguiente documento para llevar el control de la planificación establecida:

Responsable de Mantenimiento:						
Diagnóstico:						
Actividad	Fecha programada	Fecha realización	Responsable	Objetivo	Recursos empleados	Firma

Observaciones:						
Observaciones:						
Observaciones:						

7.4.2 Realización de las Pruebas de Regresión

Se realizarán las pruebas de regresión definidas anteriormente en la especificación del plan de pruebas.

Como las pruebas de regresión se harán de forma periódica y constante, serán automatizadas. Cada vez que hay una modificación en el sistema de información, ejecutaremos una selección de pruebas relevantes incluyendo pruebas unitarias, de integración, de implantación, de aceptación y pruebas de auditoría periódicas.

El especialista que realiza las pruebas ha de ser diferente a la que lleva a cabo la petición de mantenimiento y a la persona que lo supervisa, los test los realizará el experto en integración y test. En caso de detectarse problemas, se recogerán las incidencias ocasionadas por el cambio y se remitirá el documento al comité de mantenimiento encargada de la petición.

Cuando finalmente el funcionamiento sea correcto, se documenta el resultado global de las pruebas que se han efectuado y se remite al responsable de mantenimiento para su aprobación.

Este informe de cambios debe incluir:

- Información del programa software o hardware implicado.
- Lenguaje de programación utilizado.
- Fecha de instalación del programa.
- Número de ejecuciones del programa desde la instalación.
- Número de fallos.
- Número de sentencias añadidas, modificadas y eliminadas en el cambio.
- Número de personas-hora.
- Identificación de la persona responsable.

- Identificación de la solicitud de mantenimiento.
- Tipo de mantenimiento.
- Fechas de comienzo y final del mantenimiento.
- Beneficios netos que supone el cambio.

7.4.3 Aprobación y Cierre de la Petición

Una vez se aprueba por el responsable de mantenimiento el correcto funcionamiento del sistema la que se le ha realizado el cambio, se da por finalizada la petición y se actualiza el correspondiente catálogo registrando su finalización.

Para llevar un control de costes y evaluar la facilidad de mantenimiento, es conveniente registrar datos cuantitativos relativos al tiempo empleado en cada parte del desarrollo de la petición de mantenimiento desde que se solicita la misma hasta su cierre.

Para cuantificar el tiempo empleado en cada parte del desarrollo de la petición de mantenimiento, se adecuan los siguientes parámetros que sirven de referencia, dividiendo en porcentajes el total del tiempo estimado para la petición:

Actividad	**% Tiempo**
Estudio de las peticiones	18%
Estudio de la documentación	6%
Análisis del código, o lo establecido en la petición	23%
Modificación de lo establecido en la petición	19%
Actualización de la documentación	6%
Realización de pruebas	28%

En el estudio y análisis, tanto el comité como el técnico a cargo, recogerán en la documentación de cada petición, el tiempo empleado y el tiempo que se estima para el cambio. Además, en la actividad del seguimiento de los cambios, hemos expuesto un documento que nos ayudará a saber el tiempo empleado en las modificaciones, actualizaciones y pruebas.

De esta forma, podremos saber el tiempo total empleado en cada petición de mantenimiento y con esto podremos evaluar futuros mantenimientos con un mejor ajuste. Además podremos evaluar cada parte del mantenimiento por si se perdiera más tiempo de lo establecido y poder tomar medidas.

8. Gestión de la configuración

El sistema de gestión de la configuración mantiene un registro acerca de los sistemas configurables de la empresa almacenando su información actualizada y de forma independiente a la del resto de productos. De este modo se puede acceder rápidamente a su información y simplificar el proceso de mantenimiento. Para ello, su implementación se lleva a cabo durante las fases de desarrollo descritas anteriormente y finaliza cuando los productos son abandonados.

8.1. Estudio de la viabilidad del sistema

En esta primera fase, el responsable de gestión de configuración deberá obtener y analizar los requisitos de configuración para los tres subsistemas de información implantados en la empresa.

- Se llevará a cabo un control de versiones de los tres subsistemas para conocer el número de la versión actual, el histórico de versiones y de modificaciones incorporadas.
- Los desarrolladores podrán subir sus cambios en los repositorios en los que estén trabajando pero será el jefe de programación el encargado de analizarlos y aceptarlos o denegarlos.
- Adicionalmente, se creará y mantendrá actualizada una línea de referencia o *baseline* para facilitar la gestión de la configuración conjunta de los distintos módulos del sistema.
- Se mantendrá un registro acerca del estado de las configuraciones de los módulos para monitorizar el estado actual y analizar el histórico de los anteriores.
- Se realizarán auditorías de los subsistemas de información para comprobar que los requisitos de la gestión de configuración son satisfechos en todo momento.

8.2. Establecer el plan de gestión de la configuración

En primer lugar comenzaremos formulando el plan de gestión de la configuración para. posteriormente, especificar la infraestructura en la que se alojará el sistema de gestión de la configuración, de modo que pueda llevar a cabo todas las tareas detalladas.

8.2.1. Definir el plan de gestión de la configuración

Para su definición vamos a seguir el estándar *IEEE 828* que propone un conjunto de requisitos mínimos para definir los procesos con los que se gestionará la configuración del sistema. Entre los diversos aspectos que se tratan, proponemos los siguientes.

- A cada subsistema configurable se le asigna un identificador único compuesto por sus iniciales. Por ejemplo, para el módulo de control de horarios su identificador unívoco sería “SCH”.
- Los subsistemas asociados al control del personal en diferentes ámbitos, como es el de la jornada y el acceso a las zonas del edificio, serán categorizados dentro de la clasificación *Sistemas de control*. Mientras que el subsistema asociado a la gestión

de las tareas se clasificará en una segunda categoría denominada *Sistemas de gestión*.

- Los tres subsistemas se encuentran alojados en los servidores de aplicación propios de la empresa, situados a su vez en el CPD del edificio.
- La relación entre los distintos subsistemas se puede explicar con el siguiente caso práctico. Si un empleado no ha registrado el inicio de su jornada laboral no podrá acceder a ningún área del edificio ni gestionar sus tareas. Por lo que el módulo de control de horarios se encuentra relacionado con el de control de acceso y gestión de tareas, mientras que estos dos últimos son independientes entre sí.
- El dominio de la gestión de la configuración abarca tanto las aplicaciones como los servidores a los que acceden y se alojan. Por lo tanto se tratarán aspectos de configuración relativos a la infraestructura tecnológica de los subsistemas, modificaciones de los mismos, componentes hardware y software, esquemas de comunicación y redes y su documentación asociada. Para ello se establecen los siguientes procesos.
    - Control de acceso y modificación de la configuración de los subsistemas y los sistemas en los que se alojan y/o tienen acceso, como el sistema de almacenamiento.
    - Control de acceso y modificación de los usuarios y sus permisos.
    - Control para generar nuevas versiones de los productos así como para la publicación de las mismas.
    - Control del estado de los componentes hardware, software y de comunicaciones.
    - Control de la configuración de la red en aspectos tales como rendimiento, seguridad, accesos, entre otros.
    - Control en el acceso, modificación y/o actualización de la documentación de explotación y manuales de usuario.
- Solo se podrán incorporar cambios en la implementación de los módulos una vez hayan pasado el conjunto de pruebas de validación definido en etapas anteriores, añadiendo los tests pertinentes para probar las nuevas funcionalidades. A continuación, será necesaria la aprobación del supervisor correspondiente.
- Los estados por lo que puede pasar un producto se definen a continuación.
    - En elaboración. El producto continúa en la fase de desarrollo. Al finalizar pasará al siguiente estado de validación para comprobar el impacto de las modificaciones realizadas.
    - En revisión. El producto se encuentra en la etapa de validación, ya sea por la implementación de nuevas funcionalidades o por la corrección de incidencias. Una vez haya terminado, pasa directamente al siguiente estado en el que se encuentra listo para comenzar la aceptación por parte del cliente, si no existen motivos para volver al estado anterior del desarrollo.
    - Finalizado. El producto ya se encuentra listo para funcionar a la espera de la aprobación por parte del cliente. Cuando esta suceda, entonces pasa la siguiente estado de forma automática, siempre y cuando no sean necesarias nuevas implementaciones y/o validaciones.
    - Aprobado. El producto ha sido aceptado por el cliente y se encuentra en funcionamiento. En caso de que, de nuevo, se apruebe alguna petición de

cualquier naturaleza pasará al primer estado una vez haya comenzado su implementación.

- Para realizar las auditorías será necesario recopilar información tal como el tiempo invertido en la planificación y revisión de la gestión de configuración, número de modificaciones realizadas a nivel de requisitos, diseño, componentes, aplicaciones y recursos, estado de todos los sistemas, registro de incidencias y mejoras, etc.
- Por último se establece la siguiente política de gestión de la configuración.
    - Control y seguimiento de la implementación de los productos y su configuración a partir de las etapas de su desarrollo.
    - Se realizará una auditoría de configuración a todos los subsistemas cada tres semanas.
    - El estado de los productos será actualizado automáticamente por el sistema de gestión de configuración en función de los criterios propios de cada estado.
    - Las peticiones y/o incidencias podrán ser creadas, modificadas y/o descartadas solo por el equipo de mantenimiento.

8.2.2. Definir el entorno tecnológico para la gestión de la configuración

Para la gestión de la configuración de los subsistemas vamos a hacer uso del servicio *AWS OpsWorks* el cual ya se ocupa de proveer la infraestructura tecnológica y las herramientas para el sistema de gestión de configuración. Tras estudiar diversas alternativas, hemos seleccionado esta puesto que es la que nos parece más cómoda ya que basta con definir la arquitectura de los subsistemas a gestionar, sus recursos y configuración deseable para que este proveedor realice la administración correspondiente. Además, permite establecer una configuración tal que su gestión permita el funcionamiento de los tres subsistemas como si de uno solo se tratara.

8.3. Análisis, diseño, construcción, implantación, aceptación y mantenimiento del sistema

En la etapa en la que se define el ciclo de vida del sistema se deben llevar a cabo ciertas actividades relacionadas con el sistema de gestión de la configuración. Entre ellas destaca el registro del nuevo producto, las versiones y procesos efectuados durante su desarrollo, los sistemas sujetos a mantenimiento, etc. Para realizar los registros en el servicio *AWS OpsWorks* se deberán desarrollar *scripts* en *Chef* o *Puppet* para almacenar la información tanto de los nuevos productos a gestionar como de los generados a partir de las peticiones para su modificación.

8.3.1. Identificación y registro de los productos

En nuestro caso los tres productos que se van a añadir en el sistema de gestión de configuración son los tres subsistemas desarrollados: control de horarios, control de acceso y gestión de tareas. Al comienzo de su desarrollo, se registran los tres con sus correspondientes identificadores únicos formados por sus siglas como se explicó anteriormente, una versión inicial 0.0, el estado *Aprobado* que indica que inicialmente no existen peticiones en curso, y su localización en el sistema de gestión de la configuración, el cual se establece según el orden en el que se han mencionado anteriormente.

8.3.2. Registro de las modificaciones

Toda petición de mantenimiento, tanto correctivo como evolutivo, se registrará en el sistema de gestión de la configuración. Para ello se anotará la versión inicial de los productos afectados, sus estados actuales de entre los definidos anteriormente, las versiones que se pretenden generar durante el desarrollo, además de la información asociada a la petición, como los requisitos a satisfacer o el diseño actual del producto. De este modo, durante las diferentes etapas descritas anteriormente, desde el análisis hasta la aceptación del sistema, se registrará información acerca de los nuevos prototipos obtenidos.

8.3.3. Seguridad

De forma general a los tres subsistemas desarrollados, disponemos de un servicio cloud como es *AWS Backup* para realizar copias de seguridad de los datos almacenados. Así, si ocurre algún tipo de desastre natural o tecnológico que dañe los servidores de datos siempre podemos recuperar la mayor parte de la información. Del mismo modo, también disponemos del código fuente del sistema y su despliegue en repositorios cloud, en este caso *GitHub*, y de un sistema de gestión de la configuración también en la nube gracias al servicio anteriormente descrito con *AWS OpsWorks*.

Asimismo, como hemos indicado anteriormente todos los equipos disponen de antivirus y *firewalls* para la prevención y actuación frente a ataques de terceros. En caso de que estos no sean perpetrados con programas maliciosos, como por ejemplo un ataque de denegación de servicio o acceso no autorizado, los servidores disponen de una configuración específica para bloquear los recursos atacados y notificar al administrador acerca de la situación.

Finalmente contratamos formación sobre aspectos concretos de seguridad para que la plantilla cuente con los conocimientos necesarios para identificar cuándo se está produciendo un ataque así como el protocolo a seguir en cada caso. Para ello se asistirá a conferencias, congresos y talleres de seguridad al menos una vez por trimestre.