



PROYECTO CPD

Frances Simó Olma

Jaime Climent Cardona

Jonman Jimenez Mendoza

| | |
|--|----|
| 1. CPD para el alojamiento del sistema de gestión de las actividades deportivas de Tavernes. | 3 |
| 1.1 Objetivos..... | 3 |
| 1.2. Requisitos | 4 |
| 1.2.1. Requisitos del sistema de Gestión:..... | 4 |
| 1.2.2. Requisitos del CPD: | 4 |
| 1.3. WBS..... | 5 |
| 1.4. Cronograma | 6 |
| 1.5. Equipo | 7 |
| 2. DOCUMENTO DE ROLES Y RESPONSABILIDADES | 7 |
| 2.1. Roles y Responsabilidades | 8 |
| 2.1.1. Rol..... | 8 |
| 2.1.1.1. Responsabilidades | 8 |
| 2.1.2. Rol..... | 8 |
| 2.1.2.1. Responsabilidades | 9 |
| 2.1.3. Rol..... | 9 |
| 2.1.3.1. Responsabilidades | 9 |
| 2.2. Tareas Asignadas | 9 |
| 2.2.1. Miembro: Jonman Jiménez Mendoza | 10 |
| 2.2.2. Miembro: Jaime Climent Cardona | 10 |
| 2.2.3. Miembro: Frances Simó Olmo..... | 11 |
| 2.3. Tareas en Equipo | 11 |
| 2.3.1. Miembros involucrados | 12 |
| 2.4. Firmas..... | 13 |
| 3. Análisis de requisitos | 13 |
| 3.1. Materiales que se van a utilizar | 14 |
| 3.1.1. Requisitos de Maquinaria | 14 |
| 3.1.1.1. Servidores | 14 |
| 3.1.1.2. Estaciones de trabajo..... | 14 |
| 3.1.1.3. Equipos de red..... | 15 |
| 3.1.1.4. Almacenamiento en red (NAS) | 15 |

| | |
|---|----|
| 3.1.2. Requisitos de Software..... | 15 |
| 3.1.2.1. Sistema de gestión..... | 15 |
| 3.1.2.2. Bases de datos | 15 |
| 3.1.2.3. Seguridad..... | 16 |
| 3.1.2.4. Otras herramientas | 16 |
| 3.1.3. Requisitos de Infraestructura de Red | 16 |
| 3.1.3.1. Conectividad | 16 |
| 3.1.3.2. Diseño de red | 16 |
| 3.1.3.3. Seguridad..... | 16 |
| 3.1.3.4. Monitorización..... | 17 |
| 3.1.4. Escalabilidad y Disponibilidad | 17 |
| 4. Recursos necesarios..... | 17 |
| 4.1. PRESUPUESTO | 18 |
| 4.1.1. HARDWARE..... | 18 |
| 4.1.2. SOFTWARE..... | 19 |
| 4.1.3. INFRAESTRUCTURA DE RED | 20 |
| 4.1.4. SERVICIOS PROFESIONALES..... | 20 |
| 5. Evaluación de riesgos y planificaciones de contingencias | 21 |
| 5.1. Identificación de riesgos..... | 22 |
| 5.1.1. Riesgos tecnológicos | 22 |
| 5.1.2. Riesgos ambientales | 22 |
| 5.1.3. Riesgos Humanos | 23 |
| 5.2. Plan de contingencia | 23 |
| 5.2.1. Medidas Preventivas | 23 |
| 5.2.3. Respuesta a accidentes | 23 |
| 5.2.4. Recuperación y Reanudación | 24 |
| 5.2.5. Sitio de respaldo | 24 |

Definición de los objetivos del proyecto y requisitos necesarios

1. CPD para el alojamiento del sistema de gestión de las actividades deportivas de Tavernes.

1.1 Objetivos

Los **objetivos** de este CPD estarán dedicados exclusivamente a alojar el sistema de gestión de actividades deportivas de Tavernes, proporcionando los recursos informáticos necesarios para garantizar su funcionamiento eficiente, seguro y escalable.

- Centralizar información sobre los usuarios, deportes, pistas y puestos del tipo de deporte deseado en una base de datos estructurada y accesible.
- Minimizar la intervención manual para así facilitar la tarea y ser más eficiente.
- Generar notificaciones automáticas para no tener que introducir datos manualmente.
- Integrar herramientas de planificación ya sea horario y disponibilidad.
- Implementar mecanismos de respaldo y recuperación ante desastres para evitar la pérdida de información.
- Disponer de APP, para hacer las reservas.
- Proporcionar soporte técnico.
- Mantener una buena escalabilidad para ampliar la capacidad del CPD, cuando sea necesario.
- Facilitar conexión con sistemas de pago.
- Monitoreo y mantenimiento proactivo.

1.2. Requisitos

Los **requisitos** que se abordarán a continuación enfocados en garantizar una coordinación y gestión eficiente se dividirán en requisitos del CPD y requisitos del sistema de Gestión.

1.2.1. Requisitos del sistema de Gestión:

Los **requisitos de Gestión** que se tratarán a continuación abarcan las funciones clave necesarias para garantizar su operatividad y comodidad para el usuario.

- **Iniciar sesión:** El sistema permitirá a los usuarios iniciar sesión con su nombre de usuario y contraseña.
- **Enviar correo electrónico de confirmación:** El sistema enviará un correo electrónico de confirmación al usuario después de que haya realizado un pedido con éxito.
- **Agregar al carrito:** El sistema permitirá a los usuarios agregar reservas de pistas o puestos dependiendo del deporte que desee.
- **Realizar pagos:** El sistema permitirá a los usuarios realizar pagos seguros y eficientes.
- **Usabilidad:** La interfaz de usuario debe ser intuitiva y fácil de usar para usuarios de todas las edades y niveles de experiencia.

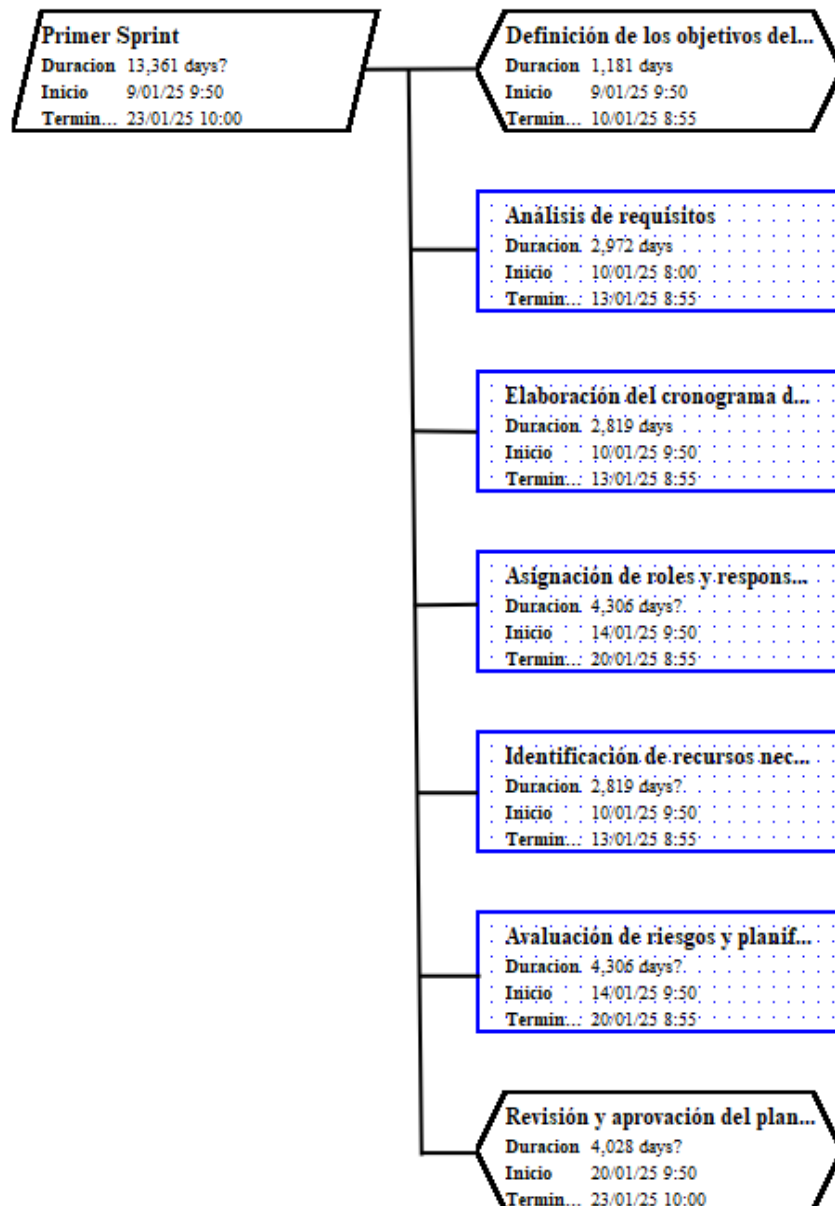
1.2.2. Requisitos del CPD:

Los **requisitos del CPD** que se tratarán a continuación se centran aspectos que no afectan directamente al usuario, pero si al CPD.

- **Rendimiento:** El sistema debe responder a las solicitudes de los usuarios en menos de 2 segundos.
- **Seguridad:** Todas las comunicaciones externas entre los servidores de datos, la aplicación y el cliente del sistema deben estar cifradas utilizando el algoritmo RSA.
- **Disponibilidad:** El sistema debe estar disponible siempre.
- **Integridad de datos:** El sistema debe garantizar que los datos no se pierdan ni se corrompan durante la transmisión.
- **Recuperabilidad:** En caso de fallos, el sistema debe poder recuperar los datos y seguir funcionando en 30 minutos.
- **Capacidad:** El sistema debe manejar hasta 1000 usuarios simultáneos.
- **Confidencialidad:** El sistema debe proteger la información personal de los usuarios y cumplir con las regulaciones de privacidad aplicables.
- **Compatibilidad:** El sistema debe funcionar en diferentes plataformas y sistemas operativos, incluyendo Windows y Linux.

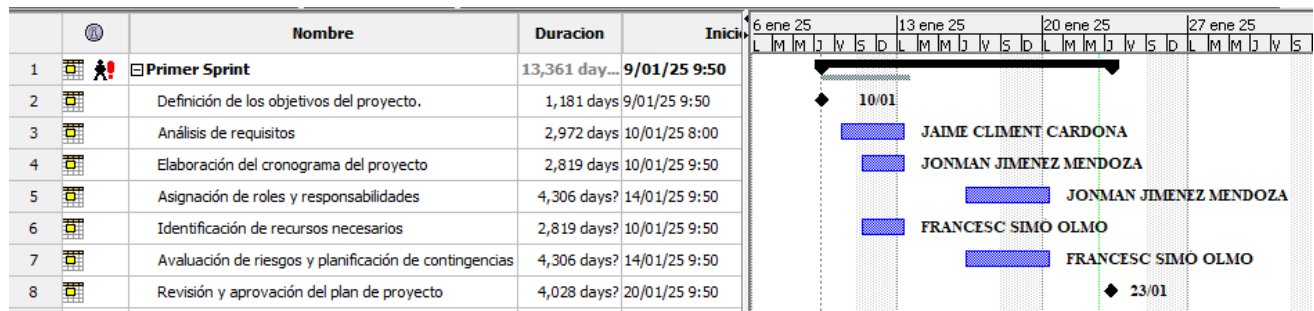
1.3. WBS

El **Work Breakdown Structure (WBS)** que se presenta a continuación desglosa las tareas. Esto permite organizar el proyecto en tareas manejables.



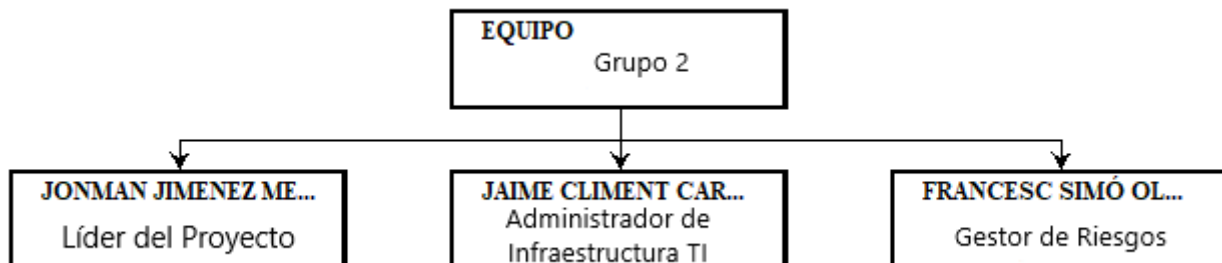
1.4. Cronograma

El **Cronograma** que se presenta a continuación detalla las fases y actividades clave del proyecto, este en específico del primer sprint, permite coordinar tareas, establecer plazos y garantizar que el proyecto avance de manera ordenada y dentro de los tiempos establecidos.



1.5. Equipo

A continuación, se ve los miembros del equipo y sus roles.



2. DOCUMENTO DE ROLES Y RESPONSABILIDADES

En este documento se redacta los roles, responsabilidades y tareas asignadas a los miembros del equipo, para poder garantizar la colaboración y objetivos.

El equipo encargado se encarga de la creación, gestión y mantenimiento del CPD que alojara el sistema de gestión de actividades deportivas de Tavernes.

2.1. Roles y Responsabilidades

2.1.1. Rol

Líder del Proyecto

Persona en quien recaen las responsabilidades generales y quien realiza las estimaciones sobre la capacidad de esfuerzo del equipo.

2.1.1.1. Responsabilidades

- Coordinar las actividades del equipo.
- Supervisar el progreso del proyecto.
- Garantizar el cumplimiento de los plazos.
- Resolver conflictos dentro del equipo.
- Gestión de la documentación.

2.1.2. Rol

Administrador de Infraestructura TI

Encargado de diseñar, planificar y supervisar la infraestructura software y Hardware.

2.1.2.1. Responsabilidades

- Selección y adquisición de hardware y software.
- Gestión de redes y seguridad.
- Mantenimiento y actualizaciones.
- Documentación y cumplimiento normativo.

2.1.3. Rol

Gestor de Riesgos

Identifica, analiza y evalúa los riesgos que podrían afectar la operación del CPD.

2.1.3.1. Responsabilidades

- Evaluación y análisis de riesgos.
- Desarrolla estrategias y medidas para o minimizar el impacto de un riesgo.
- Gestión de incidentes y crisis.
- Monitoreo y seguimiento de riesgos.

2.2. Tareas Asignadas

Las **Tareas Asignadas** que se explicarán a continuación, describen las responsabilidades específicas asignadas a los distintos miembros involucrados.

2.2.1. Miembro: Jonman Jiménez Mendoza

Rol asignado: Líder del Proyecto.

Tareas específicas:

- Dividir las fases del proyecto en tareas concretas mediante la estructura WBS (Work Breakdown Structure).
 - Fecha inicio: 10-01-25
 - Fecha final: 13-01-25
- Establecer un plan detallado con la secuencia temporal de las tareas, asegurando que el sprint finalizo dentro de la fecha tope establecida.
 - Fecha inicio: 10-01-25
 - Fecha final: 13-01-25
- Designar un líder de proyecto responsable de la coordinación general.
 - Fecha inicio: 14-01-25
 - Fecha final: 20-01-25
- Asignar responsables para cada fase y tarea específica del proyecto.
 - Fecha inicio: 14-01-25
 - Fecha final: 20-01-25

2.2.2. Miembro: Jaime Climent Cardona

Rol asignado: Administrador de Infraestructura TI.

Tareas específicas:

- Identificar las necesidades de hardware y software.
 - Fecha inicio: 10 – 01-25
 - Fecha final: 20-01-25
- Determinar las capacidades de procesamiento, almacenamiento y red necesarias.
 - Fecha inicio: 14-01-25
 - Fecha inicio: 20-01-25

2.2.3. Miembro: Frances Simó Olmo

Rol asignado: Gestor de Riesgos.

Tareas específicas:

- Determinar la disponibilidad de recursos y planificar su adquisición o asignación.
 - Fecha inicio: 10-01-25
 - Fecha final: 13-01-25
- Enumerar los recursos materiales y humanos requeridos.
 - Fecha inicio: 10-01-25
 - Fecha final: 13-01-25
- Identificar posibles riesgos que puedan afectar el proyecto.
 - Fecha inicio: 14-01-25
 - Fecha final: 20-01-25
- Desarrollar planes de contingencia para mitigar los riesgos identificados.
 - Fecha inicio: 14-01-25
 - Fecha final: 20-01-25

2.3. Tareas en Equipo

Las **Tareas en equipo** que se abordarán a continuación incluyen la planificación de las tareas de manera conjunta de todos los miembros del equipo.

- Establecer los objetivos generales del CPD virtual.
 - o Fecha inicio: 09-01-25
 - o Fecha final: 10-01-25
- Determinar los requisitos funcionales y no funcionales.
 - o Fecha inicio: 09-01-25
 - o Fecha final: 10-01-25
- Revisar el plan completo del proyecto para asegurarse que todos los aspectos están cubiertos.
 - o Fecha inicio: 20-01-25
 - o Fecha final: 20-01-25
- Obtener la aprobación final por parte del profesor y los responsables del proyecto.
 - o Fecha inicio: 20-01-25
 - o Fecha final: 23-01-25

2.3.1. Miembros involucrados

Jonman Jiménez Mendoza - Líder del Proyecto.

Jaime Climent Cardona - Administrador de Infraestructura TI.

Frances Simó Olmo - Gestor de Riesgos.

2.4. Firmas

Al firmar este documento se está de acuerdo y comprometen a cumplir con las tareas y responsabilidades asignadas.



Jonman Jiménez Mendoza



Jaime Climent Cardona



Frances Simó Olmo

3. Análisis de requisitos

El **Análisis de Requisitos** que se presentará el análisis que incluyen, materiales, de seguridad, rendimiento y escalabilidad.

3.1. Materiales que se van a utilizar

3.1.1. Requisitos de Maquinaria

Todo el hardware que se va a necesitar.

3.1.1.1. Servidores

- **Servidor de aplicaciones:**
 - o Procesador: Mínimo 8 núcleos (AMD EPYC).
 - o Memoria RAM: 32 GB escalable a 64 GB.
 - o Almacenamiento: SSD de 1 TB con soporte para RAID 1.
 - o Sistema operativo: Windows Server (22.04 o superior)
- **Servidor de bases de datos:**
 - o Procesador: Mínimo 16 núcleos.
 - o Memoria RAM: 64 GB escalable a 128 GB.
 - o Almacenamiento: SSD de 2 TB con RAID 5.
 - o Sistema operativo: Windows Server (compatible con bases de datos)
- **Servidor de respaldo:**
 - o Procesador: Mínimo 4 núcleos.
 - o Memoria RAM: 16 GB.
 - o Almacenamiento: 4 TB HDD para backups incrementales y totales.

3.1.1.2. Estaciones de trabajo

- Procesador: Intel i5 o equivalente.
- Memoria RAM: 8 GB.
- Almacenamiento: SSD de 512 GB.
- Sistema operativo: Windows Server 22 (nos ofrecen la licencia el ayuntamiento).

3.1.1.3. Equipos de red

- Switches de red Gigabit con soporte para VLAN.
- Routers con redundancia y balanceo de carga.
- Firewall hardware para protección perimetral.
- Puntos de acceso Wifi de doble banda (2.4 GHz y 5 GHz).

3.1.1.4. Almacenamiento en red (NAS)

- Capacidad: 10 TB escalable.
- Soporte para RAID y replicación de datos.
- Compatible con protocolos SMB y NFS.

3.1.2. Requisitos de Software

Todo el software que se va a necesitar

3.1.2.1. Sistema de gestión

- Aplicación web para inscripciones y reservas.
- Compatible con navegadores modernos (Chrome, Edge, Firefox).
- Integración con pasarelas de pago seguras.
- Soporte para múltiples idiomas.

3.1.2.2. Bases de datos

- PostgreSQL o MySQL.
- Herramientas de replicación y respaldo automático.

3.1.2.3. Seguridad

- Software de monitorización de red.
- Antivirus y sistemas de detección de intrusiones.
- Certificados SSL para comunicaciones seguras.

3.1.2.4. Otras herramientas

- Sistema de virtualización: VMware o Proxmox.
- Software de backup: Veeam o Bacula.

3.1.3. Requisitos de Infraestructura de Red

3.1.3.1. Conectividad

- Conexión principal de alta velocidad: Mínimo 1 Gbps.
- Conexión redundante con proveedor diferente para garantizar la continuidad del servicio.

3.1.3.2. Diseño de red

- Segmentación de red mediante VLANs:
 - Red para gestión interna.
 - Red para usuarios finales.
 - Red de servidores.

3.1.3.3. Seguridad

- Firewall perimetral con inspección profunda de paquetes.
 - IPSec, encriptación de y autenticación de tráfico de red.
 - SNORT; Detección y prevención de intrusiones.
 - SSL; Inspección de tráfico cifrado.
- Redes privadas virtuales (VPN) para accesos remotos seguros, con los siguientes protocolos.
 - WireGuard; VPN moderna, segura y rápida.
 - OpenVpn; Protocolo basado en SSL/TLS.
 - IPSec; Alta Seguridad para túneles VPN en redes corporativas.
- Políticas de acceso basadas en roles.
 - LDAP; Para la gestión de permisos en los usuarios.
 - OAuth; Para autenticación federada en aplicaciones web.
 - RADIUS; Autenticación de usuarios en la red wifi empresarial.

3.1.3.4. Monitorización

- Implementación de herramientas de monitorización y alerta.
- Gráficos en tiempo real de consumo de ancho de banda y estado del hardware.

3.1.4. Escalabilidad y Disponibilidad

- Diseño modular que permita añadir servidores y almacenamiento según la demanda.
- Balanceo de carga para aplicaciones críticas.
- Clúster de bases de datos para alta disponibilidad.
- Plan de recuperación ante desastres.

4. Recursos necesarios

Los **Recursos Necesarios** que se abordarán a continuación, enfocados en el aspecto financiero del Proyecto para alojar el sistema de gestión de actividades deportivas de Tavernes, detallan el presupuesto requerido y su por qué.

4.1. PRESUPUESTO

4.1.1. HARDWARE

| ELEMENTO | CANTIDAD | COSTE (unidad) | COSTE TOTAL |
|--------------------------------------|----------|----------------|-----------------|
| Servidor de aplicaciones | 1 | 3.776 € | 3.776€ |
| Servidor de bases de datos | 1 | 4.777 € | 4.777 € |
| Servidor de respaldo | 2 | 3.000 € | 3.000 € |
| NAS (10TB escalable) | 1 | 1.500€ | 1.500 € |
| Estaciones de trabajo | 3 | 800 € | 2.400 € |
| Switches de red Gigabit (paquete 24) | 2 | 215 € | 430 € |
| Routers | 2 | 210 € | 420 € |
| AP Wifi | 1 | 137 € | 137 € |
| Medidas de seguridad fisicas | 1 | 3.500 € | 3.500 € |
| SAI | 1 | 278 | 278 |
| | | | 20.218 € |

- **Servidor de aplicaciones:** Son programas de servidor en una red distribuida que proporciona el entorno de ejecución para un programa de aplicaciones, es decir es el componente de tiempo de ejecución principal en todas las configuraciones y donde una aplicación se ejecuta.
- **Servidor de base de datos:** Hardware que permite organizar la información usando tablas, índices y registros.
- **Servidor de respaldo:** Es un tipo de servidor que facilita el respaldo de datos, archivos, aplicaciones o base de datos.
- **NAS:** Es un dispositivo de almacenamiento conectado a la red. Su función es hacer copias de seguridad de los archivos que tú le indiques.

- **Estación de trabajo:** Consiste en equipos que se emplean en cualquier trabajo con necesidades específicas, suelen formar parte de una red de trabajo donde se almacenan archivos y carpetas.
- **Switch de red:** Es un dispositivo informático que permite interconectar dispositivos a través de una red de área local o red LAN.
- **Router:** Es un dispositivo de hardware que sirve de punto de conexión entre una red local e Internet.
- **AP Wifi:** Es un dispositivo para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa.
- **Medidas de seguridad físicas:** Se encarga de proteger todo el hardware, aquí incluimos;
 - Extintores de CO2.
 - Detectores de humo y calor.
 - Aspersores de gas inerte (FM-200, Novec 1230).
- **SAI: O UPS (Uninterruptible Power Supply),** es un dispositivo que proporciona energía de respaldo en caso de fallos eléctricos.

4.1.2. SOFTWARE

| ELEMENTO | LICENCIAS | COSTE (unidad) | COSTE TOTAL |
|--|-----------|----------------|----------------|
| Sistema operativo servidores (Windows Server) | 4 | 0 € | 0 € |
| Soporte empresarial (MySQL) | 1 | 2.000 € | 2.000 € |
| Software de backup (Aomei Backup) | 1 | 700 € | 700 € |
| Sistema de virtualización (VMWare Workstation Pro) | 1 | 193 € | 193 € |
| Antivirus y herramientas de seguridad (F-Secure) | 10 | 10 € | 100 € |
| Monitorización (Pandora FMS) | 1 | 34 € | 34 € |
| | | | 3.027 € |

- **Sistema operativo servidores:** Es el software que se encarga de gestionar los recursos, servicios y usuarios. Windows Server se consideraría mejor opción para este proyecto ya que dependería del ayuntamiento de Tavernes

y este ya tiene la infraestructura hecha con Windows Server y las licencia se proporcionaría gratis por el ayuntamiento.

- **Soporte empresarial:** El soporte empresarial que hemos decidido utilizar ha sido el MySQL para poder gestionar la base de datos del polideportivo.
- **Software de backup:** Es la aplicación o los diferentes comandos y scripts que se utilizarán para poder realizar los backups del sistema y guardar-los.
- **Sistema de virtualización:** Es la tecnología que se puede usar para crear las representaciones virtuales de los servidores.
- **Antivirus y herramientas de seguridad:** Son las medidas de seguridad que se tienen en cuenta para que en caso de recibir algún ataque que no pueda ser una amenaza muy grande.
- **Monitorización:** Las medidas que se llevan a cabo para poder observar los servidores y prevenir fallos y tomar medidas a tiempo.

4.1.3. INFRAESTRUCTURA DE RED

| ELEMENTO | CANTIDAD | COSTE (unidad) | COSTE TOTAL |
|--------------------------------------|----------|----------------|-------------|
| Conexión principal (1Gbps) | 1 | 2.500 € | 2.500 € |
| Conexión redundante | 1 | 2.000 € | 2.000 € |
| Estructuración y montaje de cableado | 1 | 3.000 € | 3.000 € |
| | | | 7.500 € |

Conexión principal: Es la velocidad que tendrá que soportar nuestro servidor.

Conexión redundante: Es la velocidad de apoyo.

Estructura y montaje de cableado: Como se diseñará nuestra sala de servidores.

4.1.4. SERVICIOS PROFESIONALES

| ELEMENTO | HORAS ESTIM. | COSTE (hora) | COSTE TOTAL |
|---|--------------|--------------|----------------|
| Instalación y configuración de hardware | 50 | 50 € | 2.500 € |
| Configuración de software y pruebas | 60 | 50 € | 3.000 € |
| Auditoría inicial de seguridad | 20 | 80 € | 1.600 € |
| | | | 7.100 € |

- **Instalación y configuración de hardware:** Es el proceso de agregar o modificar los componentes físicos de un sistema informático, como discos duros, memorias, tarjetas gráficas, etc.
 - **Configuración de software y pruebas:** Son el proceso de evaluar y verificar que un producto o aplicación de software hace lo que se supone que debe.
- Auditoria inicial de seguridad:** Es un proceso estandarizado destinado a verificar que los sistemas informáticos y la información almacenada en los mismos cumplan con los estándares de seguridad requeridos.

5. Evaluación de riesgos y planificaciones de contingencias

La **Evaluación de Riesgos y Planificación de Contingencias** que se explicará a continuación identifica posibles problemas que podrían afectar al CPD. Esto incluye riesgos técnicos, operativos y de seguridad. Asimismo, se detallarán estrategias de mitigación y planes de contingencia para minimizar su impacto.

5.1. Identificación de riesgos

5.1.1. Riesgos tecnológicos

- **Fallo de hardware:** Posible avería de servidores, almacenamiento o componentes de red.
- **Fallo de software:** Errores en el sistema operativo, bases de datos o aplicaciones.
- **Ciberataques:** Malware, ransomware, accesos no autorizados.
- **Pérdida de datos:** Eliminación accidental, daño de alguno de los datos o fallos en las copias de seguridad.
- **Fallo de red:** Interrupciones en la conexión o caída de la red interna.

5.1.2. Riesgos ambientales

- **Fallo eléctrico:** Apagones, sobretensiones o fallos en la alimentación eléctrica.
- **Incendios o inundaciones:** Desastres naturales o incidentes que afectan a la infraestructura física.
- **Temperaturas extremas:** Fallo en el sistema de refrigeración que provoca un fallo.

5.1.3. Riesgos Humanos

- **Errores operativos:** Configuraciones erróneas, manipulación inadecuada de equipos o eliminaciones accidentales.
- **Sabotaje interno:** Actos intencionados de empleados con acceso al sistema.

5.2. Plan de contingencia

5.2.1. Medidas Preventivas

- **Monitoreo proactivo:** Implementación de sistemas de monitoreo en tiempo real (Zabbix/Nagios) para hardware, software y redes.
- **Backups regulares:** Copias de seguridad automatizadas y almacenamiento en una ubicación remota.
- **Firewall y seguridad perimetral:** Uso de firewalls avanzados, IDS/IPS y software antimalware.
- **Actualización y mantenimiento:** Aplicación de parches de seguridad y revisión periódica de sistemas.
- **Suministro eléctrico redundante:** Uso de UPS.
- **Capacitación del personal:** Formación en seguridad y procedimientos de emergencia para empleados.

5.2.3. Respuesta a accidentes

| Incidente | Acciones Inmediatas |
|---------------------|--|
| Fallo de hardware | Conmutación a servidores de respaldo, aviso a soporte técnico |
| Ciberataque | Aislamiento del sistema, análisis de logs, restauración de backup |
| Pérdida de datos | Restauración de la última copia de seguridad, análisis de causa |
| Corte eléctrico | Uso de UPS y generador, notificación a proveedor eléctrico |
| Incendio/Inundación | Activación de protocolos de evacuación, traslado a sitio alternativo |

5.2.4. Recuperación y Reanudación

- **Evaluación del impacto:** Análisis del incidente y sus efectos en la operatividad.
- **Restauración de servicios:** Implementación del plan de recuperación según la criticidad del sistema afectado.
- **Pruebas y verificación:** Validación de la integridad de los datos y correcto funcionamiento.

5.2.5. Sitio de respaldo

- **Ubicación alternativa** con servidores espejo listos para ser activados en caso de desastre.
- **Replicación de datos en tiempo real** para minimizar la pérdida de información.