CONFIDENCIAL

MEMORIA TÉCNICA

Contratación de los servicios de diseño, desarrollo, puesta en marcha, mantenimiento y alojamiento de los sitios web de la Empresa Municipal Mixta d'Aigües de Tarragona

EVELB TÉCNICAS Y SISTEMAS

1. ARQUITECTURA DE LA SOLUCIÓN Y CARACTERÍSTICAS DEL HOSTING 4

1.1. ARQUITECTURA DE LA SOLUCIÓN. 4
1.2. CARACTERÍSTICAS DEL HOSTING 10

2. SEGURIDAD 12

3. METODOLOGÍA DE MANTENIMIENTO.....16

3.1. MANTENIMIENTO CORRECTIVO. 16
3.2. MANTENIMIENTO PREVENTIVO. 17
3.3. MANTENIMIENTO EVOLUTIVO. 18
3.4. PLAN DE PRUEBAS..... 19
3.5. PROTOCOLO DE COMUNICACIÓN DE INCIDENCIAS. 20

CONFIDENCIAL

CONFIDENCIAL

Declaración de confidencialidad y protección de datos

La presente documentación es propiedad de evelb Técnicas y Sistemas S.L., tiene carácter confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de evelb Técnicas y Sistemas S.L, titular del Copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a la ley.

Cualquier dato, inclusive de carácter personal, entregado y/u obtenido por las partes como consecuencia de la provisión/recepción del Servicio, única y exclusivamente podrá ser utilizado o aplicado para dicho fin, no pudiendo ser entregados o cedidos a terceros bajo ningún título (salvo el tratamiento o acceso por aquellos terceros relacionados con la recepción/provisión del Servicio o aquellos casos en los que legalmente la parte viniera obligada, sirviendo en dicho caso esta cláusula como consentimiento expreso a tales efectos), ni siquiera a los meros efectos de su conservación. Las partes deberán adoptar las medidas de índole técnico y organizativas necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Los datos de contacto de los interlocutores proporcionados por el Cliente para la gestión de la presente solicitud de oferta comercial y/o relación contractual con evelb Técnicas y Sistemas S.L, así como para otras finalidades que nos permita o autorice en virtud de lo establecido en la Política de Datos de Empresa, cuyo contenido íntegro podrá consultar en la web *https://evelb.es/politica-privacidad/*. En este contexto, le rogamos que facilite esta información a los interlocutores cuyos datos se estén tratando por evelb Técnicas y Sistemas S.L.

En caso de que como consecuencia de la provisión del Servicio el proveedor de este accediera o implicara la realización de obligaciones o actuaciones que, según la normativa aplicable en materia de protección de datos, se consideren un encargo de tratamiento de datos de carácter personal, tales actuaciones nunca constituirán una cesión de datos por parte del Cliente a evelb Técnicas y Sistemas S.L, sino un tratamiento de datos personales por cuenta del Cliente que será el único responsable del tratamiento. En tal caso, las Partes formalizarán el correspondiente Anexo de encargo del tratamiento.

1. Arquitectura de la solución y características del Hosting

1.1. Arquitectura de la solución.

La solución propuesta por su entidad para la realización de la solución web es WordPress. En este sentido debemos indicar que nuestra empresa, a través del departamento de desarrollo e implementación web se encuentra especializada en la implantación de CMS entre los que podemos destacar tanto WordPress como Drupal.

En este contexto vemos la elección de WordPress como acertada, ya que es un gestor de contenidos cuya arquitectura está diseñada para ser muy flexible, extensible y fácil de usar, lo que conlleva una gran funcionalidad y unos altos estándares de calidad. En este sentido se realizarán nuevos desarrollos o integraciones de módulos que cubran las necesidades que se planteen desde a Empresa Municipal Mixta de Aguas de Tarragona.

A continuación, pasaremos a detallar pormenorizadamente la arquitectura de WordPress y así poder observar las características de esta herramienta y su potencial a la hora de poder realizar el sitio web de la Empresa Municipal Mixta de Aguas de Tarragona.

Modelo de base de datos: WordPress utiliza una base de datos MySQL de tipo relacional, donde se van a almacenar y gestionar todos los datos de la web. En esta base de datos podemos tener toda la información que queramos almacenar respecto al modelo que se ha implementado, desde contenidos de las páginas, entradas de blog, comentarios, configuraciones de temas y complementos, usuarios, así como los roles que los usuarios van a tener en el sistema.

Temas: Son los responsables de la apariencia visual y el diseño del sitio. La arquitectura WordPress nos permite la instalación y activación de temas personalizados, a criterio de cliente, en este caso la Empresa municipal de Aguas de Tarragona. De la misma manera que venimos trabajando con multitud de entidades locales, desde Evelb nos complace poder ofrecer nuestros servicios en este ámbito y poder gestionar la implementación de una serie de temas personalizados para nuestros clientes. Es importante destacar que esta arquitectura nos va a permitir realizar modificaciones durante todo el proceso de desarrollo de la web sin que esta pierda funcionalidad. Desde un punto de vista más técnico debemos decir que los temas se componen de diferentes

CONFIDENCIAL

tipos de archivos, PHP, CSS, JavaScript y plantillas HTML, que podemos combinar para permitir una salida visual limpia en el navegador.

API REST: La interfaz de programación de aplicaciones Reresentational State Transfer permite el acceso a los datos y funcionalidades del sistema desde aplicaciones externas. Proporciona puntos finales (endpoints) que permiten la creación lectura, actualización y eliminación de datos. También nos permite interactuar con WordPress utilizando diferentes lenguajes de programación y construir aplicaciones personalizadas utilizando sus datos y servicios. Todo esto nos permite una integración eficaz de su web con diferentes aplicaciones y servicios.

Complementos: Estos son conocidos como plugins y son extensiones que nos van a permitir agregar multiplicidad de funcionalidades diferentes a nuestro sitio web. Desde Evelb podemos ampliar la capacidad de su gestor de contenidos con la integración de este tipo de herramientas que nos va a permitir incluir formularios, establecer una integración con redes sociales, mejorar la SEO, implementar sistemas de reservas, entre otros muchos que se pueden implementar y que pueden ser consultados para su implantación a cualquier persona del departamento de desarrollo web de nuestra entidad.

Actualizaciones y seguridad: En Evelb entendemos la seguridad como algo primordial a la hora de implementar cualquier tipo de herramienta. En este sentido podemos decir que WordPress cuenta con un enfoque activo en la seguridad y en la corrección de errores, ya que continuamente se están lanzando actualizaciones que permiten corregir errores y agregar nuevas características. Una característica muy importante es la gran comunidad que se encuentra detrás de esta herramienta, la cual contribuye en gran medida a la detección y corrección de vulnerabilidades de seguridad que puedan surgir. Esta característica es muy apreciada ya que nos permitirá establecer altos estándares en la relación seguridad-calidad.

Sistema de permisos y roles: Podemos obtener una amplia gama de permisos y roles que nos van a permitir controlar el acceso y las capacidades de los/as usuarios/as en el sitio web. La característica principal de estos roles es la capacidad de tener diferentes niveles de accesos y permisos a la hora de trabajar dentro de la plataforma, podemos definir roles de administrador, editor, autor, colaborador o suscriptor, lo que nos permite obtener un alto grado de flexibilidad a la hora de controlar los accesos y poder estructurar de manera eficiente la entrada y salida de información.

Core de WordPress: Este es el núcleo central del sistema y proporciona la funcionalidad base para la gestión de todo el contenido. Incluye componentes

esenciales como la gestión de usuarios/as, la gestión de contenidos (páginas y entradas de blog), la gestión de comentarios y de taxonomías (categorías y etiquetas). El core es el encargado de procesar las solicitudes, interactuar con la base de datos y manejar la lógica principal del CMS.

Motor de consultas: Utiliza un motor de consultas basado en SQL para interactuar con la base de datos y recuperar la información necesaria para mostrar el contenido en el sitio web. La manejo del lenguaje SQL es fundamental para el desarrollo e implementación de consultas eficaces, que nos van a permitir optimizar la base de datos a través de la recuperación de los datos específicos que se requieran y la posibilidad de filtrarlos según las necesidades del sitio web.

Sistema de Cache: Para mejora el rendimiento y la velocidad de carga de las páginas ese sistema almacena en caché el contenido generado dinámicamente para evitar la generación repetida de las mismas páginas en cada solicitud. Para su desarrollo se utilizan diferentes técnicas como la caché de página completa, la caché de fragmentos y la caché de consultas de base de datos para acelerar la entrega del contenido al navegador lo que nos permitirá establecer una carga de página más rápida y eficaz.

Sistema de Gestión de archivos: Proporciona una gestión integral de medios que permite a los usuarios y las usuarias, subir y administrar archivos multimedia, como imágenes, video y documentos. Estos se almacenan en nuestro servidor y va a ser gestionado a través de la propia interfaz de WordPress. Los archivos multimedia pueden ser insertados tanto en las páginas como en las entradas del sitio web para su visualización.

Integración con servicios externos: Esta característica nos permitirá anexar servicios externos con la aplicación a través de una serie de complementos y extensiones que podemos integrar en la aplicación. Es posible conectar el sitio web con servicios de correo electrónico, servicios de almacenamiento en la nube, servicios de análisis y otras muchas herramientas. Esto nos va a permitir ampliar las funcionalidades de la web y establecer un mayor grado de personalización para su entidad.

Internalización y localización: Una de las características que entendemos primordial para la nueva web de la Empresa Municipal Mixta de Aguas de Tarragona es la capacidad de poder estar desarrollada en varios idiomas. En este contexto WordPress es una herramienta muy potente ya que es utilizado en todo el mundo, por lo que tiene una arquitectura que se adapta perfectamente al contenido del sitio web en diferentes idiomas y regiones. Esta arquitectura nos va a permitir poder crear, para su entidad, un sitio web multilingüe y adaptado a los requerimientos que desee con un alto grado de

accesibilidad y adaptado a audiencias tanto nacionales como internacionales.

Sistema de gestión de permalinks o enlaces permanentes: Este sistema nos permitirá ofrecer una mejor estructuración de las URL de las páginas y entradas al sitio web, lo que conlleva una mayor legibilidad y optimización en los motores de búsqueda. Una ventaja de estos permalinks es la capacidad de poder personalizarlos y generar de forma dinámica una serie de estructuras de páginas y entradas. Con esta herramienta podemos ofrecer la capacidad de personalizar la estructura de las URL de las páginas y entradas mediante la configuración de enlaces permanentes. Esto permite la creación de URL legibles y optimizadas para SEO, lo que mejora la navegación y la visibilidad del sitio web en los motores de búsqueda.

Estabilidad y rendimiento: Entendemos la escalabilidad como una cuestión fundamental a la hora de ofrecer un buen rendimiento, incluso en sitios web con elevado tráfico. En este sentido WordPress nos permite establecer una configuración personalizada en el servidor lo cual, nos va a capacitar para optimizar de manera óptima la base de datos, usar técnicas de caché apropiadas y la implementación de prácticas de desarrollo eficiente, lo que hace que podamos hacer frente a grandes volúmenes de visitas y garantizar un gran rendimiento para la web.

Gestión de sesiones y cookies: A través de la implementación de sesiones y cookies podemos gestionar la autenticación de los usuarios y las usuarias y proporcionar una experiencia personalizada. Las sesiones se van a utilizar para almacenar datos temporales sobre la interacción con el sitio web, mientras que las cookies se utilizar para recordar la información de inicio de sesión y otras preferencias de las personas que vayan a utilizar la plataforma.

Gestión de comentarios: Con este CMS podemos ofrecer un sistema de gestión de comentarios potente, incluyendo a las personas que visiten la web dejar sus comentarios en los lugares que desee su entidad. El sistema incluye funciones de moderación y aprobación de comentarios, así como la capacidad de filtrar y gestionar el spam. También debemos destacar el potencial que tiene la capacidad de poder establecer un sistema de comentarios personalizado a través de complementos específicos.

Sistema de búsqueda: Esta es una herramienta interna muy eficaz para toda persona que acceda a su web, ya que esta, podrá realizar consultas de búsqueda en la base de datos para encontrar coincidencias de palabras clave en el título y el contenido de las entradas. También es posible mejorar la funcionalidad de búsqueda utilizando una serie de complementos y extensiones específicas que pondremos a disposición de la

Empresa Municipal Mixta de Aguas de Tarragona.

Compatibilidad con estándares web: Es importante destacar que WordPress sigue los estándares web, como HTML5, CSS3 y accesibilidad web. Esto nos va a asegurar que su sitio web sea compatible con diferentes navegadores y dispositivos, y cumpla con las pautas de accesibilidad para personas en situación de discapacidad.

Integración con redes sociales: facilita la integración con redes sociales mediante complementos y widgets. Esto permite compartir contenido del sitio web en plataformas de social media, mostrar feeds de redes sociales en el sitio y permitir a los y las visitantes interactuar con el contenido utilizando sus cuentas de redes sociales.

Monitorización y análisis: Uno de los elementos fundamentales a la hora del desarrollo web en la actualidad, es la capacidad de poder realiza analíticas webs de calidad. En este sentido WordPress tiene la capacidad de poder integrar una serie de elementos para monitorización y análisis, como Google Analytics, para rastrear el rendimiento y el comportamiento de los y las visitantes. Esto nos permite ofrecerles datos valiosos para medir el éxito del sitio web, identificar patrones de uso y realizar mejoras en función de los análisis obtenidos.

Cron System: Este sistema permite la programación de tareas de manera automática, lo que se utiliza para gestionar, por ejemplo, entre otras muchas, la publicación de entradas programadas, la generación de copias de seguridad automáticas o el envío de notificaciones por correo electrónico.

Para el desarrollo y diseño de la página se implementará una plantilla base personalizada que se desarrollará en función del diseño planteado y de las funcionalidades propuestas. Esta será responsive, garantizando que el usuario y la usuaria tendrán una buena experiencia de navegación desde cualquier dispositivo, además será compatible con los navegadores webs más utilizados como Chrome, Firefox, Edge o Safari.

Los recursos usados en la plantilla serán libres de derechos de autor. El contenido de los apartados será configurable desde el panel de administración, existiendo elementos comunes como el menú principal, la cabecera o el pie de página.

La plataforma web contará con apartados de contenidos dinámicos como noticias o eventos; y estáticos donde se mostrará información más específica. Estas secciones se diseñarán pensando en las necesidades de los usuarios y las usuarias, haciendo contenidos atractivos usando recursos multimedia como imágenes, vídeos o mapas. El objetivo es que el usuario encuentre la información de manera rápida y sencilla.

La estética de una página web es lo primero que percibe el personal usuario. Junto con la usabilidad web, la sencillez y lo interesante que le pueda parecer el contenido, será lo que determine si se mantiene navegando sobre la misma o no. En este sentido debemos decir que el equipo de diseño de evelb se encuentra en continua búsqueda de las últimas tendencias en diseño y funcionalidad, lo que nos ayuda a obtener siempre resultados actualizados y más perdurables en el tiempo, de tal manera que la web no se quede anquilosada en aspectos visuales. Uno de estos casos puede ser el empleo de imágenes como reclamo de atención para acceder a nuevo contenido, o el diseño de iconos personalizados que ayuden al usuario a identificar la información que encontrará bajo el mismo.

Como hemos comentado nuestra base para el diseño de la web será el diseño responsive. Esta técnica se utiliza en el diseño e implementación de sitios web con un objetivo específico, que las diferentes páginas que forman parte del portal web puedan ser visualizadas correctamente en todos los dispositivos que intenten acceder a ella, tanto portátiles, tabletas como móviles.

Para cumplir con este objetivo, la plantilla personalizada se diseñará adaptando los contenidos al ancho de cada dispositivo, de esta forma se controlará que todos los elementos escalen correctamente, y mejoren la experiencia del usuario. Estos contenidos se modificarán mediante media-queries en CSS3 estableciendo diferentes rangos de resoluciones para proporcionar una adaptación a los diferentes anchos de pantalla de los dispositivos:

- Resolución XS/SM (Desde 0px hasta 767px de ancho):
- Este rango de resoluciones está orientado a móviles, tanto en posición vertical como horizontal.
- Resolución MD/LG (Desde 768px hasta 1200px de ancho):
- Rango utilizado para tablets orientadas tanto en vertical como en horizontal. También incluye ordenadores portátiles pequeños.
- Resolución XL (A partir de 1200px de ancho):
- Rango que incluye todas las pantallas grandes de ordenador.

Además del uso de las media-queries también se utilizarán las diferentes herramientas que nos proporciona el framework Bootstrap. Esta librería cuenta con infinidad de clases preparadas para adaptar el contenido en función del tamaño de la pantalla.

La combinación de ambas herramientas permitirá aportar a la plantilla una gran

flexibilidad cuando se cargue el contenido desde diferentes dispositivos e incluso desde diferentes navegadores web. Hoy en día los diferentes buscadores web como Google o Bing también disponen de scripts y diferentes métricas y logaritmos que puntúan si una web está correctamente diseñada en los diferentes dispositivos, influyendo notablemente en los resultados de las búsquedas y en la autoridad que estos le otorgan.

1.2. Características del Hosting

Teniendo en cuenta las características de WordPress, creemos que la configuración del hosting debe ser especialmente indicado para la implementación de este CMS. En este caso en particular, proponemos un servidor con sistema operativo Linux (PHP-FRM versiones desde la 5.6 hasta la 8.2), el sistema gestor de base de datos será MariaDB, con CPU de 8 núcleos, memoria RAM de 16 GB, espacio en el disco de 600 GB, tráfico ilimitado, VPS administrado y hasta 50 licencias de hosting diferentes.

A continuación, procedemos a describir con más detalle las características propias del hosting:

- **Conectividad y ancho de banda:** Nuestro servicio de hosting ofrecerá una conectividad redundante garantizada con máximas prestaciones de redundancia y mínimas latencias que nos permitirá garantizar una conexión máxima de velocidad en todo momento, conectividad BGP con acuerdos peering con las principales operadoras. Debemos destacar que el ancho de banda del hosting será de 100Mbps
- **Gestión de copias de Seguridad:** Para mejorar la seguridad de la web se incorporarán una serie de copias de seguridad automáticas tanto de carácter diario como semana, a requerimiento su entidad. Esto nos permitirá, en caso de cualquier problemática, la restauración completa del sitio web de manera sencilla y con los parámetros de configuración ya existente. Estas copias se podrán almacenar tanto en el propio servidor o a través de servicios de alojamientos de archivos en la nube tales como, Amanzon S3 o DropBox.
- **Seguridad en los servidores.** La red de hosting contará con un firewall perimetral. Este tipo de firewall añade protección extra a su red de computadoras haciendo que se limiten los posibles ataques a los puertos más vulnerables de los equipos y servidores, así como los accesos no autorizados, y la mayoría de los códigos maliciosos. Otra característica del firewall perimetral será el aislamiento de peticiones e ips con mala reputación. Este firewall filtrará por ips y conexiones y dispondrá de un WAF a nivel de servidor web que protegerá

contra peticiones maliciosas. Para garantizar la seguridad en el servidor se realizarán una serie de procesos periódicamente:

- **Limpieza de malware:** Se usará la herramienta Google Safe Browsing, que nos permite examinar las webs que se van indexando para poder determinar y buscar contenidos no seguros o malware. Esta herramienta identifica como no seguros los sitios que pueden poner en riesgo la vulnerabilidad del beneficiario o beneficiaria del servicio, incluyendo software malicioso o suplantación de identidad. Este servicio también nos informará sobre las amenazas que afecten a las IP alojadas en el servidor. En el caso de detectar alguna amenaza se alertará del problema a las personas afectadas y se tomarán medidas oportunas para la resolución del problema en el menor tiempo posible.
- **ModSecurity**: Es un firewall de aplicaciones web que filtra las peticiones HTTP antes de enviarlas al servidor. Funciona mediante una serie de reglas determinadas y funcionales a través de las cuales se genera determinadas acciones tales como rechazar o ignorar. Entre los ataques que se pueden filtrar se encuentran los fallos conocidos de aplicaciones, las anomalías de protocolos, los troyanos, los robots maliciosos, entre otros muchos; también bloque ataques de fuerza bruta, vulnerabilidades de cross scropting (XSS), ataques por inyección SQL (SQLi). Destacamos la posibilidad de establecer reglar propias para el ModSecurity, en función del tipo de incidencias que podamos detectar y que nos permitirá reforzar aún más si cabe la protección de su web.
- **Correo electrónico:** Para una mayor seguridad se monitorizarán las cuentas de correo del hosting. Se realizarán las comprobaciones pertinentes que nos permitan detectar si se accede a la aplicación web desde países poco comunes entre las personas usuarias. Esto nos permitirá conocer si la cuenta de esa persona ha podido ser hackeada y se procederá a realizar una notificación para que esa persona pueda realizar cambios para que se reestablezca la seguridad de su cuenta.

Se mejorará la seguridad de los diferentes formularios integrando el sistema de Google reCaptcha para evitar la llegada de mensajes spam. Esta extensión utiliza un motor de análisis de riesgos avanzado y CAPTCHA adaptables para evitar que el software automatizado participe en actividades abusivas en su entorno web.

Para aumentar la seguridad proponemos un cambio en la ruta del acceso al formulario de inicio de sesión que nos va a permitir incrementar la personalización y seguridad de acceso al panel de gestión.

Con respecto a los protocolos HTTP y HTTPS, la página web permitirá el uso de los dos protocolos de comunicación, tanto el no seguro HTTP como el seguro HTTPS. Se realizarán la configuración de los servidores para la aceptación de conexiones HTTPs, creando un certificado de clave pública, que estará firmado por una autoridad de certificación para que el navegador puede acceder a su verificado.

Entendemos que poner a disposición el certificado SSL es de vital importancia ya que la información, altamente sensible, que se transmite a través de la web se encuentra protegida y no puede ser interceptada, leída ni manipulada por terceros. En otras palabras, el intercambio de información entre el servidor y la persona usuaria está encriptada mediante algoritmos de alta eficiencia.

2. Seguridad

Desde Evelb entendemos y estamos firmemente comprometidos con la seguridad en todos los proyectos que desarrollamos e implantamos. En este sentido proponemos la realización de un protocolo de seguridad a dos niveles; el primero de ellos tendría como principal enfoque la implantación de una serie de medidas en materia de seguridad que se implantarán directamente sobre la plataforma web y el segundo un protocolo de hacking ético, donde, finalizada la implementación de la web se realizarán una serie de pruebas periódicas que permitirá conocer el estado en materia de seguridad de la plataforma.

El primer protocolo, como hemos comentado, sería la implantación de una serie de medidas de seguridad determinadas a la mayor seguridad posible de la plataforma, estas medidas son:

Gestión de logs: Para la monitorización de usuarios, errores y acciones maliciosas se utilizará el plugin Cerber Security. Ésta es una herramienta muy polivalente que monitoriza toda la actividad las personas usuarias y sus interacciones con la web. Si detecta alguna actividad maliciosa, bloqueará la dirección IP de esa persona, para posteriormente dar la opción al administrador de mantener el bloqueo o quitárselo. Toda la información es almacenada en log con el fin de llevar un registro de todos los datos obtenidos e partir de la web. El plugin también dispone de avisos periódicos a las direcciones de correo electrónico indicadas, permitiendo de esta forma dar constancia de todas las actividades realizadas en la web. Además de este tipo de acciones, también monitoriza datos del servidor como uso de la memoria, posibles errores etc.

Copias de seguridad. Como hemos comentado en el apartado anterior, se realizará copias de seguridad de todos los Servicios Administrados. Nuestro sistema de Backups

CONFIDENCIAL

hace una copia incremental cada día, de madrugada, y además una copia completa durante el fin de semana. Estas copias son almacenadas durante un mes como máximo. Esto quiere decir que se puede restaurar, si lo necesita la entidad, como tiempo límite, los contenidos correspondientes a los 30 días anteriores.

ReCaptcha: También comentado en el apartado anterior se mejorará la seguridad de todos los formularios a través del sistema reCaptcha de Google para evitar la llegada de mensajes spam.

Actualizaciones: WordPress es un gestor de contenidos en constante evolución por lo que es necesario su actualización para disponer tanto de las últimas funcionalidades, mejoras de estabilidad, rendimiento, corrector de errores detectados en versiones anteriores como parches de seguridad, que pueden atacar la vulnerabilidad de la aplicación. La experiencia es un grado y desde el departamento de diseño web de evelb proponemos un pequeño protocolo anterior a cualquier actualización. El primer paso a realizar será una copia de seguridad, que permitirá recuperar la página web al estado anterior si se produce algún fallo durante la actualización. Este backup realizará una copia de los archivos del sitio y de la base de datos, esto nos dará una perspectiva clara y un punto agregado para poder analizar la situación para conocer si tenemos o no la necesidad de esa actualización y un medio para comprobar que todos los plugins y añadidos sean compatibles con la nueva versión. Con este protocolo evitamos que exista ningún problema. Las actualizaciones se realizarán primero en los entornos de desarrollo para comprobar que todo funcione correctamente y si en caso de que algo no funcione la web seguirá siendo activa no impidiendo el buen desarrollo de la actividad. Cuando se detecte algún problema de actualización se procederá a subsanarlo y cuando funcione correctamente en el entorno de desarrollo se procederá a la actualización final de la plataforma, para que de esta manera conserve toda su funcionalidad.

Aquí debemos destacar que este CMS incorpora un sistema de actualizaciones desde donde se podrán gestionar 4 tipos diferentes:

- Actualizaciones de núcleo: que a su vez se dividen en tres categorías
    - Actualizaciones de desarrollo (versión beta o relase candidate RC)
    - Actualizaciones menores de mantenimiento y seguridad.
    - Actualizaciones mayores.
- Actualizaciones de plugins
- Actualizaciones de temas

CONFIDENCIAL

- Actualizaciones de ficheros de traducción.

Resolución de Problemas: Este apartado es primordial a la hora de establecer este protocolo ya que, conocer e identificar el error y la causa que lo provoca, nos va a lleva a poder solucionarlo en la mayor brevedad de tiempo posible. WordPress incorpora una serie de herramientas de manera nativa que nos permite explorar los registros y las actividades que se han realizado y detectar de manera muy eficiente el error para poder aislarlo y corregirlo. Estas herramientas son:

- **WordPress Modo Recovery:** A partir de la versión 5.2, se incorporó esta herramienta para identificar errores. En caso de que se produzca uno, la plataforma lo detectará automáticamente y enviará un mail a la cuenta del administrador. Este contendrá un enlace específico que nos permitirá acceder al panel de control con este modo de recuperación. Una vez dentro y logeado, se desactivarán todos los temas, plugins, widgets y cualquier programa ajeno que pueda entrar en conflicto. De este modo podremos activar todas las funcionalidades una a una e identificar de un modo muy concreto de donde proceder el error. Esta herramienta es muy potente porque nos garantiza una pronta respuesta ante cualquier problemática que se produzca en la plataforma.
- **WordPress Debug:** Este modo se activa modificando una línea de código en el archivo de la carpeta raíz wp-config.php. Una vez activado se nos mostrará los errores que tiene el código php dentro del sitio web. Además de esto, también generará un archivo de log donde se mostrará un registro de todas las actividades realizadas con todos los errores incluidos. Con todos estos datos de procederá a identificar el origen de los errores y porqué se están produciendo lo que nos permitirá subsanar la problemática rápidamente.
- **Query Monitor:** Este método de detección de errores está orientado a problemas de gran calado, como problemas graves de optimización y errores relacionados con el tema o plantilla del sitio web. Par esto se instalará el plugin correspondiente y una vez activado tendremos a nuestra disposición una serie de acciones disponibles para analizar en cada una de las páginas, tales como queries duplicadas, bucles, consultas de plugins mal optimizadas u obsoletas que pueden llegar a consumir recursos de una manera desproporcionada.

Por último, debemos destacar la opción de ver un resumen de todas las variables de configuración y entorno en el propio WordPress, donde se incluyen las configuraciones

que se han establecido, los valores declarados o las extensiones cargadas.

Con todas las herramientas anteriormente expuestas, podemos realizar una valoración muy eficaz y efectiva de los problemas que nos podemos encontrar y de esta forma entender la manera más rápida e integradora de poder subsanar las posibles problemáticas que puedan ir surgiendo.

- **Cerber Security**: Para mejorar la seguridad del portal se instalará el plugin Cerber Security. Este tiene una serie de complementos que permite defender a la web contra ataques de hackers, spam y malware. Este plugin bloqueará la actividad maliciosa antes de que dañen los datos gracias a un conjunto de algoritmos internos que mitigan los ataques de fuerza bruta al limita el número de intentos de inicio de sesión a través del formulario de inicio de sesión, las solicitudes API XML-RPC / REST o el uso de cookies de autenticación.

Por último, debemos indicar que para mayor seguridad también se cambiará la ruta de acceso al panel de administración que por defecto es /wp-admin/ por una personalizada y así evitar ataques lanzados contra esta URL.

Con respecto al segundo protocolo de seguridad proponemos un **plan de hacking ético**. Este plan se llevará a cabo con posterioridad a la implementación de la plataforma y tendrá se llevará a cabo con una periodicidad consensuada por las dos partes.

Para la realización del plan de hacking ético, primeramente, se llegaría a un acuerdo para reflejar las diferentes pruebas que se van a poder realizar sobre la plataforma web de la Empresa Municipal Mixta de Aguas de Tarragona.

Debemos destacar que nuestro plan de hacking ético contempla diversas acciones para manera la seguridad de la plataforma, controlando los accesos al servidor y al gestor de base de datos. Son muchas las técnicas que podemos utilizar para asegurar la integridad en la seguridad y vemos necesarias implementar estas acciones, dentro de nuestros proyectos, para que personas, empresas u otras entidades malintencionadas no puedan obtener información confidencial de su portal web.

Con el acuerdo de las técnicas a utilizar se pasará a una segunda fase en la que nuestro objetivo es recopilar información acerca de la seguridad del portal web y posibles vulnerabilidades que puedan surgir a través de su funcionamiento. Para ello se establecerán una serie de búsqueda por internet y se intentará encontrar contraseñas o patrones, que hemos recabado dentro del proceso de búsqueda, para lograr acceder al portal haciéndonos pasar por las personas usuarias del mismo. Aquí ponemos de relieve la importancia de tener unas contraseñas fuertes para mantener proteger el portal, por

lo tanto, no se dejará que se puedan utilizar contraseñas débiles al respecto.

En segundo lugar, se realizarán ataques de inyección SQL. Este tipo de ataques puede diseñar una cadena utilizando comandos específicos de Structured Query Language (SQL), lo que puede alterar la base de datos de la plataforma de manera que puede darse el caso de que pasemos a no poder controlarla. En este caso introduciremos una serie de comandos en lugares específicos como las cajas de búsqueda, formas de inicio de sesión, formularios e incluso directamente en una url, para así poder mitigar este tipo de ataques.

En tercer lugar, se harán ataques de denegación de servicidos (DDos) para intentar dejar inoperativo el funcionamiento de la web. Esta técnica intenta inundar un sitio web con solicitudes externas, para que no pueda estar disponible para las personas usuarias. Estos ataques tienen tres variantes:

1. Ataques de volumen: donde el ataque intenta desbordar el ancho de banda en un sitio web determinado.
2. Ataques de protocolo: donde los paquetes intentan consumir servicios o recursos de la red.
3. Ataques a aplicaciones: donde las peticiones se hacen con la intención de hace “explotar” el servidor web, mediante la capa de aplicación.

En cuarto y último lugar se hará una técnica que se denomina Cross-Site Scripting (XSS) o ejecución de comandos en sitios cruzados, este tipo de vulnerabilidades puede ser explotada de dos maneras:

1. Reflejada: consiste en modificar valores que la aplicación web usa para pasar variables entre dos páginas.
2. Almacenada: consiste en insertar código HTML peligroso en sitios web que lo permitan. De esta forma quedará visible a los usuarios que ingresen en el sitio modificado.

Para ayudarnos para la realización de alguna de estas pruebas utilizamos el software OWASP ZAP.

3. Metodología de mantenimiento.

3.1. Mantenimiento correctivo.

Consiste en la revisión y corrección de problemas de seguridad, estabilidad, errores en

CONFIDENCIAL

el código, falta de rendimiento a causa del hardware, etc. Nuestro trabajo de mantenimiento preventivo de software permitirá disponer de evaluaciones periódicas que optimicen los resultados de nuestros programas, corrigiendo errores que pudieran producirse gracias al mantenimiento correctivo de equipos, así como en el mantenimiento correctivo de cara a acciones futuras.

3.2. Mantenimiento preventivo.

Los componentes informáticos que forman una página web reciben periódicamente modificaciones para incrementar su seguridad o corregir posibles riesgos, por lo que un sitio web debe mantenerse al día. Con este tipo de mantenimiento se buscará prevenir posibles problemas en un sitio web, adelantándose a ellos para que no sucedan.

Estas son algunas tareas de mantenimiento preventivo:

- **Aplicar actualizaciones y parches de seguridad en servidores**: con cierta regularidad se descubren problemas de seguridad en el software de los servidores web. Dejarlos sin actualizar supone correr el riesgo de ser atacados y sufrir robos de información, utilizar nuestros servidores web para el envío de correo basura u otras actividades fraudulentas, o simplemente dejar nuestro sitio web fuera de servicio.
- **Aplicar actualizaciones y parches de seguridad en el software del sitio web:** además de los problemas del servidor (por ejemplo, el sistema operativo) pueden descubrirse problemas de seguridad o rendimiento en el software utilizado por el sitio web. En estos casos también hay que aplicar las actualizaciones de seguridad lo antes posible. Esta tarea incluye actualización de Plugins, temas y Wordpress, además se revisará el funcionamiento correcto de la web.
- **Actualizar versiones obsoletas:** las versiones de software utilizadas finalizan su vida (ya no tienen soporte técnico) y deben ser sustituidas por nuevas versiones. Al no tener soporte técnico, los problemas de seguridad que van apareciendo no son corregidos, dejando en riesgo a los sitios web que utilizan esas versiones.
- **Copia de seguridad:** se realizarán copias de seguridad semanales tanto de la web como de la base de datos.
- **Revisión de seguridad y rendimiento de la web:** usando herramientas web que permiten identificar diferentes aspectos del sitio web como SEO, visibilidad

en redes sociales, semántica web, calidad de código, optimización para móviles, entre otros.

- **Analítica web:** Revisión Mensual de herramientas Search Console de Google y BING para detectar errores de rastreo. Revisión mensual de visitas de la web con informe de resultados.
- **Posicionamiento web (SEO):** Es imprescindible revisar regularmente el posicionamiento web, estudiar su evolución y analizar las oportunidades existentes para garantizar el tráfico a la página web.
- **Vigilancia de registros de acceso:** lo sitios web crean un registro de todas las solicitudes que reciben. Su uso más habitual suele ser obtener estadísticas de uso, del tráfico web, pero también pueden servir para detectar intentos de acceso fraudulentos, páginas que no se encuentran o páginas que producen algún tipo de error y que requieren alguna corrección en el sitio web.

3.3. Mantenimiento evolutivo.

El mantenimiento evolutivo y adaptativo comprende las acciones a llevar a cabo en función de determinadas necesidades surgidas a partir de diferentes análisis e indicadores.

Estas tareas para desarrollar pueden ser el resultado del análisis de los logs del portal web, mediante los cuales se tutelará el comportamiento de las misma y que en un determinado momento puede indicar la necesidad de un cambio o evolución.

Otro factor desencadenante de una tarea evolutiva o adaptativa, puede ser la obsolescencia de alguno de los sistemas o tecnologías, así como la aparición de nuevas versiones de los mismos.

Por otra parte, además de ofrecer la posibilidad de realizar una evolución sugerida por iniciativa tanto de Evelb como del cliente, se propone un análisis mensual de la situación de los sistemas, para determinar necesidades de evolución o adaptación.

Debido a las buenas prácticas de clean code y metodologías ágiles que se emplearán durante el desarrollo del contrato, las tareas de mantenimiento pueden surgir pueden surgir desde el primer despliegue en pre-producción del producto obtenido en el primer sprint.

Estas acciones de refactorización de código podrían englobarse dentro del denominado mantenimiento perfectivo, que consideramos que debe llevarse a cabo junto al evolutivo y adaptativo. Como mantenimiento evolutivo podríamos calificar las tareas a llevar a

cabo para cubrir la expansión o cambio en las necesidades del cliente.

Dentro del mantenimiento adaptativo se encuentran las acciones necesarias para adecuarse a cambios en el entorno tecnológico, legislación, etc…

3.4. Plan de pruebas

Las pruebas son un mecanismo clave que evelb propone específicamente para garantizar los servicios al cliente. Este enfoque define funciones específicas dentro del equipo técnico para los testers y establece cuatro niveles de prueba. Los niveles también definen la distribución de las actividades de prueba en el equipo del proyecto entre los desarrolladores y los testers.

Evelb alineará la adopción de estos cuatro niveles con el marco de desarrollo de software Scrum propuesto para el proyecto y con el entorno de integración continua. La definición de las actividades en el ámbito de cada sprint incluirá los diferentes niveles de pruebas.

El plan de pruebas es un conjunto de casos de pruebas que se encarga de probar una funcionalidad completa de un producto o software en concreto.

Evelb creará un plan de pruebas donde se definirán para cada funcionalidad las pruebas necesarias para su validación. Los casos de prueba a diseñar deben cubrir los aspectos funcionales y no funcionales del sistema. Para el diseño de los casos de prueba el equipo debe utilizar como bases de prueba entregables tales como requerimientos iniciales, historias de usuario, diseños, manuales técnicos, manuales de usuario, …

Cada caso de prueba estará compuesto por:

- El tipo de prueba.
- El tipo de usuario que realizará la prueba (administrador, editor, usuario autenticado, usuario anónimo, …)
- La definición de las condiciones que se deben cumplir para alcanzar las metas y objetivos.
- La definición de lo esperado en la realización de la prueba.
- Resultado esperado.

A continuación, se definirán los cuatro niveles de prueba con una breve descripción de cada uno:

- **Pruebas unitarias o de componente**: son ejecutadas por el equipo de desarrollo en sus entornos locales. Básicamente consisten en comprobar que

CONFIDENCIAL

los componentes unitarios están codificados cumpliendo lo esperado de la funcionalidad, que se validan los datos erróneos o inesperados.

- **Pruebas de integración**: son ejecutadas por el equipo de desarrollo en el entorno de desarrollo. Consisten en comprobar que las funcionalidades que interactúan entre sí funcionan de manera correcta.
- **Pruebas de sistema:** deben ser ejecutadas idealmente por un equipo de pruebas ajeno al equipo de desarrollo. Estas pruebas se realizarán en el entorno de desarrollo o preproducción. Se debe ejecutar el plan de pruebas completo, de esta forma se verifica que la funcionalidad total del sistema fue implementada de acuerdo con el documento funcional definido en el proyecto.
- **Pruebas de aceptación:** deben ser ejecutadas por personal asignado por el cliente. Deben ejecutar todos los procesos de negocio para la ejecución de pruebas de aceptación. Es incluso recomendable que los usuarios finales que participan en este proceso sean independientes al personal que apoyó el proceso de desarrollo. Cuando las pruebas de aceptación son ejecutadas en el entorno de desarrollo, se les denominan pruebas Alpha, cuando son ejecutadas en el entorno de preproducción se les denomina pruebas Beta. En los casos en que las pruebas de aceptación del producto se hayan ejecutado en el entorno de desarrollo, el aplicativo no podrá salir a producción, sin que se hayan ejecutados las respectivas pruebas Beta en el en el entorno de preproducción, en el caso de no existir, deben realizarse directamente en el entorno de producción. Es importante concluir, que las pruebas Alpha son opcionales, pero las pruebas Beta son obligatorias.

3.5. Protocolo de comunicación de incidencias.

Durante el periodo del contrato se realizará la publicación, creación y actualizaciones de contenidos de manera diaria. Se pondrá a disposición de EMTASA una dirección de correo electrónico y un número de teléfono para la comunicación de incidencias, peticiones o consultas disponibles.

El equipo de mantenimiento y soporte de Evelb utilizará un sistema de tickets en línea (Help Desk OTRS), para organizar, seguir y gestionar las solicitudes de soporte. Evelb proporcionará un informe de finalización de cada tarea que muestre claramente las horas utilizadas.

Debemos destacar que, por experiencia, elegimos la herramienta Help DesK OTRS por dos razones principalmente; la primera por su ágil gestión que nos permite ofrecerle una

gran calidad en el soporte y dos por los buenos resultados que recogidos hasta la fecha por nuestra entidad.

OTRS es uno de los sistemas Help Desk de tickets web más flexibles del mercado y se emplea en la asistencia a clientes, la asistencia de escritorio y la gestión de servicios informáticos.

Su implementación y uso es muy sencillo, lo que facilita la adaptación a las diferentes necesidades que se planteen y se ofrece servicio de soporte las 24 horas de todos los días del año.

3.5.1. Alta de incidencias

El alta de incidencias dentro del OTRS se puede generar de dos maneras:

- Alta directa: Crear una nueva incidencia a través del panel de gestión (incidencia telefónica)
- Alta a través de email: Cualquier usuario puede generar una incidencia enviando un email a la cuenta de correo generada para ello.

Cada incidencia presente, generará de forma automática un ticket y se compondrá de:

- Referencia asignada: Código identificativo compuesto por letras y números
- Nivel de prioridad: Crítica, Alta, Media o Baja
- Ubicación
- Fecha y hora de apertura y registro
- Breve descripción
- Personal técnico asociado

3.5.2. Procedimiento

Registro

Cada reporte recibido, independientemente del canal de comunicación, se registrará en el OTRS. Contará con un número/ código identificativo, una descripción, persona vinculada a la misma y será clasificada en solicitud o incidencia.

Priorización y Categorización

<u>Categorización</u>

Una vez recibida una incidencia/ solicitud, esta es clasificada en las categorías

CONFIDENCIAL

previamente creadas y aprobadas por el responsable del proyecto de su entidad.

Priorización

Dependiendo de las características de las incidencias estas se clasificarán en 4 niveles:

Baja: Incidencias que no afectan al correcto funcionamiento de los portales.

Media: Incidencias que impliquen un impacto mínimo en los servicios.

Alta: No funcionamiento de procesos esenciales.

Crítica: Corte total del servicio

Esta priorización es esencial para asegurarse de que se están solucionando aquellos incidentes que primero lo requieren.

3.5.3. Resolución

Una vez la incidencia ha sido resuelta, se le pasa por una serie de pruebas de calidad y correcto funcionamiento. Toda esta nueva información será trasladada al OTRS, lo cual nos implementaría un cambio de estado de la incidencia. Esta información será notificada a la persona implicada y al responsable de forma inmediata una vez se haya completado el contenido de la resolución.

Así pues, en el momento en el que se recibe una incidencia, independientemente del canal empleado, esta será registrada en el OTRS por el técnico de soporte. La tarjeta se cubrirá con todos los datos indicados anteriormente y se generará un email automático que se enviará al técnico/a vinculado.

Esta incidencia será analizada al momento por el personal técnico y se comenzará a ejecutar la resolución cumpliendo siempre con los plazos establecidos.

Una vez la incidencia ha sido resuelta, se establecerá contacto con la persona solicitante, donde se le informará del estado y se procederá a cerrar la incidencia dentro del OTRS.

Para una mayor organización, las incidencias podrán ser organizadas por categorías definidas en la reunión inicial.

CONFIDENCIAL

CONFIDENCIAL

Declaración de confidencialidad y protección de datos

La presente documentación es propiedad de evelb Técnicas y Sistemas S.L., tiene carácter confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo,tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de evelb Técnicas y Sistemas S.L, titular del Copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a la ley.

Cualquier dato, inclusive de carácter personal, entregado y/u obtenido por las partes como consecuencia de la provisión/recepción del Servicio, única y exclusivamente podrá ser utilizado o aplicado para dicho fin, no pudiendo ser entregados o cedidos a terceros bajo ningún título (salvo el tratamiento o acceso por aquellos terceros relacionados con la recepción/provisión del Servicio o aquellos casos en los que legalmente la parte viniera obligada, sirviendo en dicho caso esta cláusula como consentimiento expreso a tales efectos), ni siquiera a los meros efectos de su conservación. Las partes deberán adoptar las medidas de índole técnico y organizativas necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida tratamiento o acceso no autorizado, habidacuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuestos, ya provengan de la acción humana o del mediofísico o natural.

Los datos de contacto de los interlocutores proporcionados por el Cliente para la gestión de la presente solicitud de oferta comercial y/o relación contractual conevelb Técnicas y Sistemas S.L, así como para otras finalidades que nos permita o autorice en virtud de lo establecido en la Política de Datos de Empresa, cuyocontenido íntegro podrá consultar en la web *https://evelb.es/politica-privacidad/*. En este contexto, le rogamos que facilite esta información a los interlocutores cuyos datos se estén tratando por evelb Técnicas y Sistemas S.L.

En caso de que como consecuencia de la provisión del Servicio el proveedor de este accediera o implicara la realización de obligaciones o actuaciones que, según la normativa aplicable en materia de protección de datos, se consideren un encargo de tratamiento de datos de carácter personal, tales actuaciones nuncaconstituirán una cesión de datos por parte del Cliente a evelb Técnicas y Sistemas S.L, sino un tratamiento de datos personales por cuenta del Cliente que seráel único responsable del tratamiento. En tal caso, las Partes formalizarán el correspondiente Anexo de encargo del tratamiento.