



INSTITUTO TECNOLÓGICO SUPERIOR DE POZA RICA

INGENIERÍA SISTEMAS COMPUTACIONALES

Materia

Desarrollo en Internet

Nombre

Javier Alexis Mendoza Gracia

Docente

Simón García Ortiz

Introducción

Como introducción acerca de este tema tenemos que, la tecnología es un conjunto de soluciones que nos permite observar crear Web está basada en el protocolo HTTP para la transmisión de hipertexto sobre protocolos de comunicaciones TCP/IP, sirve para poder proporcionar una nueva visión de internet.

Si antes, con servicios como FTP, la Red se concebía como un conjunto de nodos servidores cuya topología y estructura física había que conocer, ahora se logra un nivel de abstracción mayor: lo que importa es la información, los contenidos en términos del WWW, en lugar de su ubicación, de las características de los servidores en los que se encuentra ubicada o de los dispositivos empleados para acceder a la misma: computadora personal, PDA , WebTV, teléfono móvil, etc.

Desarrollo de aplicaciones web

2.4 Ambientes para el desarrollo de aplicaciones Web.

Un ambiente de desarrollo para aplicaciones web es una estructura definida, reusable en el que sus componentes facilitan la creación de aplicaciones web. En cierto sentido podemos afirmar que nos proveen una capa de abstracción sobre la arquitectura original ocultándola o adaptándola para no tener que utilizar el protocolo http de manera nativa y así acelerar los tiempos de desarrollo y mantenimiento.

Los ambientes de desarrollo más importantes son los siguientes:

- **FrontPage.-** Es un programa de Microsoft para crear y mantener sitios web. Permite diseñar y crear páginas directamente en el propio sitio de Internet, así como en una computadora personal y luego publicarlas por completo en un servidor. Con este software se pueden elaborar páginas sin saber absolutamente nada del lenguaje HTML, se escriben los textos, se les da formato, y se le insertan imágenes mientras el programa elabora el código HTML correspondiente que es el que entienden los navegadores de internet.
- **Dreamweaver.-** Es un editor visual profesional para la creación y administración de sitios y páginas Web. Con Dreamweaver resulta fácil crear y editar páginas compatibles con cualquier explorador y plataforma. Dreamweaver proporciona herramientas avanzadas de diseño y formateo, y facilita el uso de funciones de HTML dinámico, como capas y comportamientos animados, sin necesidad de escribir una sola línea de código. El establecimiento de destino de exploradores comprueba el trabajo para averiguar si hay problemas potenciales en las plataformas y los exploradores más habituales. La tecnología Roundtrip HTML de Macromedia importa documentos HTML sin necesidad de cambiar el formato del código y, además, es posible configurar Dreamweaver para limpiar y cambiar el formato HTML cuando lo desee. Dreamweaver se puede personalizar totalmente. Puede crear sus propios objetos y comandos, modificar menús y métodos abreviados de teclado, e incluso escribir código JavaScript para ampliar las posibilidades que ofrece Dreamweaver con nuevos comportamientos e inspectores de propiedades.
- **Eclipse** es un proyecto de desarrollo de software de código fuente abierto cuyo objetivo es la construcción de herramientas integradas para el desarrollo de aplicaciones, este a su vez se compone de diversos subproyectos entre los cuales está el Eclipse Web Tools Platform (WTP), el cual contiene herramientas para el desarrollo de aplicaciones web, que incluyen editores gráficos para simplificar el desarrollo.
- **ASP.NET:** es un conjunto de tecnologías definidas por Microsoft para la capa de presentación WEB que forma parte del .NET Framework. En pocas palabras, una página ASP.NET es un archivo de texto con extensión aspx que el servidor sabe que debe procesar de una manera especial. El texto de las páginas puede ser html junto con código scripting que se compila dinámicamente y se ejecuta en el servidor. La página aspx se compila (sólo la primera vez) a código ejecutable .net cuando algún cliente la solicita al servidor. Para incluir código embebido en la página se utilizan los separadores `<%` y `%>`. En este sentido es similar al funcionamiento de las páginas JSP de java. Las páginas ASP.NET pueden tener controles que se ejecutan del lado del servidor (server controls) que son objetos que representan elementos de la interfaz de usuario que se ejecutan en el servidor y generan código html como resultado de su ejecución. Los controles tienen propiedades, métodos y eventos a los que pueden responder y mediante los que se puede modificar su estado y comportamiento. Este comportamiento se puede declarar en

los atributos de su declaración html o de manera programática. Los controles permiten contener otros controles dentro de ellos y es posible, al igual que cualquier objeto, heredar y redefinir parte de su comportamiento. Un control de servidor se identifica en una página html por su atributo `runat="server"`. De esta manera un webform es una página html que contiene en algún lado una etiqueta del estilo.

2.5 Metodologías para el desarrollo de aplicaciones Web.

Las metodologías más usadas son:

1. RMM Relationship Management Methodology: se define como un proceso de análisis, diseño y desarrollo de aplicaciones hipermedia. Esta metodología es apropiada para dominios con estructuras regulares es decir, con clases de objetos bien definidas, y con claras relaciones entre esas clases. Por ejemplo, catálogos o bases de datos tradicionales. El modelo propone un lenguaje que permite describir los objetos del dominio, sus interrelaciones y los mecanismos de navegación hipermedia de la aplicación. Los objetos del dominio se definen con la ayuda de entidades, atributos y relaciones asociativas, sus principales características son:

- Aproximación para el diseño de sitios web, bajo una aproximación centrada en la información.
- Lenguaje de modelado de sitios web a nivel lógico (dominio de información + estructuras de navegación + elementos de presentación)
- Integrado en una metodología de desarrollo
- Facilitar la estructuración de páginas web complejas que contienen elementos de distintas entidades (vistas múltiples)
- Permitir la reutilización de elementos en el diseño (vistas jerárquicas)
- Diseño de enlaces más potentes y versátiles
- Mantener el contexto durante la navegación
-

2. OOHDM Object Oriented Hypermedia Design Method: OOHDM propone el desarrollo de aplicaciones hipermedia a través de un proceso compuesto por cuatro etapas: diseño conceptual, diseño navegacional, diseño de interfaces abstractas e implementación.

• **Diseño Conceptual.** En OOHDM, el desarrollo se inicia diseñando la capa conceptual, siendo el principal objetivo de esta etapa capturar los conceptos involucrados en el dominio de la aplicación y describirlos en detalle, haciendo uso de diagramas que permitan expresar con claridad el comportamiento, la estructura y las relaciones entre dichos conceptos. La Programación Orientada a Objetos facilita el traslado del diseño conceptual a la implementación, proveyendo al programador con herramientas que permiten reducir la distancia entre el problema del mundo real y la programación de la solución en la computadora.

• **Diseño Navegacional.** La capa navegacional se compone de objetos contruidos a partir de objetos conceptuales, y constituyen en general los elementos canónicos de las aplicaciones hipermedia tradicionales: nodos, enlaces, anclas y estructuras de acceso. Sin embargo, estas clases pueden extender el comportamiento característico para funcionar como adaptadores de los objetos conceptuales y delegar así operaciones específicas del dominio. Entonces, los objetos navegacionales pueden actuar como observadores, para construir vistas de objetos conceptuales, y como adaptadores, para extender la actividad navegacional de un nodo y poder aprovechar el comportamiento conceptual del objeto adaptado.

- **Diseño de Interfaz Abstracta.** Una vez que las estructuras navegacionales son definidas, se deben especificar los aspectos de interfaz. Esto significa definir la forma en la cual los objetos navegacionales pueden aparecer, cómo los objetos de interfaz activarán la navegación y el resto de la funcionalidad de la aplicación, qué transformaciones de la interfaz son pertinentes y cuándo es necesario realizarlas. Una clara separación entre diseño navegacional y diseño de interfaz abstracta permite construir diferentes interfaces para el mismo modelo navegacional, dejando un alto grado de independencia de la tecnología de interfaz de usuario. El aspecto de la interfaz de usuario de aplicaciones interactivas (en particular las aplicaciones web) es un punto crítico en el desarrollo que las modernas metodologías tienden a descuidar. En OOHDM se utiliza el diseño de interfaz abstracta para describir la interfaz del usuario de la aplicación de hipermedia. El modelo de interfaz ADVs (Vista de Datos Abstracta) especifica la organización y comportamiento de la interfaz, pero la apariencia física real o de los atributos, y la disposición de las propiedades de las ADVs en la pantalla real son hechas en la fase de implementación.

- **Implementación.** En esta fase, el diseñador debe implementar el diseño. Hasta ahora, todos los modelos fueron construidos en forma independiente de la plataforma de implementación; en esta fase es tenido en cuenta el entorno particular en el cual se va a correr la aplicación. Al llegar a esta fase, el primer paso que debe realizar el diseñador es definir los ítems de información que son parte del dominio del problema. Debe identificar también, cómo son organizados los ítems de acuerdo con el perfil del usuario y su tarea; decidir qué interfaz debería ver y cómo debería comportarse. A fin de implementar todo en un entorno web, el diseñador debe decidir además qué información debe ser almacenada.

3. UML-Based Web: Se trata de un método que hace uso de técnicas procedentes de la orientación a objetos para especificar aplicaciones hipermedia. UWE plantea un enfoque iterativo y progresivo cuyas actividades fundamentales son el análisis de requisitos y el diseño conceptual, de la navegación y de la presentación. Los elementos hipermedia se representan por medio de elementos propios de los diagramas de clases UML. Así por ejemplo, los nodos son clases, los enlaces son asociaciones estereotipadas y las ayudas a la navegación (como índices o mapas) son clases estereotipadas. Para modelar aspectos dinámicos se hace uso de modelos de tarea y diagramas de estado, mientras la navegación y la presentación se representan por medio de UML y de estereotipos creados al efecto. Los principales aspectos en los que se fundamenta UWE son los siguientes: Uso de una notación estándar, para todos los modelos (UML: Lenguaje de modelado unificado). Definición de métodos: Definición de los pasos para la construcción de los diferentes modelos. Especificación de Restricciones: Se recomienda el uso de restricciones escritas (OCL: Lenguaje de restricciones de objetos) para aumentar la exactitud de los modelos. Este proceso de autoría está dividido en cuatro pasos o actividades:

- **Análisis de Requisitos:** Fija los requisitos funcionales de la aplicación Web para reflejarlos en un modelo de casos de uso. Esto da lugar a los diagramas de casos de uso.
- **Diseño Conceptual:** Se construye el modelo conceptual del dominio de la aplicación considerando los requisitos reflejados en los casos de uso. El resultado es el diagrama de clases de dominio.
- **Diseño Navegacional:** Se obtienen el modelo de espacio de navegación y el de estructura de navegación, que muestra como navegar a través del espacio de navegación. El resultado son diagramas de clases que representan estos modelos.
- **Diseño de Presentación:** Representa las vistas del interfaz del usuario mediante modelos estándares de interacción UML.

2.6 Aspectos de seguridad.

Debido a los pocos mecanismos de seguridad informática en Internet, el hecho de colocar una página Web en ella trae determinados riesgos que pueden ser controlados con alguna estrategia adecuada.

La seguridad en una página debe cumplir con tres aspectos: operatividad, integridad y privacidad, al igual que cualquier otro dispositivo de cómputo.

1. Operatividad: La información que contenga la página debe estar siempre en condiciones operativas para quienes acceden a la misma puedan recorrerla sin problemas, sin encontrar fallas, faltas, o cualquier tipo de anomalía. Hay que considerar también que el ingreso de un intruso al sistema puede provocar daños que afecten a la operatividad.

2. Integridad: De nada sirve que una información esté en condiciones operativas si es incompleta o está alterada. Para que una información resulte inútil no es necesario que sea destruida, puede ser suficiente una acción tan sutil como cambiar los unos por ceros. Por lo tanto la integridad de la información que se muestra en una página Web es uno de los factores más importantes de la seguridad, pues de él dependen el interés y la credibilidad de la página. La integridad de la página puede ser dañada por fallas de hardware o software, o atacada por intrusos en el sistema que toman el control sobre algún sector y modifican el contenido de las páginas

3. Privacidad: Es lógico pensar que quien quiere que una información sea privada no debe colocarla en una página Web. Pero puede ocurrir que parte de la información esté reservada a usuarios registrados o que exista algún tipo de restricción.

Cada una de las condiciones de seguridad de una página Web: operatividad, integridad y privacidad, tienen sus propios riesgos que actúan dentro o fuera del sistema.

Para establecer una estrategia de seguridad se debe evaluar el grado de importancia de cada uno de ellos y basándose en ello, establecer normas y procedimientos necesarios para contenerlos:

Para muchas aplicaciones de negocios, como la publicidad y promociones simples, es probable que no se necesite tratar con precauciones de seguridad. Pero si se permite que los usuarios tengan acceso a datos delicados, se deberán tomar medidas para proteger a los datos. Debido a que cada vez son más las personas que desean transferir documentos e información de tarjetas de crédito o cualquier tipo de transmisión de datos en forma segura y sin el temor a los crackers y piratas.

Las medidas de seguridad básicas a tener en cuenta son:

1. La encriptación de Datos: Es una técnica para ocultar datos de manera que sólo puedan ser vistos por aquellos que deben verlos. Consiste en reemplazar un mensaje enviado con un algoritmo difícil de adivinar. Los servidores seguros tratan de encriptar los datos entre el navegador y el servidor. En algún momento durante el ciclo de compras, después que los datos llegan al servidor seguro, el sistema debe desencriptar los datos. Aun si los datos son desencriptados sólo por un instante, la información podría ser interceptada por algún pirata. Crear un sistema en el que la información permanezca encriptada a lo largo del ciclo es prácticamente imposible. La configuración más segura es una que transmita la información al propietario de la empresa en formato encriptado, pase la información a una computadora que no esté en Internet y luego desencripte la información. Además si en una empresa se utiliza un mismo algoritmo para encriptar y desencriptar datos, se necesitará que alguna tercera pieza de datos desencripte el código, que sería una clave. Esto sólo funcionará si tanto la persona transmisora como la parte receptora conocen la clave. Si la persona receptora no conoce la clave, tiene que enviar la clave a esa parte, y ésta puede ser interceptada.

2. Firma Digital: Ofrece un método de encriptación de datos que evita tener que compartir claves para leer mensajes. Es la técnica llamada encriptación de clave pública, donde cada usuario tiene dos claves: una clave pública y una clave privada. Los algoritmos de encriptación y desencriptación son adaptados de manera que sólo la clave pública puede desencriptar los datos

encriptados por la clave privada. Por consiguiente, puede transmitir con libertad la clave pública al mundo.

3. Creación de un Sitio Seguro: Las ventajas de crear un sistema seguro antes de ser pirateado deben ser obvias. La prevención es la mejor medicina y esto se aplica también a la seguridad de las computadoras. Se debe mantener la seguridad de los archivos de datos de tal forma que solo las personas correctas puedan verlos. Esto es crucial para los siguientes tipos de datos y archivos: contraseñas de usuarios, archivos de facturación, registros de sistema y de usuarios, información de tarjetas de créditos, información confinada de sistemas remotos, compiladores, herramientas de administración.

4. Firewalls, Wrappers y Proxies: Los firewalls, wrappers y proxies ofrecen una buena línea de defensa para los propietarios de servidores Web y administradores de sistemas. Los firewalls pueden ser software o hardware que protege los puertos y evita que los piratas penetren al sistema. Los firewalls permiten que tengan acceso al sistema sólo ciertos nombres de dominio confiables. Los wrappers se encuentran disponibles en CERT al igual que en otros archivos en Internet. Los wrappers se ejecutan como una capa de software alrededor de su otro software. Un usuario que se conecta a FTP primero entraría en contacto con el wrapper, el cual luego habilitaría al FTP. El usuario no sabe que existe el wrapper y no puede detectar ninguna diferencia en el sistema. Los wrappers son interesantes porque son flexibles. Pueden actuar como firewalls y en realidad pueden rechazar usuarios con base en sus nombres de usuarios al igual que en sus nombres de dominios. Además permite crear callejones sin salida que permiten atrapar piratas. El modo proxy es un método que permite ocultar datos por medio de reenrutamiento de las solicitudes. Es útil para usuarios que están detrás de una firewall. Los usuarios establecen una dirección proxy de su navegador para que apunte hacia su servidor Web. El servidor Web maneja entonces la dirección real de los datos hacia el mundo exterior. Esto reduce la dirección que el usuario está tomando cuando deja su sistema, permitiéndole al usuario enrutar los datos a través de los agujeros en sus propias firewalls. La otra ventaja es que las solicitudes pueden ser filtradas por el software del servidor. Al filtrar la información, puede restringir el contenido y rastrear el uso al igual que modificar la información en ese instante. Los servidores proxy también pueden ser dirigidos a otros servidores proxy, lo cual les permite ocultar datos en forma efectiva. Otra ventaja de los servidores proxy es que los servicios como FTP, Telnet, Gopher, NetNews, etc., pueden ser enrutados a servidores diferentes. Esto le permite distribuir diversas cargas de servidor Web a diferentes servidores físicos. Además de beneficiarse con el ocultamiento de los datos, se reduce la carga del servidor.

Algunas de las definiciones más importantes en el manejo de la seguridad son las siguientes:

- **Clave pública:** Es una clave alfanumérica creada por medio de algoritmos matemáticos que sirve para encriptar una serie de datos. Suele ser creada junto con una clave privada, la clave pública se suele llamar también llave pública.
- **Clave privada:** Es una clave alfanumérica creada por medio de algoritmos matemáticos que sirve para desencriptar una serie de datos que han sido creados por la clave pública que forma la pareja.
- **Certificado:** Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.
- **Autoridad certificadora:** Es la autoridad que garantiza que una firma es de quien dice ser, esta garantía se da por medio de certificados digitales.
- **Prestador de servicios de Certificación:** Es una empresa o entidad que expide certificados digitales, puede ser una autoridad de certificación o expedirlos en nombre de ésta.

Conclusión

En la actualidad nos damos cuenta de que hablar de tecnologías web engloba muchos campos y que sus áreas son diversas y complejas, desde solo consultar información con un navegador ya sea Firefox, safari, opera, chrome, buscar una imagen, consultar sitios de empresas, hacer compras electrónicas, jugar, conocer lugares en 3D, así como consultar datos estadísticos, bases de datos, sitios de gobierno, etc., etc... Las tecnologías juegan un papel muy importante en la web, debido a estas herramientas podemos acceder al internet, que no es solo sentarte frente a un ordenador y abrir el internet sino que hay un gran trabajo detrás para hacer posible este tipo de tecnología, donde miles de personas trabajan actualizando datos, creando los métodos para mantener todos los enlaces y las comunicaciones.

Referencias

- Manuel Montenegro.
- (2018).
- Introducción a las tecnologías Web.
- 26/06/2018,
- Instituto Tecnológico de Matehuala Sitio web: <https://programacionwebisc.wordpress.com/1-2-2-urls>