Publicación y seguridad de un portafolio web

Universidad CENFOTEC

Portafolio Profesional

Estudiantes:

Rolando Quiros Artavia

Gabriel Porras Brenes

Alexander Quesada Vargas

Profesor:

Francisco Jose Jimenes Bonilla

Fecha: 4, 2024

Tabla de Contenido

Elección del Servicio de Alojamiento (Hosting)

Existen diversos servicios de alojamiento web, con diferentes características, sin embargo vamos a mencionar 3 de estos servicios que se adaptan a nuestras necesidades:

1. HostGator es una de las principales plataformas de alojamiento de sitios web desde hace mucho tiempo. No sólo ofrece alojamiento compartido, VPS y dedicado como su rival, Bluehost, sino que también tiene planes de alojamiento que incluyen un editor de sitios web con la función drag-and-drop que facilita la creación de páginas.

   Un beneficio que obtendrás con HostGator es que incluso los planes básicos ofrecen almacenamiento y ancho de banda no medidos, lo que elimina la preocupación de la futura escalabilidad de tu sitio.

- Precio: Los planes van desde 3 a 140 dólares al mes.
- Ancho de banda: Ilimitado
- Almacenamiento: Ilimitado

2. GoDaddy entró en el mercado con sus planes de compra de dominios a finales de los 90. Ahora, además de alojamiento de sitios web, esta plataforma ofrece gestión DNS avanzada y sencillas herramientas para la creación de páginas. GoDaddy cuenta con una variedad de funciones y servicios que lo hacen muy atractivo para sus clientes. Además, si no sabes lo que necesitas en términos de alojamiento web para tu negocio, con GoDaddy no tendrás que preocuparte.

- Precio: Los planes van de 5 a 130 dólares al mes.
- Ancho de banda: Ilimitado.
- Almacenamiento: 25 GB - ilimitado.

3. Hostinger es la mejor opción. Aunque sus tarifas suelen ser estándar, también ofrecen algunos planes básicos de hosting compartido con descuentos imperdibles. Al igual que muchos otros proveedores de alojamiento web, Hostinger también ofrece alojamiento de correo electrónico independiente, lo que te permitirá conectar las diferentes áreas de tu negocio. Debes estar atento a las rebajas, pero incluso sin ellas, sigue siendo un buen alojamiento web de gama media.

- Precio: Los planes oscilan de 3 a 250 dólares al mes.
- Ancho de banda: 100 GB - Ilimitado.
- Almacenamiento: 10GB - 400GB.

Registro de dominio

El registro de dominio es un proceso esencial en la configuración de una presencia en línea. Consiste en adquirir el derecho exclusivo de utilizar un nombre de dominio en internet durante un período de tiempo determinado. Este nombre de dominio es la dirección única que identifica un sitio web en la red. Por ejemplo, "miportafolio.com" sería un nombre de dominio. Es como la dirección de tu casa en el mundo digital, y el sufijo del dominio, como ".com" o ".net", es

como el código postal. El registro de dominio te brinda la propiedad total del nombre de dominio deseado y es un paso importante para establecer tu identidad en línea.

Al elegir un nombre de dominio, es crucial seleccionar uno relevante y fácil de recordar para tu portafolio web. Debería reflejar tu identidad profesional y ser fácil de pronunciar y escribir. Además, es importante considerar la disponibilidad del nombre de dominio, ya que algunas opciones pueden estar ocupadas. El nombre de dominio es fundamental para que las personas encuentren fácilmente tu sitio web y también ayuda con la optimización de motores de búsqueda, lo que significa que será más visible en Google y otros motores de búsqueda.

Existen diferentes tipos de dominios, como los dominios de nivel superior genérico (gTLD), los dominios de nivel superior de código de país (ccTLD), los subdominios y los dominios de nivel superior patrocinados (sTLD). Cada uno tiene su propio propósito y aplicación, como .com para empresas comerciales, .edu para instituciones educativas y .gov para organismos gubernamentales. La elección del tipo de dominio dependerá del propósito y la audiencia de tu sitio web.

Para elegir un buen dominio, es importante investigar cuidadosamente y considerar algunos consejos prácticos. Se recomienda optar por una palabra o frase corta y fácil de recordar, evitar el uso de guiones y evitar incluir el año de registro en el nombre de dominio. También es útil probar diferentes extensiones de dominio para encontrar la más adecuada para tu marca.

Una vez seleccionado el nombre de dominio, el proceso de registro implica completar un formulario de solicitud en el sitio web de un registrador de

dominios autorizado y proporcionar información de contacto. El dominio debe renovarse periódicamente para mantener su propiedad y evitar perderlo.

Tipos de dominios

Dominios de nivel superior genérico (gTLD): Estos son los dominios de primer nivel más populares y reconocidos, como .com, .net y .org. Son ampliamente utilizados y pueden ser registrados por empresas, organizaciones o individuos para diversos propósitos.

Dominios de nivel superior de código de país (ccTLD): Los ccTLD son códigos de país de dos letras que se corresponden con países de todo el mundo, como .us para Estados Unidos, .uk para el Reino Unido y .ca para Canadá. Estos dominios se utilizan para identificar sitios web asociados con un país específico.

Subdominios: Los subdominios son dominios que forman parte de un dominio mayor. Se utilizan para organizar sitios web en categorías o para crear versiones específicas de un sitio para diferentes países o propósitos. Por ejemplo, un subdominio de blog podría ser blog.ejemplo.com.

Dominios de nivel superior patrocinados (sTLD): Los sTLD son extensiones de dominio que se han creado para un propósito o industria específicos. Por ejemplo, .edu está reservado para instituciones educativas, .gov para organismos gubernamentales y .aero para la industria de la aviación. Estas extensiones de dominio están destinadas a proporcionar una identificación clara del tipo de organización o industria a la que pertenece el sitio web.

Protocolo de Transferencia de Hipertexto Seguro (HTTPS)

Un certificado SSL utiliza un sistema de cifrado de clave pública y clave privada para asegurar la comunicación entre un servidor y un cliente, como un navegador web. La clave pública, conocida por el servidor y de dominio público, se utiliza para cifrar los datos antes de enviarlos. Solo la clave privada correspondiente, que está en posesión exclusiva del servidor, puede descifrar esos datos. Esto garantiza que incluso si los datos son interceptados en el camino, permanecen encriptados y solo el servidor autorizado puede leerlos, proporcionando así seguridad en la transferencia de datos, ya sea entre dispositivos o en una conexión web.

Tipos de Certificados

De dominio: Ofrecen una capa básica de seguridad para cifrar la información entre dos puntos, ideal para sitios web que requieren una seguridad básica.

De organización: Proporcionan mayor seguridad y verificación de la identidad del sitio, además de cifrado de información. Su tarea principal es verificar el sitio al que se accede, lo que resulta extremadamente útil.

Certificados EV (Extended Validation): Similar a los de organización pero con una verificación adicional y exhaustiva de la identidad. Son reconocibles por una barra verde en las direcciones del navegador, indicando seguridad adicional.

Wildcard: Permiten proteger subdominios de un sitio con un solo certificado, lo cual es útil cuando un sitio enlaza con varios subdominios.

Multi-dominio: Permiten proteger múltiples dominios con un solo certificado, ideal para sitios con varios dominios (.com, .es, .net, etc.).

De extensión de validación: Proporcionan una seguridad mayor y una verificación de identidad más rigurosa que los certificados SSL estándar. Son ampliamente utilizados en entornos comerciales y financieros.

Instalar un certificado SSL en un servidor es esencial para garantizar la seguridad y la confianza de los visitantes en un sitio web. El proceso puede variar dependiendo del proveedor de hosting, pero sigue pasos similares.

Obtención del certificado SSL: Puede adquirirse a través del proveedor de hosting, otro proveedor externo o incluso obtenerse de forma gratuita. Es crucial elegir una opción confiable y adecuada para las necesidades del sitio.

Acceder al panel de control del hosting: Utilizando herramientas como cPanel, se accede a la sección de seguridad y luego a SSL/TLS.

Instalación del certificado SSL: Se selecciona el dominio al que se desea aplicar el certificado y se completan los campos con la clave privada (KEY) y el certificado (CRT) proporcionados. Al hacer clic en "Instalar certificado", el proceso se completa.

Vigilancia y renovación: Los certificados SSL tienen una fecha de caducidad, por lo que es importante estar al tanto de su vencimiento y renovarlos a tiempo para evitar problemas de seguridad y mantener la confianza de los visitantes.

Beneficios y importancia: La instalación del certificado SSL asegura la protección de la información transferida entre el servidor y el navegador, mejora la imagen del sitio web y su posicionamiento en los buscadores, y aumenta la confianza de los visitantes al garantizar una navegación segura.

Política de privacidad y cookies

Cookies

La información proporcionada por Google sobre el uso de cookies es fundamental para comprender cómo se recopila y utiliza la información personal en un sitio web, así como para garantizar la transparencia y el cumplimiento de las regulaciones de privacidad en línea.

En primer lugar, destaca la importancia de las cookies y tecnologías similares para mejorar la experiencia del usuario al recordar preferencias, configuraciones de idioma y sesiones de navegación. Estas cookies son esenciales para funciones básicas del servicio, como el almacenamiento de contenido del carrito de compras o las preferencias de reproducción en plataformas como YouTube.

Además, Google subraya el papel de las cookies en la seguridad de los usuarios, como la autenticación de cuentas y la prevención de fraudes. Las cookies ayudan a proteger las cuentas al verificar la identidad del usuario y al detectar actividades sospechosas, como intentos de robo de información.

En el ámbito de la analítica, las cookies son cruciales para recopilar datos sobre la interacción de los usuarios con los servicios, lo que permite mejorar el contenido y las funciones del sitio web. Google Analytics utiliza cookies para recoger información sobre el comportamiento de navegación de los usuarios, sin identificar personalmente a cada visitante, lo que contribuye a optimizar la experiencia del usuario.

En cuanto a la publicidad, Google destaca el uso de cookies para personalizar y mostrar anuncios relevantes para los usuarios, así como para medir la eficacia de las campañas publicitarias. Esto incluye la personalización de anuncios

basada en preferencias y la medición del rendimiento de los anuncios en términos de interacciones y conversiones.

Por último, Google proporciona información sobre cómo gestionar cookies en los navegadores y dispositivos, destacando la importancia de la transparencia y el control por parte del usuario sobre su privacidad en línea. Esto incluye opciones para eliminar cookies, bloquear su uso y gestionar las preferencias de cookies en los ajustes del navegador o dispositivo.

Puntos importantes

La política de privacidad y cookies es un componente esencial de cualquier sitio web, incluido un portafolio en línea, ya que informa a los visitantes sobre cómo se recopila, utiliza y protege su información personal y cómo se utilizan las cookies en el sitio. Aquí hay algunos aspectos importantes a considerar al redactar una política de privacidad y cookies para un portafolio web:

Información recopilada: Debes especificar qué tipo de información personal se recopila de los usuarios cuando visitan tu sitio web. Esto puede incluir datos como nombres, direcciones de correo electrónico, información de contacto y cualquier otra información que los visitantes proporcionen voluntariamente a través de formularios de contacto u otros medios.

Uso de la información: Debes explicar cómo se utiliza la información personal recopilada. Esto puede incluir el propósito de la recopilación de datos, cómo se almacenan y protegen los datos, y si se comparten o divulgan los datos con terceros.

Consentimiento del usuario: Es importante indicar cómo los usuarios pueden dar su consentimiento para la recopilación y el uso de su información personal. Esto puede incluir el uso de casillas de verificación para aceptar los términos de la política de privacidad o mensajes emergentes que informen a los usuarios sobre el uso de cookies y soliciten su consentimiento para continuar navegando por el sitio.

Cookies: Debes informar a los usuarios sobre el uso de cookies en tu sitio web. Esto incluye explicar qué son las cookies, qué tipos de cookies se utilizan (por ejemplo, cookies de sesión, cookies persistentes, cookies de terceros) y cómo se utilizan las cookies para mejorar la experiencia del usuario y recopilar información sobre el comportamiento de navegación.

Control de cookies: Es importante proporcionar a los usuarios opciones para controlar el uso de cookies en tu sitio web. Esto puede incluir la capacidad de aceptar o rechazar cookies a través de la configuración del navegador, así como la opción de optar por no participar en el seguimiento de cookies de terceros.

Actualizaciones de la política de privacidad: Debes indicar que la política de privacidad y cookies puede actualizarse periódicamente para reflejar cambios en las prácticas de privacidad del sitio web. Se recomienda informar a los usuarios sobre cualquier cambio significativo en la política y proporcionar la fecha de la última actualización.

Gestión de permisos

La gestión de permisos en un portafolio web es crucial para garantizar la seguridad y la privacidad de la información que se comparte en el sitio. Implica establecer y controlar quién tiene acceso a qué recursos y funciones dentro del sitio web. Aquí hay algunas consideraciones importantes sobre la gestión de permisos en un portafolio web:

Acceso de usuarios: Es importante definir quiénes serán los usuarios que tendrán acceso al portafolio web. Esto puede incluir al propietario del sitio, administradores, colaboradores y visitantes. Cada tipo de usuario puede tener diferentes niveles de acceso y permisos dentro del sitio.

Control de roles: Es útil asignar roles específicos a los usuarios según sus responsabilidades y funciones dentro del portafolio web. Por ejemplo, un administrador puede tener acceso completo para realizar cambios en el diseño y

el contenido del sitio, mientras que un colaborador puede tener acceso limitado para agregar o editar proyectos específicos.

Permisos de edición: Deberías definir quiénes tienen permiso para editar o modificar el contenido del portafolio. Esto puede incluir la capacidad de agregar, eliminar o actualizar proyectos, publicaciones o información personal.

Permisos de visualización: Es importante controlar quién puede ver qué contenido dentro del portafolio web. Por ejemplo, es posible que desees restringir el acceso a ciertos proyectos o secciones del sitio solo a usuarios autorizados, mientras que otros contenidos pueden ser públicos y accesibles para todos los visitantes.

Autenticación y autorización: Implementar un sistema de autenticación sólido para verificar la identidad de los usuarios y un sistema de autorización para controlar qué acciones pueden realizar estos usuarios una vez autenticados. Esto puede incluir el uso de contraseñas seguras, autenticación de dos factores y controles de acceso basados en roles.

Auditoría y seguimiento: Es recomendable llevar un registro de las actividades de los usuarios dentro del sitio, como quién accede, qué cambios se realizan y cuándo se realizan. Esto puede ayudar a identificar y resolver posibles problemas de seguridad, así como a rastrear el historial de cambios en el contenido del portafolio.

Optimización de Imágenes y Recursos

1. Habilitar la compresión Gzip: Gzip es un formato de compresión de archivos para el sitio web. Es decir, reduce el tamaño de los archivos enviados por el servidor y el tiempo de transferencia, con tasas de compresión de hasta 90% en archivos más grandes.

2. Reduce el tamaño de las imágenes: Las imágenes tienen un gran impacto en el peso y la carga de un sitio web. Según HTTP Archive, en mayo de 2019, representaban más de la mitad de los bytes de un sitio web. Optimizarlos, entonces, puede ser uno de los primeros pasos para mejorar la velocidad del sitio web.

3. Utiliza formatos de última generación para las imágenes: Otra acción importante para optimizar las imágenes es utilizar los formatos de archivo más actualizados, como JPEG 2000, JPEG XR y WebP. Tienden a tener una mejor compresión mientras mantienen la calidad en comparación con JPEG y PNG. Esto reduce el consumo de datos móviles y acelera la carga.

4. Reduce HTML, CSS y Javascript: Cuando un desarrollador crea los códigos para un sitio web, es común incluir saltos de línea, espacios en blanco y comentarios.Esa información no influye en el contenido que ve el usuario, pero está ocupando espacio y puede aumentar el tiempo de carga.Por lo tanto, las herramientas generalmente recomiendan la eliminación de estos caracteres superfluos. Esto es lo que se hace al "minificar" los códigos HTML, CSS y Javascript, para que sean más ligeros.

5. Pospón la carga de imágenes fuera de pantalla: Incluso las imágenes que no aparecen en la pantalla afectan el tiempo de carga de las páginas, lo interesante es que es posible posponer la carga a medida que el navegante se desplaza por la página. Esto significa que el desarrollador utiliza la función de carga diferida para imágenes ocultas en la pantalla. Por lo tanto, estas solo se cargan en el caso de que el usuario las alcance con el desplazamiento.

Seguridad y mejores prácticas

La seguridad de un sitio web es un aspecto crucial en el panorama digital actual. Una práctica fundamental para garantizar esta seguridad es mantener actualizadas las bibliotecas, frameworks y parches de seguridad.

En esta sección, se explicará la importancia de estas actualizaciones en la protección contra vulnerabilidades y el mantenimiento del rendimiento óptimo del sitio web.

Actualizaciones de Bibliotecas y Frameworks:

Importancia de las Actualizaciones:

Las bibliotecas y frameworks son componentes fundamentales en el desarrollo de software web, proporcionando funcionalidades preconstruidas y soluciones a problemas comunes.

Las actualizaciones periódicas de estas bibliotecas y frameworks son cruciales para:

Parchear vulnerabilidades de seguridad conocidas.

Corregir errores y mejorar el rendimiento.

Añadir nuevas funcionalidades y mantener la compatibilidad con estándares actuales.

Fuentes de Actualizaciones:

Las actualizaciones suelen ser proporcionadas por los desarrolladores de las bibliotecas o frameworks a través de canales oficiales, como repositorios de código, sitios web o gestores de paquetes.

Es importante seguir los canales oficiales y mantenerse informado sobre nuevas versiones y cambios importantes.

Gestión de Dependencias:

Las bibliotecas y frameworks suelen tener dependencias de otras bibliotecas o paquetes. Es importante gestionar estas dependencias y asegurarse de que todas estén actualizadas y sean compatibles entre sí.

La utilización de herramientas de gestión de dependencias, como npm para proyectos de JavaScript, Composer para proyectos de PHP, o pip para proyectos de Python, para gestionar y actualizar las dependencias de manera eficiente.

Integración Continua/Despliegue Continuo (CI/CD):

Implementar un proceso de CI/CD puede mejorar la seguridad al permitir la automatización de pruebas de seguridad, análisis estático de código y escaneo de vulnerabilidades durante el ciclo de desarrollo.

Utilizar herramientas como Jenkins, GitLab CI/CD, Travis CI o GitHub Actions para integrar estas pruebas de seguridad en tu pipeline de despliegue.

Autenticación de Múltiples Factores (MFA) en el Código Fuente:

1. Protección Adicional:

La implementación de la autenticación de múltiples factores (MFA) para proteger el acceso al código fuente alojado en sistemas de control de versiones como GitHub, GitLab o Bitbucket.

El MFA requiere que los usuarios proporcionen múltiples formas de autenticación, como una contraseña y un código generado dinámicamente a través de una aplicación de autenticación móvil.

2. Prevención de Acceso No Autorizado:

El MFA añade una capa adicional de seguridad al requerir un segundo factor de autenticación, lo que dificulta el acceso no autorizado incluso si las credenciales de usuario están comprometidas.

Referencias

Mauricio. (2022, September 14). *Qué es un dominio en Internet y cómo funciona » Dongee*. Tutoriales Dongee. https://www.dongee.com/tutoriales/que-es-un-dominio/?utm_source=google&utm_medium=cpc&utm_campaign=tutoriales&utm_id=dominios&tm=tt&ap=gads&aaid=adaFnZvkSdpvp&gad_source=1&gclid=Cj0KCQjwiMmw

BhDmARIsABeQ7xRV8nCoiXJr4LixrJar_223lw1luM9GEzq8pfiE2OOOprEiNv-RQ5IaAkYhEALw_wcB

Cómo utiliza Google las cookies – Privacidad y Condiciones – Google. (n.d.). Privacy & Terms – Google. https://policies.google.com/technologies/cookies?hl=es

Islas, D. S. (2024, March 24). Las mejores plataformas que ofrecen servicios de hosting en 2024. *Blog de Wix | Diseño Web, Fotografía y Tips de Negocios*. https://es.wix.com/blog/2023/03/mejores-hostings

Jiménez, J. (2024, February 4). Qué tener en cuenta al instalar un certificado SSL TLS. *RedesZone*. https://www.redeszone.net/tutoriales/servidores/como-instalar-certificado-ssl/

De Souza, I. (2021, February 12). *Descubre cómo mejorar el tiempo de carga de tu web con estas 11 técnicas*. Rock Content - ES. https://rockcontent.com/es/blog/mejorar-el-tiempo-de-carga/