ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Implementación de Autenticación (PASSPORT) de Sistemas.

Utilizando Algoritmo de Encriptación"

TESIS DE GRADO

Previa a la obtención del título de:

LICENCIADO EN SISTEMAS DE INFORMACION

Presentado por:

Mercedes E. Triviño Gilces

Shirley H. Villón Lindao

Jorge Daniel Lam Arias

GUAYAQUIL – ECUADOR

AÑO

2005

AGRADECIMIENTO

Agradezco a DIOS, a mi familia por su constante apoyo en todos los momentos de mi vida.

Agradezco la valiosa ayuda brindada a mi amigo José Francisco Rodríguez Rojas.

Un agradecimiento en especial a mis profesores Ing. Albert Espinal e Ing. Nestor Arreaga por toda su ayuda incondicional.

Mercedes Triviño Gilces

Shirley H. Villón Lindao

Jorge Daniel Lam Arias

DEDICATORIA

Dedico este trabajo a mis padres quienes a lo largo de mi vida me han dado una educación fundamentada en valores que han servido para guiar mis pasos en la correcta toma de decisiones y acciones.

Mercedes Triviño Gilces

DEDICATORIA

El proyecto va dedicado especialmente a mi Sra. Mamá, hermanos, a mi familia y amigos que me dieron apoyo en todo momento. A mis compañeros de trabajo y en especial a José que nos dió una luz para el desarrollo de este trabajo. A mi amigo Ángelito, por sus consejos y apoyo moral; y porque siempre me recuerda que debemos dar gracias ante todo a nuestro papá DIOS por todo lo que nos brinda cada día.

Shirley Villón Lindao.

DEDICATORIA

Este trabajo va dedicado a mis padres hermanos y familia en general y también a Dios.

Jorge Daniel Lam Arias

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

Anl. Mercedes E. Triviño Gilces

Anl. Shirley H. Villón Lindao

Sr. Jorge Daniel Lam Arias

TRIBUNAL DE GRADUACION

Ing. Mónica Villavicencio

Coordinadora

Ing. Albert Espinal

Director de Tesis

MIEMBROS PRINCIPALES

Ing. Cristina Abad

Ing. Marcelo Loor

RESUMEN

El proyecto a exponerse, diseña e implementa el manejo de Cuentas Passport para brindar una autenticación segura al momento en que un cliente intente ingresar a los sitios asociados. La aplicación esta desarrollado en entorno Web e incluye opciones de Creación de Cuentas (opción Regístrese), Recuperación de una cuenta (en caso de olvido de contraseñas), la opción para Inicio de Sesión con el previo ingreso del nombre e ingreso de contraseñas. Además presenta opciones de información acerca de cuales son los beneficios al obtener una cuenta Passport , posibles causas al presentarse problemas en el momento de inicio de sesión y otras informaciones de interés a la comunidad de nuestro servicio.

En el primer capitulo realizamos una introducción dando a conocer conceptos, uso y beneficio al obtener el servicio de Cuentas Passport . Además le mostramos los beneficios en cuanto a seguridad y confiabilidad de autenticidad.

En el segundo capítulo hacemos una explicación breve acerca de la evolución, conceptos, y usos de la seguridad informática. Es

importante mencionar las herramientas de uso para mantener seguridad en la red.

En el capitulo tres exponemos el esquema de requisitos de seguridad que posee una aplicación Web. Se incluye un análisis para la selección de la plataforma así como de herramientas a usarse para el desarrollo e implementación del proyecto. En esta parte se ha tomado en cuenta su rendimiento, requisito de funcionamiento y costos de cada herramienta utilizada para la selección. Para el desarrollo de nuestro proyecto fue necesario tomar en cuenta tres herramientas necesarias: la Base de Datos, el entorno de desarrollo y el servidor. En esta parte también incluimos todas las herramientas utilizadas para el análisis y desarrollo de la aplicación Web, estos son: casos de uso, diagramas de interacción de objetos y el diseño del modelo Entidad-Relación.

En el capitulo cuatro hace un recuento de los puntos que se incluyen en la aplicación Web desarrollada. Tenemos incluidos el uso de emisión de cuentas de usuarios, como iniciar una sesión, recordatorios de contraseñas, renovación de cuentas Passport y

una explicación de configuración de clientes para la verificación de cuentas Passport .

En el capitulo cinco exponemos las políticas de seguridad que protegen la información personal. Se consideran como políticas de seguridad a: los procedimientos y tecnologías que protegen información personal; revelación, uso y accesos no autorizados. También se considera hacer recomendaciones de puntos a tomar en cuenta para la creación de una contraseña, el tomar en cuenta la importancia de realizar respaldos de información. Es importante tener presente la actualización de software por las constantes mejoras que sufren los mismos, para seguir manteniendo confiabilidad en cuanto a seguridad.

En el último capitulo se presentan las conclusiones que hemos obtenido en cuanto al desarrollo de nuestro trabajo y las recomendaciones apropiadas para el uso del mismo.

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

CAPITULO 1

1 Introducción

1.1 Antecedentes

Las cuentas Passport son un servicio basado en Web, que nos permite autenticar la identidad de un usuario al momento de ingresar a los diferentes sitios asociados, además de permitir el acceso en una forma rápida y sencilla.

Este servicio elimina la necesidad de recordar numerosas contraseñas para cada sitio a donde se intente ingresar. Basta con una cuenta Passport para permitir el acceso a diferentes sitios.

El servicio permite el acceso mediante la creación de una cuenta y contraseña para el inicio de sesión, que será utilizado para acceder a los diferentes sitios y servicios colaboradores.

1.2 Creación y Autenticación De Cuentas

Una cuenta Passport recopila la información necesaria para llevar a cabo la operación de un servicio de autenticación, para facilitar el registro de sitios colaboradores que soliciten información personal respetando la privacidad del mismo, mejorar la seguridad y proporcionar soporte al cliente de su cuenta.

Cuando se utiliza la cuenta Passport para iniciar sesión en un sitio colaborador, este servicio registra temporalmente el lugar en que ha iniciado sesión como parte de su actividad de inicio de sesión. Sin embargo, no se recopila ningún otro tipo de información acerca de la actividad que realiza mientras está conectado en el sitio colaborador.

Cuando se registra para obtener una cuenta de Passport , se le pedirá que proporcione determinada información personal que se almacenará en el "perfil" de la cuenta. Como se describe a continuación, la cantidad de información solicitada variará en función del sitio de registro.

Al registrarse para obtener una cuenta Passport , se pedirá que cree una contraseña para su cuenta. Además se le solicita que proporcione preguntas y respuestas secretas. Estas preguntas y respuestas secretas

contribuyen a comprobar su identidad en relación con su cuenta en determinados casos, como por ejemplo, cuando necesite restablecer su contraseña.

La autenticación es el proceso por el que se comprueba la identidad de alguien o algo, para ver si es lo que dice ser. Ese "alguien" o "algo" se denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Por ejemplo, una aplicación cliente puede presentar una contraseña como sus credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

1.3 Objetivos

- Incorporar el servicio de autenticación único a su sitio Web o servicio.
- Proporcionar servicio de autenticación personal que le faciliten el desplazamiento entre sitios Web.

- Brindar la posibilidad de usar un nombre de inicio de sesión y una contraseña en todos los sitios colaboradores.
- Lograr que el registro a los sitios Web sea rápido y sencillo.
- Proporcionar la privacidad y la protección de su información personal ya que todo esto es muy importante para todos nosotros.
- Nuestro servicio de autenticación no permitirá su información a terceros.
- Nuestro servicio de Pasaporte usará la información personal de cada usuario para la operación y mantenimiento de su cuenta y servicio.
- Autentificación segura mediante la aplicación de Algoritmos de Seguridad.

1.4 Metodología

Al registrarse se asocia un identificador único a cada una de las cuentas. El identificador es un número único de 64 bits que la cuenta Passport envía **(cifrado)** a cada sitio colaborador en el que inicia sesión. El identificador consta de una clave de 56 bits más 8 de paridad. Este identificador único permite que el sitio determine si se trata de la misma persona entre un inicio de sesión y el siguiente.

El sitio Web, también registra temporalmente inicios de sesión individuales con el propósito de asegurar la eficacia y la seguridad de nuestro servicio. La información de estos registros sólo se puede identificar con el número de Id. único de la cuenta y nunca está vinculado a información personal, a no ser que el usuario llame al servicio para solicitar asistencia.

Puede registrarse para obtener una cuenta @mipasaporte.com en un servicio o sitio colaborador del sitio Web. La cantidad de información recopilada durante el registro es determinada por el sitio de registro.

1.5 Contribución

El servicio de autenticación única de la cuenta Passport permite a los usuarios generar un solo conjunto de credenciales que pueden ser utilizadas para acceder a cualquier sitio asociado que soporte el servicio. El objetivo del servicio de autenticación única de la cuenta es aumentar la satisfacción del cliente permitiendo a los visitantes de sitios Web acceder fácilmente sin la molestia de registros repetitivos y el olvido de contraseñas.

1.6 Soluciones que Implementan Seguridad Mediante Cuentas Passport .

A continuación se mencionan los beneficios a brindar el servicio de manejo de cuentas Passport para mantener un acceso seguro en aplicaciones Web.

- **Ahorrar Tiempo para Construir Sistemas de autenticación**

  La cuenta Passport atenúa la necesidad de construir, hospedar y mantener sistemas de autenticación, permitiendo a una empresa centrar los recursos de desarrollo. Adicionalmente, la disminución de contraseñas olvidadas puede reducir gastos de soporte al cliente.

- **Brindar a Usuarios de cuentas Passport un Acceso Sencillo a un Sitio**

  La cuenta simplifica la autenticación y la inscripción eliminando barreras para los titulares de cuentas para acceder a su sitio Web,

proporcionar a los usuarios un acceso sencillo, sin la molestia de registrarse en forma repetida u olvidar contraseñas puede ayudar a aumentar el alcance y la satisfacción del cliente.

Incrementa la lealtad del cliente mediante personalización sencilla y confiable, la cuenta le permite personalizar la experiencia Web de clientes habituales basándose en un perfil único. Al ofrecer personalización al gusto del consumidor usted puede establecer una relación más estrecha y significativa con sus clientes e incrementar así su lealtad.

- **Asegura la Propiedad y el Control de los Datos de sus clientes.**

  La cuenta Passport no posee acceso a ninguno de sus datos. Esta es sencillamente una tecnología que le permite brindar servicios autenticados, centrados en el usuario para sus clientes. La relación entre su compañía y sus clientes le pertenece únicamente a usted.

CAPITULO 2

2 Definiciones relacionadas a la seguridad de la información y las cuentas Passport

2.1 Evolución del Término Seguridad

En la actualidad, las organizaciones son cada vez mas dependientes de sus redes informáticas y un problema que les afecte, por lo mínimo que sea, puede llegar a comprometer una continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección de corrección de los múltiples y variados problemas de seguridad que va apareciendo. En medio de esta variedad, ha ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de redes.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

A la hora de plantearse en que elementos del sistema se deben ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

Protección de los sistemas de trasferencias o transportes: En este caso el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma transparente posible. Ejemplos de este tipo de planteamiento serian el establecimiento de un nivel de transporte seguro, de un servicio de un firewall, que defiende el acceso a una parte protegida de una red.

Aplicaciones seguras extremo a extremo. Si pensamos, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procesamiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de asegurar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por responsables de seguridad de su organización. Esta misma operatoria, puede usarse para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso de bases de datos, etc.

En ambos casos, un problema de capital importancia es la gestión de passwords. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario este en condiciones de enviar un solo bit.

Mediante el uso de cuenta Passport nos proponemos facilitar las tareas de todos aquellos que se encuentran actualmente involucrados en las decisiones respecto de las redes de información y de sus modos de administración, al tiempo de alertar sobre la importancia crítica de la seguridad. Creemos que un adecuado tratamiento de la problemática resulta absolutamente vital.

2.2 Definición de Seguridad

Dado que se esta tratando conceptos que pueden tener múltiples interpretaciones, parece prudente acortar ciertos significados específicos. Por tanto, hemos recurrido a algunas definiciones, todos ellas extraídas del diccionario ESPARSA CALPE.

Seguridad: es “calidad de seguro”, y seguro esta definido como “libre de riesgo”

Información: es “acción y efecto de informar”

Informar: es “dar noticia de una cosa”

Redes: es “el conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinación fin”.

Uniendo todas estas definiciones, podemos establecer que se entiende por seguridad en redes.

Seguridad en redes

Es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.

Si trabajamos en definir seguridad en redes con los elementos que conocemos, podemos llegar a una definición mas acertada.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Seguridad Global.

El concepto de red global incluye todos los recursos informáticos de una organización, aun cuando estos no estén interconectados:

- Redes de área Local.
- Redes de área metropolitana.
- Redes nacionales y mundiales.
- Computadoras personales, minis y grandes sistemas.

De manera que, seguridad global es mantener bajo protección todos los componentes de una red global.

Al fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuanta que la seguridad comienza y terminan con personas.

2.3 Usos de la Seguridad de la Información

Se la puede utilizar para evitar un sin número de ataques que aquí detallamos:

Negación de servicio (denial of service)

Es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinando o a sus propios recursos.

Algunos ejemplos de tipo de ataque:

- Tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos a la misma.
- Tentativas de interrumpir las conexiones entre dos máquinas evitando de esta manera el acceso al servicio.
- Tentativas de evitar que una determinada personas tenga acceso a un servicio.
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario.

Habría de tener en cuenta que el uso ilegítimo de recursos también da a lugar la negación de un servicio. Por ejemplo, un hacker puede utilizar un área del ftp anónimo.

Cracking Passwords

El objetivo inicial consiste en entrar al servidor; para ello, se procede como si se tratase de una máquina

remota telnet. Pero, debido a que se permite el acceso a múltiples usuarios, los sistemas nos solicitaran un usuario y contraseña. En los sistemas que usan Unix ésta información se guarda en un archivo siendo ese el punto más débil y fácil de atacar.

Email bombing y spamming

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del usuario.

El spamming, que es una variante del e-mail bombing, se refiere a enviar el e-mail a centenares o millares de usuarios e, inclusive, a listas de interés. El Spamming puede resultar aun más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban respuesta.

El e-mail bombing se puede combinar con el e-mail spoofing que altera la identidad de la cuenta que envía el mail, logrando que sea más difícil determinar quien está enviando realmente el mail.

2.4 Herramientas de Seguridad en la Red

En este apartado se encuentran aquellas herramientas que nos permitirán tener una información - mediante archivos de trazas o logísticos - de todos los intentos de conexión que se han producido sobre nuestro sistema o sobre otro que nosotros hayamos señalado, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP (herramientas de tipo SATAN).

Este tipo de herramientas nos permite tener un control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL, etc.). Estas herramientas pueden ser utilizadas junto con otras que nos permitan definir

desde qué máquinas permitimos ciertas conexiones y cuales se prohíben. Algunas de las herramientas descritas en este apartado no necesitan estar instaladas en la máquina que se quiere controlar, ya que se puede poner en una máquina cuya interfaz de red funcione en modo compartido, permitiendo seleccionar la dirección IP o máquina que queremos auditar.

Algunas de las herramientas descritas en este apartado pueden tener un doble uso. Es decir, nos permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas. Por eso es importante que el uso de estas herramientas esté restringido - en la manera que se pueda - para que no todo el mundo esté utilizándolas de forma aleatoria y nos oculten realmente un ataque.

También podrán ser utilizadas para realizar seguimientos en la red cuando creamos que alguna de nuestras máquinas ha sido comprometida.

Las herramientas que permiten este tipo de operatividad son: tcp-wrapper, netlog, argus, tcpdump, SATAN, ISS, courtney, gabriel, nocol, tcplist.

tcp-wrappers.

El tcp-wrappers es un software de domino público desarrollado por Wietse Venema (Universidad de Eindhoven, Holanda). Su función principal es: proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática.

Con este paquete podemos monitorear y filtrar peticiones entrantes a distintos Servicios TCP-IP, como: SYSTAT, FINGER, FTP, RLOGIN, RSH, REXEC, TFTP, TALK. El software está formado por un pequeño programa que se instala en el "/etc/inetd.conf".

Una vez instalado, se pueden controlar los accesos mediante el uso de reglas y dejar una traza de todos los intentos de conexión tanto admitidos como rechazados (por servicios, e indicando la máquina que hace el intento de conexión).

Netlog

Este software de dominio público diseñado por la Universidad de Texas, es una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser

"sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico).

Tcplogger

Este programa escucha todos los servicios sobre TCP, dejando una traza de cada servicio en un archivo de trazas, indicando la hora, la máquina origen y el puerto de esa conexión.

Udplogger

Es semejante al anterior, pero para los servicios sobre UDP.

Icmplogger

Se encarga de trazar el tráfico de ICMP.

Etherscan

Es una herramienta que monitorea la red buscando ciertos protocolos con actividad inusual, como puedan ser conexiones tftp - en este caso, si se han realizado con éxito nos indica qué archivos se han llevado -, comandos en el puerto de sendmail (25 tcp) como vrfy, expn, algunos comandos de rpc como rpcinfo, peticiones al servidor de NIS (algunas herramientas utilizan este tipo de servidores para obtener el archivo de password, ej: ypx), peticiones al demonio de mountd, etc. Etherscan se ejecuta en modo promiscuo en la máquina utilizando (al igual que las anteriores) el NIT (Network Interface Tap de SunOs 4.1.x), y también el "Packet Filtering Interface" para realizar esas capturas.

Nstat

Esta herramienta que originariamente fue diseñada para obtener estadísticas de uso de varios protocolos, se puede utilizar para detectar cambios en los patrones

de uso de la red, que nos puedan hacer sospechar que algo raro está pasando en la misma.

Esta herramienta viene acompañada por dos utilidades que nos permiten analizar la salida que origina nstat, a saber: nsum, nload. La primera de ellas, nos da información de ciertos periodos de tiempo. La segunda, es un programa awk que produce una salida que puede ser vista de forma gráfica por herramientas como xvgr. Para concluir este apartado, podemos decir que esta herramienta es muy útil para detectar ciertos tipos de ataques, tal como hemos reflejado anteriormente (con etherscan), así como dar una idea de qué tipo de protocolos están viajando por la red.

Además, tiene la ventaja de que al estar en modo promiscuo, con sólo tenerlo en una máquina del segmento se puede tener monitoreado todo el segmento en el que esté conectado.

Argus

Es una herramienta de dominio público que permite auditar el tráfico IP que se produce en nuestra red, mostrándonos todas las conexiones del tipo indicado que descubre.

Este programa se ejecuta como un demonio, escucha directamente la interfaz de red de la máquina y su salida es mandada bien a un archivo de trazas o a otra máquina para allí ser leída. En la captura de paquetes IP se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.

A la hora de leer esa información disponemos de una herramienta que incluye el software (llamado ra) y que nos permite también realizar filtros de visualización. Una característica de esta herramienta es la posibilidad de filtrar paquetes de acuerdo a las listas de acceso de los routers CISCO. Es posible por tanto decirle que nos

capture aquellos paquetes que no cumplen las reglas de la lista de acceso definida para esa interfaz del router. Como en el caso anterior (netlog) es posible ejecutar el comando en modo compartido (si lo que queremos es auditar todo nuestro segmento). Este programa divide las transacciones en cuatro grupos: TCP, UDP/DNS, MBONE, ICMP. Algunos ejemplos de captura pueden ser:

argus -w NombreArchivoTraza & Seguridad en Redes 5-8.

En este ejemplo le indicamos que nos capture todas la transacciones que se producen en nuestra subred y que lo almacene en un archivo.

argus -w ArchivoSalida IP and not ICMP & todo el tráfico IP pero no el ICMP.

Como decíamos antes, el ra es el programa para leer la información generada por Argus, y así podemos nombrar muchos más.

CAPITULO 3

3 Diseño de una Aplicación segura para una autenticación Passport .

3.1 Requisitos de Seguridad.

El esquema de seguridad que posean las aplicaciones Web, es un punto muy importante en su funcionamiento, ya que la aplicación debe garantizar que los usuarios trabajarán sobre un medio seguro y confiable, impidiendo que personas ajenas en la red puedan acceder a la información de forma no autorizada.

3.1.1 Servicios de Seguridad

La seguridad en la Internet tiene varios componentes, los cuales se clasifican como servicios de seguridad:

- ***Confidencialidad:*** Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos o porciones de los datos intercambiados por las entidades autorizadas.
- ***Autenticación:*** Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), contraseñas, etc. Y de origen de información.

- ***Integridad:*** Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y actualización de los mensajes transmitidos.
- ***No repudio:*** Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación.
- ***Disponibilidad:*** Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

3.1.2 Seguridades usando el protocolo SSL

Netscape ha propuesto un protocolo para proveer una capa de seguridad de los datos entre el nivel de aplicación y TCP/IP. Este protocolo de seguridad, se llama Secure Socket Layer (SSL), el mismo que brinda encriptación de datos, autenticación de servidor, integridad

de mensajes y autenticación opcional de usuario para una conexión TCP/IP; da una manera segura de establecer una comunicación con usuarios. SSL garantiza la autenticidad del contenido Web mientras verifica la identidad de los usuarios que acceden a sitios restringidos.

SSL conforma una capa entre los protocolos de aplicación, como http, SMTP, TELNET, FTP, GOPHER y NNTP, y el protocolo de conexión a Internet, TCP/IP. SSL da seguridad para iniciar una conexión TCP/IP.

SSL encripta la información en el pedido y en la respuesta HTTP, incluyendo la URL que el cliente está demandando, cualquier contenido de formulario aceptado (por ejemplo número de tarjetas de crédito), información sobre autorización de accesos (nombre de usuario y clave) y todos los datos del servidor que se envían al usuario.

SSL está incluido en los paquetes Netscape Secure Server y Netscape communicator. Actualmente se dispone de varias implementaciones para múltiples plataformas y aplicaciones, y es utilizado en diferentes productos, especialmente para la comunicación entre browsers y servidores Web.

En resumen, SSL brinda un método de encriptación y desencriptación de la información que viaja por la Web, protegiéndola de los hackers[1].

3.1.3 Autenticación

[1] Individuo que siente una gran afición por los aspectos relacionados con la informática y la electrónica y que posee conocimientos profundos sobre el funcionamiento de las computadoras. A menudo son contratados por compañías e instituciones para que evalúen las condiciones de seguridad de sus sistemas.

Como mencionamos anteriormente, la autenticación es un servicio de seguridad que necesita una identificación del cliente para comprobar que es quien dice ser.

Un mecanismo para realizar la autenticación es POP3 (Postal Office Protocol v3) que permite la comunicación por correo electrónico de forma análoga al sistema. Puede servir para saber si un usuario está registrado en el sistema operativo, lo cual se logra utilizando las funciones para el envío de e-mail al usuario del que se desea saber si es válido en el sistema. Si el resultado de este envío es correcto, significa que el usuario existe en el sistema operativo.

Ningún sistema de autenticación es totalmente confiable, y las claves de un sistema operativo también pueden ser descubiertas, por esta razón los sistemas de detección de intrusión son el

complemento perfecto para una buena autenticación, por ejemplo firewall[2].

Existen otras técnicas de autenticación, las cuales mencionamos a continuación:

- ***Kerberos:*** Es un sistema de autenticación diseñado para la utilización sobre redes inseguras (por ejemplo, Internet). El sistema Kerberos fue diseñado con dos propósitos, proveer autenticación y distribuir claves. El sistema Kerberos actúa como autoridad de certificación que garantiza una relación correcta entre claves y personas.
- ***Palabras de paso de uso único (one-time password):*** Una palabra de paso de uso único actúa exactamente como su nombre indica. Se usa una única vez y no vuelve a ser empleada. Esto proporciona una gran

[2] **Firewall.** Sistema de seguridad insertado entre Internet y una red local de empresa, que sirve de barrera lógica o filtro para evitar las intrusiones.

seguridad frente a intrusos que utilicen la repetición ciega de palabras de paso (replan).

3.1.4 Cookies

Las cookies constituyen una potente herramienta empleada por los servidores Web para almacenar y recuperar información acerca de sus visitantes. Dado que el Protocolo de Transferencia de HiperTexto (HTTP) es un protocolo sin estados (no almacena el estado de la sesión entre peticiones sucesivas), las cookies proporcionan una manera de conservar información entre peticiones del cliente, extendiendo significativamente las capacidades de las aplicaciones Cliente/Servidor basadas en Web. Mediante el uso de cookies se permite al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese

servidor, nombre y contraseña, productos que más le interesan, etc.

Una cookie es un fichero de texto que algunos servidores piden al navegador que lo almacene en el disco duro, con información acerca de lo que hemos estado haciendo por sus páginas, logrando de esta manera disminuir la carga sobre el servidor.

Los cookies no pueden extraer información de otros cookies pertenecientes a otros sitios, no pueden interactuar con otros datos en el disco duro del usuario. Sólo pueden grabar o re-llamar información.

Antes que cualquier dato pueda ser almacenado en un cookie, el sitio debe obtener tal información, diciéndole al usuario que llene una forma. Los cookies pueden llegar hasta 4K, pero en la práctica pocos exceden. También poseen

fecha de caducidad, por lo cual después de un tiempo dejan de ser operativos.

3.1.5 Seguridad de los Algoritmos

Las restricciones al uso de la criptografía se centra en lo que se conoce por criptografía segura. Se considera criptografía segura aquélla cuya decodificación está fuera del alcance de las tecnologías actuales, incluso para gobiernos o empresas que cuenten con grandes recursos materiales y humanos.

Existen varios factores que influye de manera decisiva en la seguridad de un algoritmo de criptografía:

- **Tamaño de las claves**

  Una de los factores que se emplea frecuentemente para evaluar la seguridad de un algoritmo, es el tamaño de la clave; ésta,

generalmente, es un número, y cuanto mayor sea éste, más seguro es el algoritmo, dado que serán necesarios más recursos para llevar a cabo un ataque de fuerza bruta. La siguiente tabla muestra el número de claves correspondiente a unos cuantos tamaños de clave en bits

Bits	Posibilidades
56	72057594037927936
64	18446744073709551616
128	340282366920938463463374607431768211456

Tabla 1: Tamaños de clave

Como podemos ver, al aumentar el número de bits el número de claves posibles aumenta dramáticamente. Esto se traduce en un incremento de trabajo necesario por parte de un ordenador para descifrar un mensaje encriptado.

No hay que olvidar en ningún caso que el tamaño de la clave no es una garantía de la seguridad de un algoritmo.

- **Uso de los algoritmos**

  Un factor que influye de manera decisiva en la seguridad de un algoritmo de criptografía es su uso.

  Se debe tener en cuenta el no cometer errores ya que se puede facilitar enormemente el trabajo de los criptoanalistas para descifrar los mensajes enviados.

- **Herramientas seguras**

  Es también apropiado hablar de la seguridad de las herramientas. De la misma forma que no sirve de mucho disponer de una puerta blindada con una cerradura de seguridad si en nuestro llavero llevamos el nombre y la dirección, un algoritmo seguro mal empleado no protege en absoluto el secreto del mensaje.

Por lo tanto, emplear incorrectamente un algoritmo puede ser más peligroso que no emplear encriptación, ya que esto puede producir una falsa sensación de seguridad.

- **Influencia de los avances tecnológicos**

La criptografía es una carrera constante. Por un lado, los diseñadores crean algoritmos cada vez más seguros, mientras por el otro los criptoanalistas inventan métodos de análisis más eficaces y la industria produce ordenadores más rápidos y más baratos.

La disponibilidad de ordenadores baratos cada vez más potente, empieza a hacer factibles los ataques de fuerza bruta contra algunos algoritmos. De hecho, a través de Internet, miles de usuarios han cooperado en varias ocasiones para descifrar un mensaje encriptado mediante un algoritmo seguro. Cada usuario recibe el mensaje y un paquete de claves, y prueba a desencriptarlo. Con

miles de ordenadores trabajando en paralelo, ya han sido descifrados algunos mensajes que se habían planteado como reto para los criptoanalistas.

3.2 Selección de la Plataforma y herramientas de Desarrollo

3.2.1 Administrador de Base de Datos (DBMS).

Database Management System “Sistema Administrador de Base de Datos” (DBMS), es un proceso servidor cuyo objetivo principal es proveer datos o servicios a procesos clientes que los soliciten.

El servidor de Base de Datos, a veces también llamado “Motor SQL”, proporciona las vistas lógicas y físicas de los datos, administra el control y ejecución de comandos SQL, permite

que múltiples procesos clientes accedan a la base al mismo tiempo y provee un entorno que protege a la base.

SQL

SQL (Structured Quero Lenguaje “Lenguaje Estructurado de Consulta”), es un lenguaje de programación orientado a las bases de datos, que nos permite obtener información referente a los datos almacenados en la misma. SQL es un estándar de lenguaje a partir del cual han surgido diferentes versiones según el fabricante que los ha ido desarrollando, así nos encontramos con el SQL de Microsoft, SQL Server, el de Oracle, son muy similares entre sí, pero pueden tener diferencias significativas.

SQL nos permite organizar, administrar y recuperar datos almacenados en una base de datos informático.

SQL es el lenguaje que se utiliza para interactuar con una base de datos, particularmente con bases de datos relacionales.

Cuando es necesario recuperar datos de la BD, la petición se realiza utilizando SQL. El DBMS procesa la petición SQL, recoge los datos solicitados y los devuelve a quien los solicitó.

Este procedimiento de petición de datos y posterior recepción de resultados se llama “query”.

SQL se utiliza para controlar todas las funciones de un DBMS lo cual incluye:

- **Definición de datos:** Le permite a un usuario realizar la estructura y la

organización de los datos almacenados así como las relaciones existente entre ellos.

- **Recuperación de datos:** Permite que un usuario o a un programa recuperar y utilizar los datos almacenados en una base de datos.
- **Manipulación de datos:** Permite a un usuario o a un programa actualizar la base de datos añadiendo datos nuevos, borrando los viejos y modificando los almacenados previamente.
- **Control de Acceso:** Permitir restringir la capacidad de un usuario para recuperar, añadir y modificar datos, protegiendo los datos almacenados contra accesos no autorizados.
- **Compartición de Información:** Permite coordinar la compartición de datos entre usuarios concurrentes asegurando que no haya interferencia entre ellos.
- **Integridad de Datos:** Permite definir restricciones de integridad en la base de

datos protegiéndolas de alteraciones debidas a actualizaciones inconsistentes o fallas del sistema.

Funciones que desempeña SQL

- **Es un lenguaje interactivo de consultas.-** Permite a los usuarios de manera interactiva recuperar datos y presentarlo en pantalla.
- **Es un Lenguaje de Programación de base de datos.-** Permite a los programadores introducir ordenes SQL de sus programas para acceder a los datos.
- **Es un Lenguaje de Administración de base de datos.-** Permite al administrador de una microcomputadora o sistema basado en una computadora central que utiliza SQL para definir la estructura de la base de datos y el control de acceso a los datos almacenado.

- **Es un Lenguaje de arquitectura C/S.-** Los programas de las computadoras personales utilizan SQL para comunicarse, a través de una red de área local, con los servidores de base de datos que almacenan los datos compartidos. Muchas nuevas aplicaciones utilizan esta arquitectura C/S, que minimiza el tráfico de la red.
- **Es un lenguaje de base de datos distribuidas.-** Los sistemas de administración de base de datos distribuidas utilizan SQL para ayudar a distribuir los datos a través de muchos sistemas informáticos conectados.

El DBMS de cada sistema utiliza SQL para comunicarse con el resto de sistemas, enviando peticiones para el acceso a los datos.

Acceso a Base de Datos JDBC/ODBC

Open Database Connectivity (ODBC), controlador de Microsoft Windows que tiene un API estándar para realizar conexiones a Base de Datos, sentencia SQL, conjunto de resultados, llamadas a funciones (CLI), etc.

Acceso a Base de Datos ADO.NET

ADO.NET (ActiveX Data Object) proporciona un acceso consistente a las fuentes de datos tales como Microsoft SQL Server, al igual que fuentes de datos expuestas a través de OLE DB y XML. Las aplicaciones para el consumidor de uso compartido de datos pueden utilizar ADO.NET para conectarse a estas fuentes de datos y recuperar, manipular y actualizar datos.

ADO.NET es una tecnología mucho más sencilla de utilizar, con un modelo de objetos basado en

XML, lo que permite una mejor interacción con la información desde y hacia las bases de datos.

Como sucede en ASP.NET, los objetos se encuentran encapsulados en Namespaces cada vez que quieran utilizar los objetos de ADO.NET, se deberá declarar en la página aspx, el nombre del Namespaces a utilizar.

La pieza central de una solución de software que utilice ADO.NET es el conjunto de datos. Un conjunto de datos es una copia en memoria de los datos de una base de datos. Los conjuntos de datos contienen una serie de tablas de datos, cada una de las cuales corresponde a una tabla o vista de la base de datos. Un conjunto de datos constituye una vista "desconectada" de los datos de la base de datos, es decir, existe en memoria sin una conexión activa a una base de

datos que contenga la correspondiente tabla o vista. Esta arquitectura desconectada ofrece mayor escalabilidad al utilizar los recursos del servidor sólo cuando lee o escribe en la base de datos.

Durante la ejecución, los datos pasarán de la base de datos a un objeto de negocio de la capa intermedia y después a la interfaz de usuario. Para alojar el intercambio de datos, ADO.NET utiliza un formato de persistencia y de transmisión basado en XML. Para transmitir los datos de una capa a otra, una solución ADO.NET expresa los datos en memoria (el conjunto de datos) como XML y, a continuación, envía el XML al otro componente.

La siguiente ilustración muestra los componentes principales de una solución ADO.NET.

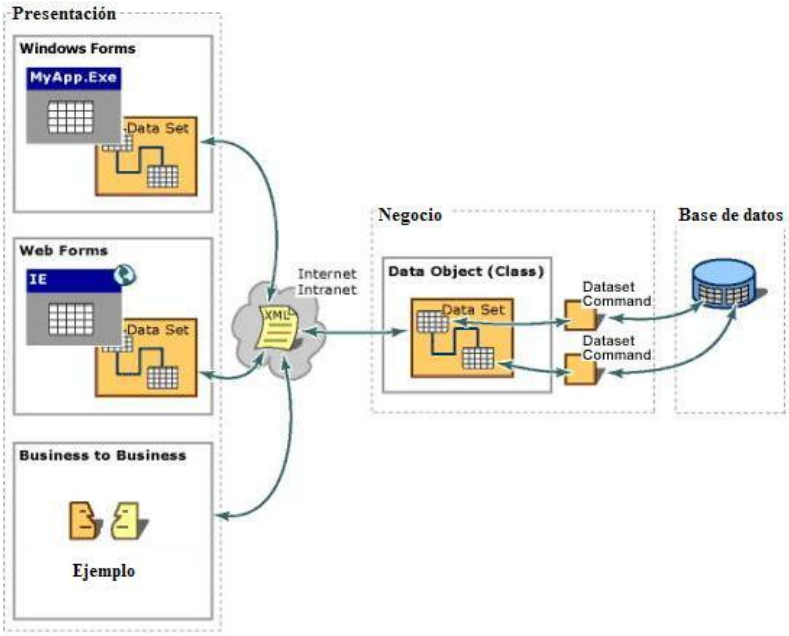


Figura 1: Arquitectura ADO.NET

3.2.2 Plataforma y Herramientas de Desarrollo

Hay que tener en cuenta muchos factores para iniciar el desarrollo de una aplicación o sitio Web, los cuales deberían estar basados en los objetivos de la aplicación y en la funcionalidad que se desea tener.

Herramientas de Desarrollo de Páginas Web: Para el desarrollo de páginas Web existe una variedad muy grande de herramientas que

facilitan el trabajo a los integrantes de un equipo de desarrollo (programador, diseñador, ingeniero de sistemas, soporte técnico, etc).

Podemos clasificar las herramientas en varios grupos, de acuerdo a la función que desempeñan:

- **Editores de Páginas Web:** Son utilizadas principalmente por los programadores, puesto que generan código HTML conforme se vayan incluyendo partes visuales en una página (tablas, entry text, radio buttons, check boxes, etc).

  - Editores de Microsoft
  - Front Page
  - Visual InterDev
  - Top Style Lite. Provisto en conjunto con Home Site, permite crear dinámicamente archivos de estilo (CSS)

- AOLpress
- HTMLtool
- Visual Studio .NET

- **Herramientas para el manejo gráfico de páginas Web:** Permiten manipular y optimizar las imágenes que formarán parte de la página. Estas herramientas son utilizadas principalmente por los diseñadores de páginas Web.

  - Microsoft Image Componer
  - Adobe Illustrator
  - Macromedia Dreamweaver mx
  - Macromedia Fireworks mx
  - Macromedia UltraDev
  - Macromedia ShockWave
  - CorelDraw
  - Flash mx
  - CorelPhotoPaint
  - Adobe Photoshop

- **Herramientas para el manejo de las base de datos:** Proveen facilidades para diseñar las estructuras de las tablas y sus relaciones en una base de datos. A partir de un diseño gráfico, se puede generar archivos con los comandos que generan los diferentes componentes de una base de datos (tablas, integridad referencial, triggers, store procedures, indices, etc). Estas herramientas son utilizadas principalmente por los administradores de base de datos.

    - Erwin

- **Herramientas orientadas a objetos:** Proveen metodologías que permiten analizar y diseñar aplicaciones orientadas a objetos. Son herramientas CASE que permiten generar código fuente a partir de un diseño de aplicación.

- Racional Rose
- UML

3.2.3 Servidor de Aplicaciones

A continuación se listan los servicios más populares que ofrece la Internet, y se describen cada uno de ellos:

- **Servidor Telnet / WAIS:** Permite al usuario remoto conectarse a un computador y usar los servicios como conexión local.
- **Servidor de Correo:** Sistema de mensajes que permite intercambiar correspondencia electrónica en la red o Internet.
- **Servidor de Listas:** Permite crear y atender listas de correo y responder automáticamente a usuarios, clientes o afiliados.

- **Servidor de Noticias:** Permite establecer foros de discusión y distribuir noticias al grupo.
- **Servidor FTP/Gopher:** Permiten mover archivos en la red o crear un servicio gopher para atender grandes cantidades de información.
- **Servidor de Fax*:*** Entrega y recibe facsímiles en demanda y por lotes.
- **Servidor Chat:** Permite a los clientes participar en conversaciones en tiempo real usando texto, imagen y audio.
- **Servidor Groupware:** Permite trabajar en grupo en una oficina virtual, sin importar la ubicación.
- **Servidor IRC:** Capacidad de participar en tiempo real en discusiones basadas en texto usando un servidor “Internet Relay Chat”.
- **Servidor Web:** Hospeda Sitios Web y publica las páginas a quien las requiera. Este

es uno de los más importantes en el desarrollo de aplicaciones en el Web.

- **Servidor Proxy – Firewall:** Permite acceso a la Internet compartiendo un enlace y al mismo tiempo protege los recursos del computador.
- **Servidor de Audio/Video:** Entrega contenido multimedia en protocolo de flujo.

3.2.4 Algoritmo de encriptación

La encriptación es el proceso en el cual los datos a proteger son traducidos a algo que parece aleatorio y que no tiene ningún significado (los datos encriptados). La desencriptación es el proceso en el cual los datos encriptados son convertidos nuevamente a su forma original.

Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en combinación con una

llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos. Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados (exactamente igual a como estaban antes de ser encriptados si se usó la misma llave). Si la llave o los datos son modificados el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible. Incluso

para una llave de sólo 40 bits, esto significa 2ˆ40 (poco más de 1 trillón) de llaves posibles.

Figura 2: Ej. al Encriptar un mensaje es similar como ponerlo en una caja y cerrarla con llave. En encriptación una persona que conoce la clave puede abrir la caja y acceder al mensaje

Existen un sin número de algoritmos para cifrar y descifrar datos, pero los más conocidos son los siguientes:

- **DES (Digital Encryption Standard, Estándar de cifrado digital)**

  Creado en 1975 con ayuda de la NSA (National Security Agency), en 1982 se convirtió en un estándar. Utiliza una llave de 56 bit. En 1999 logró ser quebrado (violado) en menos de 24 horas por un servidor dedicado a eso. Esto lo calificó como un algoritmo inseguro y con falencias reconocidas.

- **MAC (Message Authentication Code)**

  Un código de autentificación de mensaje (message authentication code o MAC) es un bloque de datos de tamaño fijo que se envía con un mensaje para averiguar su origen e integridad. Son muy útiles para proporcionar autentificación e integridad sin confidencialidad. Para generar MACs se pueden usar algoritmos de clave secreta, de clave pública y algoritmos de resumen de mensajes.

  MAC se pueden usar para verificar la autenticidad de los mensajes, no se pueden usar para firmar los mensajes, ya que sólo se usa una clave secreta que comparten el emisor y el receptor, lo que hace que ambos puedan generar la misma firma.

- **Triple DES**

  Triple DES (llave de 168 bits que comprende tres claves únicas de 56 bits), es un

algoritmo desarrollado por el gobierno de EEUU y ha sido evaluado durante años sin descubrírsele debilidades. Es una configuración de encriptación en la cual el algoritmo DES es usado tres veces con tres llaves diferentes.

- **Rijndael**

  Llave de 256 bits, es un algoritmo seguro y eficiente. Sus creadores son Joan Daemen y Vincent Rijmen (Bélgica). Ha sido elegido como el nuevo Estándar Avanzado de Encriptación (AES) por el Instituto Nacional de Estándares y Tecnología (NIST) de los EEUU. Junto a 3DES es de los más seguros.

- **Blowfish**

  Llave de 448 bits, es un algoritmo de encriptación rápido y fuerte. Su creador es Bruce Schneier, uno de los más prestigiosos criptógrafos en el mundo.

- **Gost**

  Llave de 256 bits, es un algoritmo de Rusia y podría ser considerado el análogo ruso al DES. Tiene un diseño conservador y no ha podido ser vulnerado, a pesar de haber sido uno de los más estudiados, durante años, por los mejores expertos en criptoanálisis.

- **IDEA (International Data Encryption Algorithm)**

  Más conocido como un componente de PGP (encriptación de mails), trabaja con llaves de 128 bits. Realiza procesos de shift y copiado y pegado de los 128 bits, dejando un total de 52 sub llaves de 16 bits cada una. Es un algoritmo más rápido que DES, pero al ser nuevo, aun no es aceptado como un

estándar, aunque no se le han encontrado debilidades aún.

3.3 Comparación de las diferentes herramientas utilizadas en el desarrollo de la aplicación.

Para el desarrollo de la cuenta Passport , hemos considerado el uso de las siguientes herramientas, las mismas que fueron evaluadas con otras herramientas por su aceptación en el mercado, costos, facilidad de uso etc.

3.3.1 Selección del Sistema Operativo del Servidor

Windows 2000 Server es la versión básica de la familia de servidores. Este es el sistema operativo de red multipropósito para los negocios de todos los tamaños. Es la solución perfecta para servidores de archivos,

impresión, intranet e infraestructura. Escala desde 1 hasta 4 procesadores y aprovecha hasta 4 gigabytes de memoria RAM.

Existen muchas razones para usar Windows 2000 Server:

- **Valor empresarial:** Está específicamente diseñado para permitir que las empresas utilicen fiable y económicamente las tecnologías emergentes para incrementar la rentabilidad de sus negocios y su agilidad en un mercado siempre cambiante.
- **Fiabilidad:** Ninguna empresa puede permitirse que se caiga el servidor. La arquitectura del sistema de Windows 2000 ayudan a conseguir un mayor tiempo de actividad.
- **Disponibilidad:** Las ediciones Advanced Server y Datacenter Server de la familia Windows 2000 Server le permiten incrementar la disponibilidad de su sistema,

utilizando las tecnologías de clustering incluidas en el sistema operativo, que le permiten asociar servidores para soportar tareas específicas.

- **Ejecución:** Windows 2000 Advanced Server proporciona un rendimiento líder en el sector por menos de la mitad del costo de la solución más ampliable basada en UNIX.
- **Escalabilidad:** Por ello la familia Windows 2000 Server incluye tres versiones, todas ellas capaces de gestionar fiable y económicamente grandes cargas. Se puede comenzar con Windows 2000 Server e ir migrando cuando se lo necesite.
- **Manejabilidad:** Con la familia Windows 2000 Server es más fácil implementar, configurar y utilizar capacidades avanzadas de red para suministrar servicios de administración centralizados y personalizable. Y puede administrar dinámicamente el almacenamiento en los

servidores de archivos sin interrumpir a los usuarios finales.

- **Hardware:** Windows 2000 soporta una amplia gama de hardware y periféricos, para soportar aplicaciones extremadamente grandes.
- **Preparado para .NET:** La familia Windows 2000 Server encaja en el futuro .NET introduciendo bloques de construcción esenciales, tales como la simplificación del desarrollo informático centrado en Internet, soporte XML y comunicaciones, que son características centrales de la plataforma .NET

Solaris

Solaris 10 permite soportar más de 250 hardware de sistema para correr sobre unidades Unix, Sparc y también arquitecturas

x86 (PC), además de operar con los próximos procesadores de 64 bits AMD64 y EM64T.

Este sistema, uno de los Unix comerciales y propietarios con más "solera" junto al UnixWare de SCO, se propone cómo una buena alternativa a los sistemas de Microsoft e incluso a Linux en el campo de los servidores y, gracias al esfuerzo realizado estos últimos años en la creación del software adecuado, incluso se atreve a abordar el campo de los desktop. Se debe mencionar además que es el sistema operativo mas costoso tanto la adquisición de Licenciamiento como en adquisición del software.

Linux

Sistema operativo de código fuente abierto. Sun comercializará una implementación completa del sistema operativo Linux en una

nueva gama de servidores destinados a servicios punteros, al tiempo que ofrecerá tecnología Sun ONE clave en una plataforma Linux.

El software Linux así como también un sin número de aplicaciones son de código abierto (gratuitos).
No requieren supervisión tan estrecha ni pagos de pólizas de mantenimiento necesarias para obtener los Service Packs.

La plataforma Linux es más robusta lo cual hace más difícil que algún intruso pueda violar el sistema de seguridad de Linux.

Linux es el sistema operativo mas económico, ya que requieren menor mantenimiento. En servidores Windows es más costoso debido a que es necesaria una frecuente atención y

monitoreo contra ataques de virus, hackers y errores de código.

Comparación de costos

Los costos de adquisición de software por unidad de procesamiento fueron como sigue:

Caso	Adquisición Software	Compra de Equipos	Soporte del Sistema
Linux	$400	$37,511	$ 10*
Solaris	$27,500	$ 345,400	$19,309
Windows	$5,320	$ 38,524	$1,520

Tabla 2: Comparación de costos

Los modelos de licenciamiento de Linux son más flexibles que los de Solaris o Windows. Linux es una de las opciones más competitiva, pero uno de los sistemas operativos de mayor facilidad de uso es Windows que en este momento continúa siendo el sistema operativo más comercial lo cual se refleja en la disponibilidad de aplicaciones, facilidad de mantenimiento así como soporte en el desarrollo de nuevas aplicaciones, puntos que

pueden ser cruciales en la elección de servidores que corren aplicaciones web.

Además el fruto de la inversión realizada por Microsoft y aunado a una comunidad de programadores cada vez más grande se ha logrado facilitar el desarrollo de aplicaciones y sistemas que corran sobre servidores Windows lo cual se ve reflejado en tiempos de desarrollo menores. La curva de aprendizaje en el sistema Windows es mucho menor.

3.3.2 . Selección de Base de Datos

El servidor 2000 del SQL funciona solamente en plataformas Windows-based, incluyendo el CE de Windows 9x, de Windows NT, de Windows 2000 y de Windows.

En comparación con el servidor 2000 del SQL, la base de datos del Oracle 9i apoya todas las plataformas conocidas, incluyendo plataformas Windows-based, los sistemas AIX-Basados, Compaq Tru64 UNIX, serie HP-UX, Linux Intel, sol Solaris del HP 9000 etc.

Para instalar el servidor 2000 del SQL, usted debe tener Intel o las plataformas compatibles y el hardware siguiente:

Hardware	Requisitos
Procesador	Pentium 166 megaciclos o más arriba
Memoria	RAM de 32 MB (mínimo para el motor de escritorio), Con 64 MB de RAM (mínimo para el resto de las ediciones), o de 128 MB recomendado
Espacio de disco duro	270 MB (instalación completa), 250 MB (típico), 95 MB (mínimo), Motor De escritorio: 44 MB Servicios de Análisis: 50 MB mínimos y 130 MB máximo

Tabla 3: Requerimiento de instalación de Windows 2000 Server

Oracle 9i soporta todas los equipos Intel y Amd o plataformas compatibles, sistemas AIX-

Basados, Compaq Tru64 UNIX, serie HP-UX, Linux Intel, sol Solaris del HP 9000 etc.

Para instalar el Oracle 9i bajo la Intel o plataformas compatibles, usted debe tener el hardware siguiente:

Hardware	Requisitos
Procesador	Pentium 166 de MB o más.
Memoria	Capacidad: 128 MB de RAM (256 MB recomendado) Memoria Virtual: De 200 hasta 400 como máximo
Espacio de disco duro	140 MB en la ejecución del sistema más 4.5 GB para la ejecución de Oracle (FAT) o 2.8 GB para la ejecución de Oracle (NTFS)

Tabla 4: Requerimiento de Hardware para instalar Oracle bajo Intel

Para instalar la base de datos del Oracle 9i bajo sistemas de UNIX, tales como sistemas AIX-Basados, Compaq Tru64 UNIX, serie HP-UX del HP 9000, y sol Solaris, usted debe tener el hardware siguiente:

Hardware	Requisitos
Memoria	Un mínimo de RAM de 512 MB
Espacio swap	Un mínimo de RAM de 2x MB o de 400 MB
Espacio de disco duro	4.5 GB

Tabla 5: Requerimiento de Hardware para instalar Oracle bajo Unix

El servidor 2000 del SQL viene en seis ediciones: La empresa, el estándar, personal, revelador, motor de escritorio, y el CE del servidor del SQL (una versión compatible para el CE de Windows) y requiere el software siguiente:

Sistema Operativo	Edición De la Empresa	Edición Estándar	Edición Personal	Edición Del Revelador	Motor De escritorio	CE Del Servidor del Sql
CE De Windows	No	No	No	No	No	Sí
Windows 9x	No	No	Sí	No	Sí	No
Sitio de trabajo de Windows NT 4.0 con el paquete 5 del servicio	No	No	Sí	Sí	Sí	No
Servidor de Windows NT 4.0 con el paquete 5 del servicio	Sí	Sí	Sí	Sí	Sí	No
Edición de la empresa del servidor de Windows NT 4.0 con el paquete 5 del	Sí	Sí	Sí	Sí	Sí	No

servicio						
Profesional De Windows 2000	No	No	Sí	Sí	Sí	No
Servidor 2000 De Windows	Sí	Sí	Sí	Sí	Sí	No
Servidor Avanzado De Windows 2000	Sí	Sí	Sí	Sí	Sí	No
Windows DataCenter 2000	Sí	Sí	Sí	Sí	Sí	No
Profesional De Windows.xp	No	No	Sí	Sí	Sí	No

Tabla 6: Requerimiento de Software para Servidor 2000 SQL

La base de datos del Oracle 9i viene en tres ediciones: La empresa, estándar y personal requiere el software siguiente:

Plataforma	Versión Del Sistema Operativo	Remiendos Requeridos
Windows-based	Windows NT 4.0	Mantenga el Paquete 5
Windows-based	Windows 2000	Mantenga el Paquete 1
Windows-based	Windows.xp	No necesario
AIX-Basado	AIX 4.3.3	Nivel 09 e IY24568 del mantenimiento, IY25282, IY27614, IY30151
AIX-Basado	AIX 5.1	Lanzamiento 5.1 ML01+ (IY22854) de AIX 5L, IY26778, IY28766, IY28949, IY29965, IY30150
Compaq Tru64 UNIX	Tru64 5.1	5.1 patchkit 4

Compaq Tru64 UNIX	Tru64 5.1A	5.1A patchkit 1
HP-UX	Versión 11.0 de HP-UX (64-bit)	Sept. Del 2001 Paquete de calidad, PHCO_23792, PHCO_24148, PHKL_24268, PHKL_24729, PHKL _ 25475, PHKL_25525, PHNE_24715, PHSS_22868
Linux	Servidor 7 de la Empresa de SuSE Linux (o SLES-7) con el núcleo 2.4.7, y glibc 2.2.2	No necesario
Sol Solaris	Solaris 32-Bit 2.6 (5.6), 7 (5.7) o 8 (5.8)	No necesario
Sol Solaris	Solaris 64-Bit 8 (5.8)	Actualización 5

Tabla 7: Requerimiento de Software para Oracle

Comparación de costos

Una de las ventajas principales del servidor 2000 de Microsoft SQL en comparación con la base de datos de Oracle 9i, es que el servidor del SQL es más barato. La otra ventaja del servidor del SQL es que Microsoft incluye el proceso analítico en línea (OLAP) y la explotación minera de los datos como

características de estándar en la edición 2000 de la empresa del servidor del SQL. Así pues, usted puede ahorrar hasta cuatro veces con la edición 2000 de la empresa del servidor del SQL si usted utiliza OLAP y la explotación minera de los datos.

Las comparaciones del precio fueron basadas en Oracle y el servidor 2000 del sql.

Comparación de la edición estándar del servidor 2000 del SQL y la edición estándar de Oracle9i:

Número de CPUs	Edición Del Estándar De Oracle9i	Edición Del Estándar Del Servidor 2000 del Sql
1	$15.000	$4.999
2	$30.000	$9.998
4	$60.000	$19.996
8	$120.000	$39.992
16	$240.000	$79.984
32	$480.000	$159.968

Tabla 8: Comparación de costos entre Oracle y Windows 2000 server

Comparación de la edición 2000 de la empresa del servidor de SQL (que incluyen OLAP y explotación minera de los datos) y edición de la empresa de Oracle9i con OLAP y/o la explotación minera de los datos:

Número de CPUs	Edición De la Empresa De Oracle9i	Edición de la empresa de Oracle9i con OLAP o la explotación minera de los datos	Edición de la empresa de Oracle9i con OLAP y la explotación minera de los datos	Edición 2000 De la Empresa Del Servidor del Sql
1	$40.000	$60.000	$80.000	$19.999
2	$80.000	$120.000	$160.000	$39.998
4	$160.000	$240.000	$320.000	$79.996
8	$320.000	$480.000	$640.000	$159.992
16	$640.000	$960.000	$1.280.000	$319.984
32	$1.280.000	$1.920.000	$2.560.000	$639.968

Tabla 9: Comparación de costos entre Oracle y Windows 2000 empresa

Esto no es una comparación del precio completo entre el servidor 2000 del SQL y la base de datos del Oracle 9i. Es solamente una breve comparación en el que puede haber cualquier descuento, y los precios se pueden aumentar o disminuir en el futuro.

En el siguiente cuadro presentamos algunos límites del servidor 2000 del SQL y de la base de datos Oracle 9i:

Característica	Servidor 2000 del SQL	Base de datos Del Oracle 9i
longitud conocida de la base de datos	128	8
longitud conocida de la columna	128	30
longitud conocida del índice	128	30
longitud conocida de la tabla	128	30
longitud conocida de la visión	128	30
longitud almacenada del nombre del procedimiento	128	30
columnas máximas por índice	16	32
tamaño máximo del char()	8000	2000
tamaño máximo del varchar()	8000	4000
columnas máximas por la tabla	1024	1000
longitud máxima de la fila de la tabla	8036	255000
tamaño máximo de la pregunta	16777216	16777216
subqueries recurrentes	40	64
tamaño constante de la secuencia en SELECT	16777207	4000
tamaño constante de la secuencia adentro DONDE	8000	4000

Tabla 10: Limitantes entre Windows 2000 Server y Oracle

No es verdad que el servidor 2000 del SQL es mejor que el Oracle 9i o viceversa. Ambos productos se pueden utilizar para construir sistemas estables y eficiente. La estabilidad y

la eficacia de sus usos y bases de datos, dependen algo de la experiencia de los reveladores de la base de datos y del administrador de la base de datos que del abastecedor de base de datos. Pero el servidor 2000 del SQL tiene algunas ventajas en comparación con el Oracle 9i y viceversa.

Las ventajas del servidor 2000 del SQL:

- El servidor 2000 del SQL, es más barato comprar que base de datos del Oracle 9i.
- El servidor 2000 del SQL celebra los resultados del funcionamiento, precio y rendimiento del TPC-C.
- El servidor 2000 del SQL se acepta generalmente como más fácil instalar, utilizar y manejar.

Las ventajas de la base de datos del Oracle 9i:

- La base de datos del Oracle 9i apoya todas las plataformas; no solamente las plataformas windows-based.
- PL/SQL es una lengua más de gran alcance que T-SQL.

3.3.3 Comparación de tecnología Java vs .Net

Java nace como un lenguaje de programación fácil de utilizar; algunos de los programadores de Sun Microsystems, cansados de “pelear” con C++, obtienen la autorización de sus jefes para desarrollar un lenguaje de programación que sea muy sencillo de utilizar, y que pueda ser ejecutado sobre dispositivos pequeños: televisores, electrodomésticos, o cualquier implemento eléctrico instalado en casa.

Este proyecto empieza a demandar tiempo y dinero, y se obtiene un primer producto, OAK,3 con el cual no se logra la aceptación esperada, y el proyecto queda descartado. Un tiempo después, con la aparición de WWW, se piensa que el proyecto debe ser revaluado, y se le da un nuevo impulso, apareciendo Java.4 Pero, ¿qué es lo que se presenta como Java? Lo que Sun presenta al mundo como su nuevo lenguaje de programación es algo más: es un lenguaje de programación orientado a objetos, que además incluye una máquina virtual, y una serie de desarrollos básicos que pueden ser empleados por los programadores para simplificar sus nuevos desarrollos; además permite la inclusión de porciones de código ejecutables en las páginas que se publican en Internet, a través de WWW. Sun permite también que otros fabricantes de software tomen a Java como el centro de sus nuevas herramientas de software, es decir, desarrollen entornos de programación

considerando a Java como su corazón; de manera que en un tiempo relativamente corto IBM, Borland, Oracle y muchos otros (incluyendo a Microsoft) están desarrollando herramientas que les permitan ofrecer productos portables entre diferentes máquinas y sistemas operativos, pues todos compilan para la misma máquina: la máquina virtual de Java.

Hoy en día, Java cuenta con un API amplio, en el cual pueden encontrarse puntos de partida para crear los más diversos tipos de programas, tiene una serie de estándares para programación reconocidos y aceptados por la mayoría de sus programadores, existen las versiones de su máquina virtual para casi todas las plataformas comerciales vigentes en este momento y está en capacidad de hacer interfaz con casi todas las bases de datos existentes en el mercado. Además, Java tiene otra gran ventaja: Microsoft le declaró la guerra hace algún tiempo y muchas

de las personas involucradas con el negocio del software que no aceptan a esta empresa ven a Java como su aliado. A partir de lo presentado hasta el momento se puede creer que Java es un lenguaje de programación bastante popular, y en lo que a Internet se refiere esto es cierto, pues tiene buena parte de los servidores conectados a esta red. Sin embargo no todo es dicha, pues en la parte de aplicaciones comerciales para las empresas no se ha logrado tener el mercado ni la aceptación que se quisiera, y las razones son varias: Java no ofrece un entorno de programación completo, además el producto final no es muy veloz en tiempo de ejecución, entre otras cosas.

.NET prácticamente desde la aparición de Java, Microsoft ha querido ser su competencia, para ello inicialmente firmó algunos convenios con Sun, para trabajar con Java igual que lo estaban haciendo IBM y Oracle, pero en realidad trató de

crear su versión propia de Java, denominada J++, la cual no era completamente compatible con la versión estándar. Además introdujo algunas modificaciones en sus sistemas operativos y navegadores que hacían que el desempeño de aplicaciones desarrolladas en Java fuese más lento de lo que debía. Pero en el momento en que Java empieza a consolidarse como el lenguaje de Internet, la decisión es más fuerte, hay que lanzar “algo” que realmente le haga contrapeso a Java, y que pueda ser considerado como la competencia de Java en Internet, y a raíz de ello aparece .NET. Y aquí hay que tratar de revisar qué es .NET?, inicialmente se podría pensar que es un lenguaje de programación orientado a objetos, o un conjunto de lenguajes de programación todos ellos orientados a objetos, y se pueden citar C#.NET, C++.NET yVisualBasic.NET; pero a esta última Definición le hace falta incluir lo referente al acceso a las bases de datos, es decir

ADO.NET, las herramientas para desarrollo en Internet, ASP.NET y el conjunto de facilidades para construir Servicios Web, además del hecho de que todo viene integrado dentro de un entorno completo denominado VisualStudio.NET.

Para lograr elaborar estas herramientas y tener la certeza de que se integrarán bien, se definieron los siguientes elementos:

- Un lenguaje común de ejecución: CLR (Common Language Runtime).
- Un conjunto de tipos de datos básicos: CTS (Common Type System), el cual incluye, además de todos los tipos de datos básicos, las clases Object y String.
- Un CLS (Common Language Specification), que es el conjunto de reglas que especifica lo referente a la implementación de las características de la POO y a otras estructuras sintácticas.

- Un MSIL (MicroSoft Intermediate Language), o lenguaje intermedio común. Este lenguaje es el equivalente al bytecode de Java.
- Un compilador capaz de traducir del MSIL a lenguaje binario, comúnmente denominado JIT (JustIn Time).

Así pues, se puede decir que .NET es más que un conjunto de herramientas: con .NET se rompe la filosofía tradicional de Microsoft, pues se ha hecho un esfuerzo para que .NET sea abierto y estándar; para lo cual sometieron sus especificaciones del lenguaje y su tipo común de datos a la revisión de organismos internacionales dedicados a la regulación y estandarización de las plataformas de programación; y una vez aprobados los hicieron públicos. De hecho Microsoft garantiza que si otro productor de software construye un lenguaje que al compilar lleve al tipo común de datos y respete las especificaciones que ellos

han dado, ese lenguaje podrá ser incorporado a ambientes .NET, y las clases creadas a través de él podrán interactuar con los elementos de .NET sin ningún problema. Y como muestra de esto puede hacerse referencia a “Mono”, de Ximian, que se esfuerza en ofrecer una implementación para cualquier tipo de ambiente Unix, de todo el Framework de .NET, y ya ofrece el compilador para C#, el runtime (compilador, intérprete, recolector de basura, manejador de multi-hilo, etc.),versiones del API, además de versiones de ADO.NET y de ASP.NET.6

Java vs. Los lenguajes de .NET

Siguiendo con lo propuesto se van a presentar algunas diferencias entre los lenguajes de .NET y Java, vistos como lenguajes de programación orientados a objetos, para lo cual se partirá de ver la forma en la cual cada uno de ellos implementa las características de la POO, cómo es el manejo de los objetos como tales, el encapsulamiento, la herencia y el polimorfismo. Y también se verán algunas diferencias de sintaxis.

.net	Java
Tipos de estructura que les permite a un programador:	
Clases, interfaces, struct y enum.	Clases e interfaces.
Elementos que pueden definirse dentro de una clase:	
Atributos, métodos y clases internas	Atributos, métodos, clases internas, propiedades, eventos y delegates.
Niveles de encapsulamiento:	
public, private, protected y visibilidad de paquete, este último se asume cuando se	public, private, internal, protected y la combinación de estos dos últimos. En caso de omisión se

omite.	asume private.
Herencia:	
No se permite la herencia múltiple, se puede simular a través del uso de interfaces. Por omisión se hereda de Object.	No se permite la herencia múltiple, se puede simular a través del uso de interfaces. Por omisión se hereda de Object.
Polimorfismo:	
Se permite que una clase sobrecargue o sobreescriba métodos definidos por su clase padre, a menos que la clase padre lo impida mediante la palabra reservada final, en el encabezado del método. Si un objeto de una clase hija es referenciado a través de una referencia a su clase padre, su comportamiento, al invocar un método sobreescrito, será el que definió la clase a la cual él pertenece.	NET Se permite que una clase sobrecargue o sobreescriba métodos definidos por su clase padre, a menos que la clase padre lo impida empleando la palabra reservada sealed, en el encabezado del método. Si un objeto de una clase hija es referenciado a través de una referencia a su clase padre, su comportamiento, al invocar un método sobreescrito, dependerá de los permisos establecidos por la clase padre, y de la decisión tomada por quien definió la clase. Por omisión se comportará como lo definió la clase padre.

Tabla 11: Java vs .NET

3.3.4 Selección de Algoritmo de Encriptación

La longitud de las claves encriptadas proporciona una indicación del coste computacional de un ataque por fuerza bruta sobre la clave. La autentica resistencia de los algoritmos criptográficos es mucho mas difícil de evaluar.

En la siguiente tabla, la diferencia entre las dos columnas de prestaciones proviene del hecho de que las cifras dada por Schneier están basadas en el código C, sin ningún intento de optimizar el código. Y las del PRB son el resultado de un esfuerzo para producir implementaciones propietarias, optimizadas, de los algoritmos en el lenguaje ensamblador.

Algoritmo	Tamaño de clave / tamaño de dispersión(bits)	Velocidad extrapolada (kbytes/sec)	PRB optimizado (kbytes/s)
TEA	128	700	----
DES	56	350	7746
Triple-DES	168	120	2842
IDEA	128	700	4469
RSA	512	7	----
RSA	2048	1	----
MD5	128	1740	62425
SHA	160	750	25162

Tabla 12: Prestaciones de los algoritmos de encriptación y resúmenes seguros

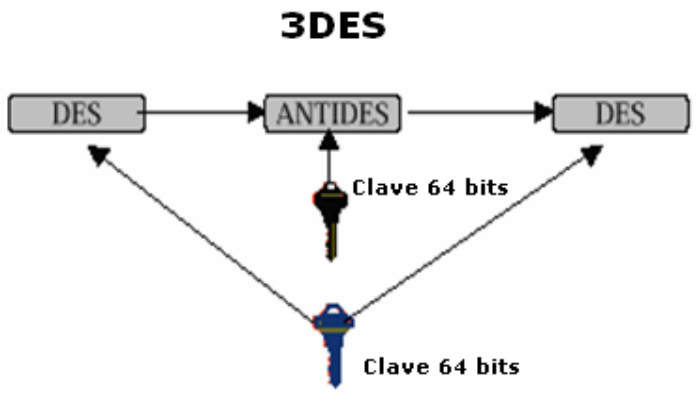
Por el momento a el algoritmo 3DES no se le ha encontrado debilidad alguna en lo que se refiere a vulnerabilidad ya que posee una configuración de encriptación en la cual el algoritmo DES es usado tres veces con tres llaves diferentes, que lo hace difícil de ser descifrado.

Funcionamiento de 3DES:

Consiste en aplicar varias veces el algoritmo DES con diferentes claves al mensaje original.

- El Triple-DES responde a la siguiente estructura:

  Codificar con la subclave k1, decodificar con k2 y volver a codificar con k1. La clave resultante es la concatenación de k1 y k2, con una longitud de 112 bits.



- Para garantizar la integridad de los datos a la clave resultante (encriptada) se utiliza un hash (o función resumen) que es sencillamente una función matemática que toma como entrada la clave y devuelve un

número bits relativamente pequeño. La característica importante de ésta función es que si se modifica aunque sea solamente un bit del dato, el hash calculado se modificará por completo.

- Una vez realizado el proceso de hash en la clave, se le aplica la conversión a cadenas de caracteres mediante una función propia del lenguaje de desarrollo.
- De esta forma se almacena en la base de datos la clave encriptada.

3.4 Análisis y Diseño de la Aplicación

Para implementar un sistema orientado a objetos distribuidos usando la arquitectura .NET, se debe realizar el análisis y diseño exhaustivo para poder identificar los objetos que interactuarán en el sistema. Uno de los métodos usados para poder identificar los posibles objetos es a través de los casos de Usos.

Un caso de uso es una tabla donde se describe paso a paso cada unas de las metas que se desea alcanzar para elaborar el sistema, detallando quienes son los actores primarios (usuarios), actores secundarios (entidad o sistema externo para poder obtener el éxito de la meta) y el escenario (secuencia de interacción que se dan bajo ciertas condiciones para alcanzar una meta).

Sobre la base de requerimientos planteados para desarrollar el Sistema de Servicio de Autenticación de cuenta Passport , se identificaron las siguientes metas:

- **Manejo de Usuarios.-** Usar la información personal de cada usuario para la operación y mantenimiento de su cuenta y el servicio Passport .
- **Autenticación personal**.- Para dar facilidad en el desplazamiento entre sitios Web.

- **Manejo de Nombre de Inicio de Sesión.-** Brindar la posibilidad de usar un nombre de inicio de sesión y una contraseña en todos los sitios asociados a nuestro servicio.
- **Control de Cuentas de Usuario expirada.-** Si la cuenta Passport no ha sido utilizada por 90 días podrá expirar y puede que sea necesario restablecer una nueva cuenta.
- **Privacidad y Protección de Información.-** Para proporcionar privacidad y protección de la información personal de los usuarios. El servicio de Passport no permitirá ésta información a terceros.

3.4.1 Análisis de Casos de Usos

Lista de Casos de Usos

- Manejo de Usuarios
- Autenticación personal
- Manejo de Nombre de Inicio de Sesión
- Control de Cuentas de Usuario expirada
- Privacidad y Protección de Información

Especificaciones de Actores:

Nombre: USUARIO

Descripción: Persona asociada al servicio de Cuenta Passport .

Notas: No se preocupa por sus seguridad de acceso al obtener el servicio Passport .

Se preocupa por obtener una cuenta de usuario segura y confible para acceder a varios sitios WEB.

Nombre: SITIOS WEB ASOCIADOS

Descripción: Portales que dan diferentes servicios (pueden ser compra, venta, etc) y que necesitan de la seguridad de la información de sus clientes como de sus transacciones.

Notas: Confiar en la seguridad de datos por contar son el servicio Passport para el acceso de sus usuarios.

Nombre: SERVICIO MI P@SAPORTE (BASE DE DATOS)

Descripción: Base de datos de la empresa que ofrece el servicio de cuentas Passport .

Notas: Contiene información personal de los usuarios que aperturan una cuentas.

Cada usuario debe definir un nombre de usuario y contraseña que se registrará en la base para permitir el acceso a los diferentes sitios asociados.

3.4.2 Modelo de Diseño de Objetos

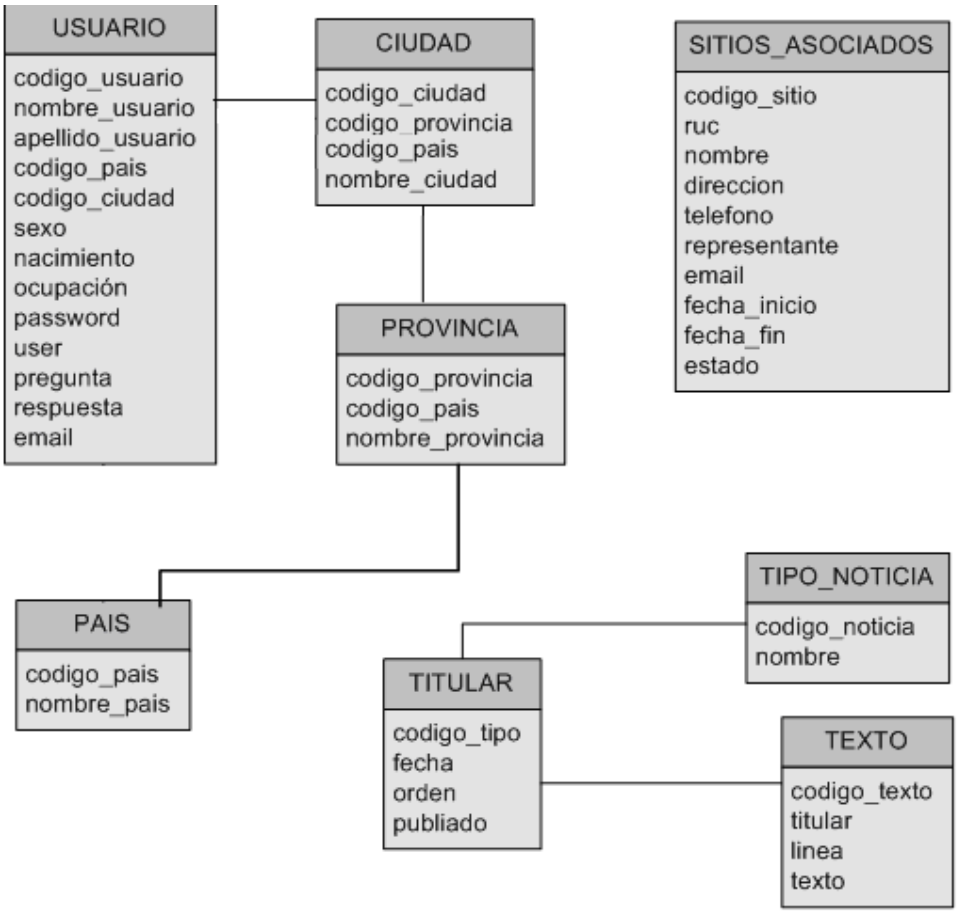


Figura 3: Modelo de Diseño Orientado a Objeto de Servicio Passport

3.4.1 Especificación de Clases

Clase: USUARIO

Descripción: Clase que administra los usuarios que aperturan cuentas Passport para el acceso seguro a los sitios Web asociados.

Atributos	Descripción
codigoUsuario	Código de identificación único de usuario
nombreUsuario	Nombre del Usuario
apellidoUsuario	Apellido del Usuario
codigoProvincia	Código de Provincia donde pertenece
codigoCiudad	Código de ciudad
Sexo	Sexo del usuario
fechaNacimiento	Fecha de Nacimiento del usuario
Ocupación	Ocupación a que se dedica el usuario
user	Nombre de Usuario para identificarse en el acceso a los sitios Webs
Password	Contraseña de definida por usuario
pregunta	Pregunta que le permitirá restablecer la contraseña en caso de olvido.
respuesta	Respuesta a la pregunta en caso de restablecer su contraseña
email	Correo electrónico para comunicación de novedades

Tabla 13: Clase de Usuario

Clase: CIUDAD

Descripción: Clase que identifica a los diferentes ciudades al que pueden pertenecer los usuarios.

Atributos	Descripción
codigoCiudad	Código único de identificación de ciudades
codigoProvincia	Código único de identificación de provincia por ciudad
nombreCiudad	Nombre de Ciudad a donde pertenece el usuario

Tabla 14: Clase Ciudad

Clase: PROVINCIA

Descripción: Clase que administra los datos de las diferentes provincias de un país.

Atributos	Descripción
codigoProvincia	Código que identifica a una Provincia
codigoPais	Código que identifica a un país
nombreCiudad	Nombre que identifica a una provincia

Tabla 15: Clase Provincia

Clase: PAIS

Descripción: Clase que administra los países de una región.

Atributos	Descripción
CodigoPais	Código que identifica a un país
NombrePais	Nombre que identifica a una país

Tabla 16: Clase País

Clase: SITIOS_ASOCIADOS

Descripción: Clase que administra y almacena datos de los diferentes sitios asociados a nuestro servicio Web.

Atributos	Descripción
CodigoSitio	Código único que identificará a un sitio Web.
Nombre	Nombre como se identifica al sitio Web
Email	Correo electrónico por el cual se puede permitir comunicación entre nuestro servicio y el sitio Web asociado
Direccion	Dirección de localización del Sitio Web
FechaInicio	Fecha en que se inicia el servicio
FechaFin	Fecha en que concluye la prestación de servicio
Estado	Estatus o estado del sitio Web

Tabla 17: Clase Asociados

Clase: USUARIO_SITIO

Descripción: Clase que contiene la relación entre un usuario y el sitio WEB al que puede acceder.

Atributos	Descripción
CodigoUsuario	Código de Usuario
CodigoSitio	Código del sitio al que se permitirá acceder al usuario

Tabla 18: Clase Usuario Sitio

3.4.2 Diagrama de Interacción

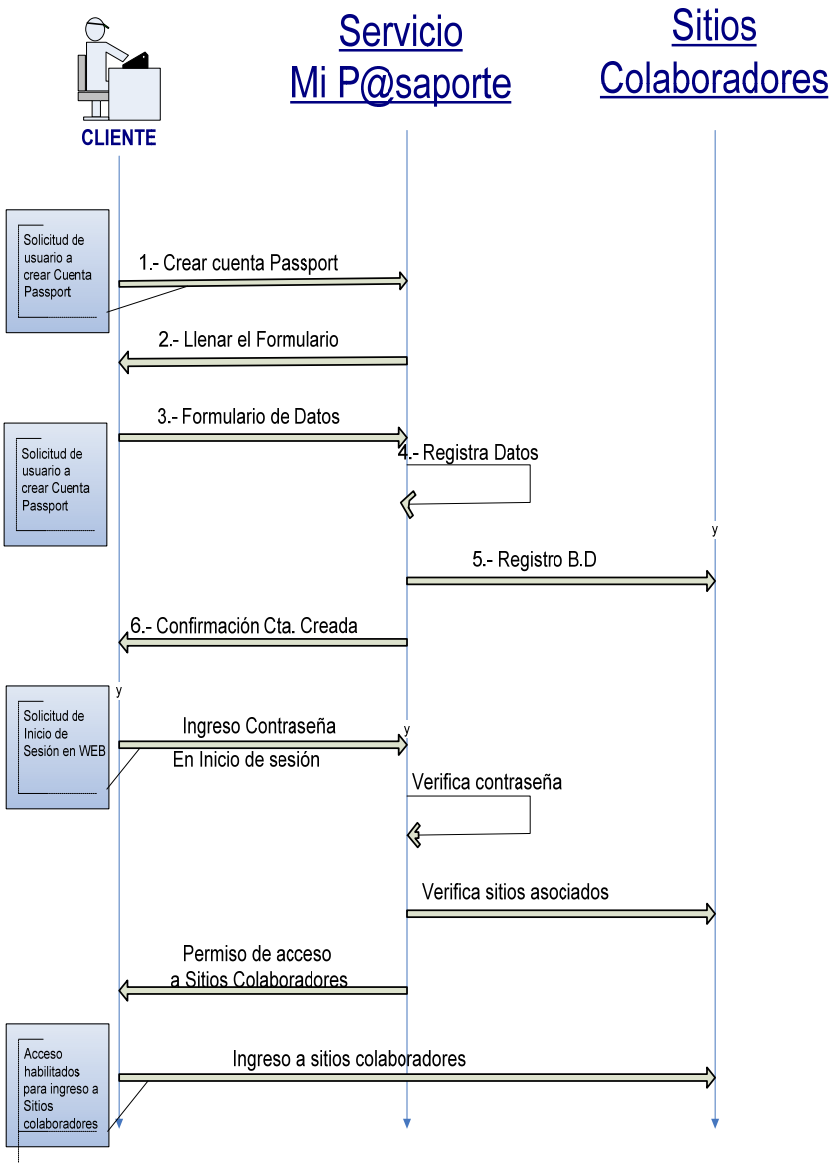


Figura 4: Diagrama de Interacción

3.4.3 Modelo Entidad Relación

Administración de Usuarios

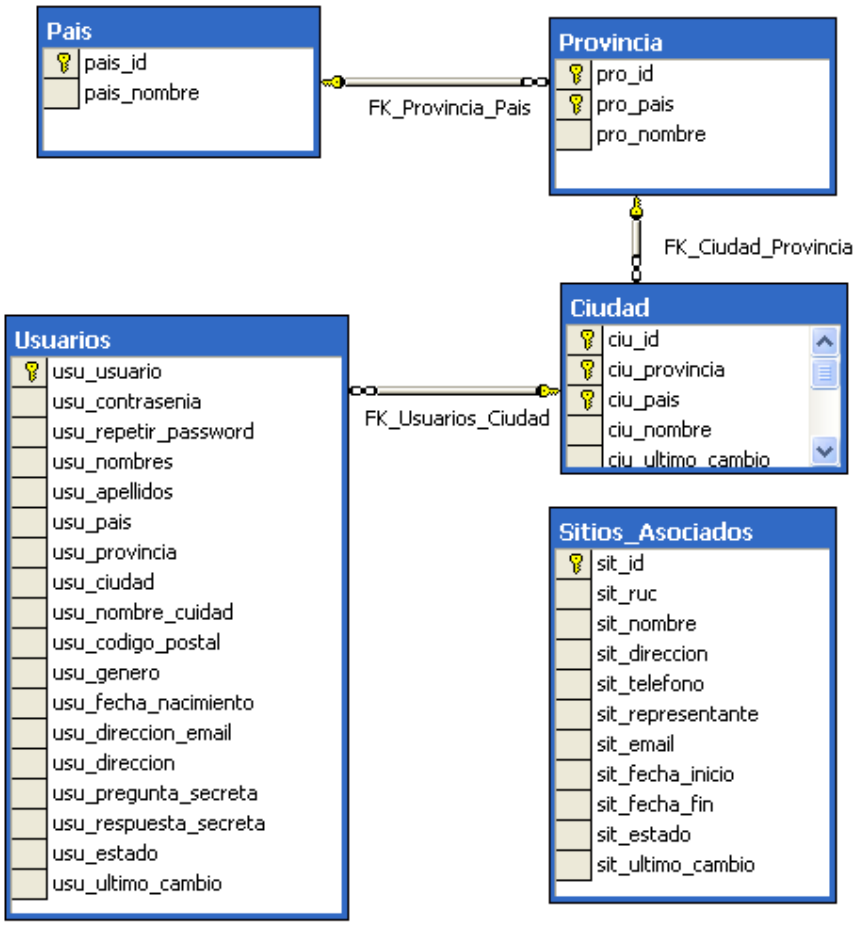


Figura 5: Modelo Entidad-Relación de Administración de Usuario

Presentación de Noticias y Eventos

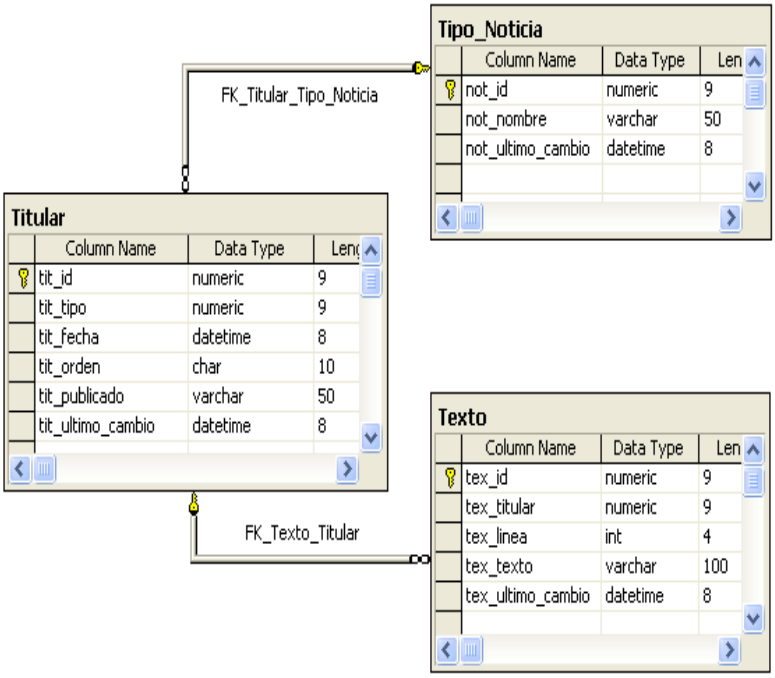


Figura 6: Modelo Entidad-Relación de Noticias y Eventos

3.4.4 Diseño de Arquitectura

Mi pasaporte esta basado en un Web Services que permite la comunicación entre aplicaciones o componentes de aplicaciones de forma estándar a través de protocolos comunes (como http) y de manera independiente al lenguaje de programación, plataforma de implantación, formato de presentación o sistema operativo.

El Web Services Mi pasaporte nos permite la autenticación de clientes a los servicios de Mi Pasaporte de la siguiente forma:

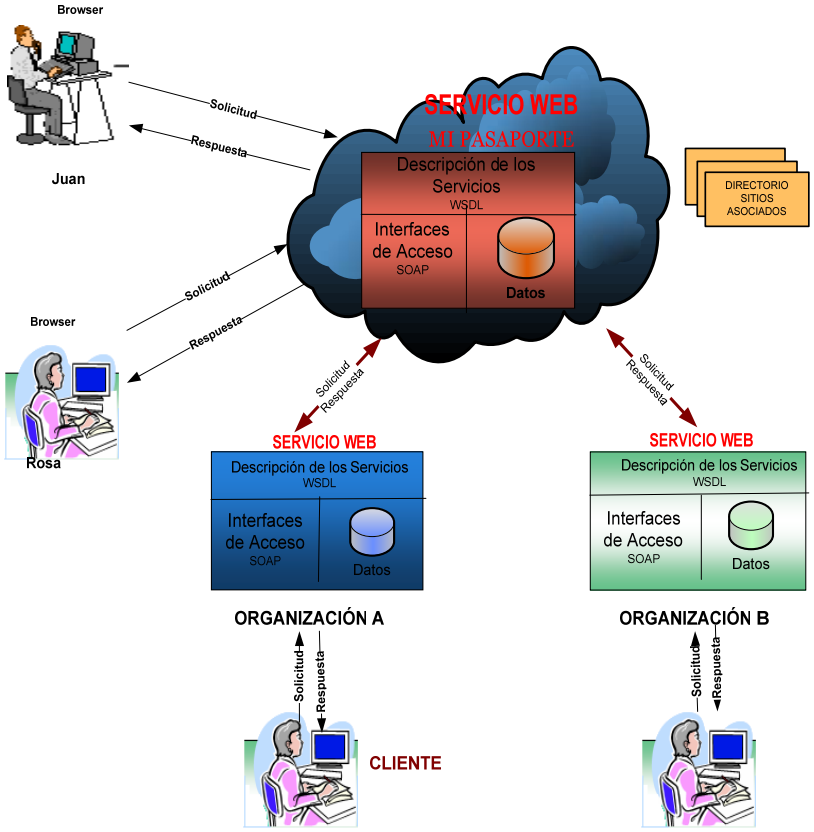


Figura 7: Arquitectura Servicio Web Mi Pasaporte

1. Mediante el browser Mi Pasaporte el cliente ingresa el usuario y contraseña.

2. Preguntamos al Servidor Web Mi Pasaporte si existe el usuario que dice ser.

3. El servidor responde en WSDL (Web Services Definition Language).

4. Hacemos petición del servicio mediante SOAP y pedimos la autenticación del usuario que intenta ingresar a nuestro servicio.

5. Si el cliente es quien dice ser, el servicio Web responde en SOAP en forma afirmativa, de lo contrario se recibirá una respuesta de Error.

6. Si el Servidor Web responde que el usuario es quien dice ser, este localiza la organización asociado mediante el directorio e identifica los servicios que ofrece y una vez elegido alguno este podrá acceder a través del método asociado.

CAPITULO 4

4 Implementación del Proyecto

4.1 Emisión de Cuentas de Usuarios

El servicio de Cuenta Passport solamente recopila la información necesaria para llevar a cabo la autenticación, facilidad de información a sitios colaboradores que lo soliciten manteniendo privacidad de los mismos y mejor la seguridad. Cuando se utiliza este servicio para iniciar sesión en un sitio colaborador,

este registra temporalmente el lugar en el que ha iniciado sesión como parte de su actividad de inicio de sesión. Sin embargo, Mi P@saporte no recopila ningún otro tipo de información acerca de la actividad que realiza mientras está conectado en el sitio colaborador, como, por ejemplo, las páginas Web que visita o los artículos que compra, tanto si ha iniciado la sesión como no.

4.1.1 Ingresando a nuestro Servicio

En el explorador de Windows digite nuestra dirección de página Web e inmediatamente visualizara nuestra portada con información acerca de nuestro servicio. Además cuenta con la opción de Inicio de Sesión en caso de formar parte como usuario. En caso de no estar registrado en nuestra base de usuario, usted debe registrarse en forma gratuita con tan solo ingresar a la opción “Regístrese”, tal como se muestra en la siguiente imagen.

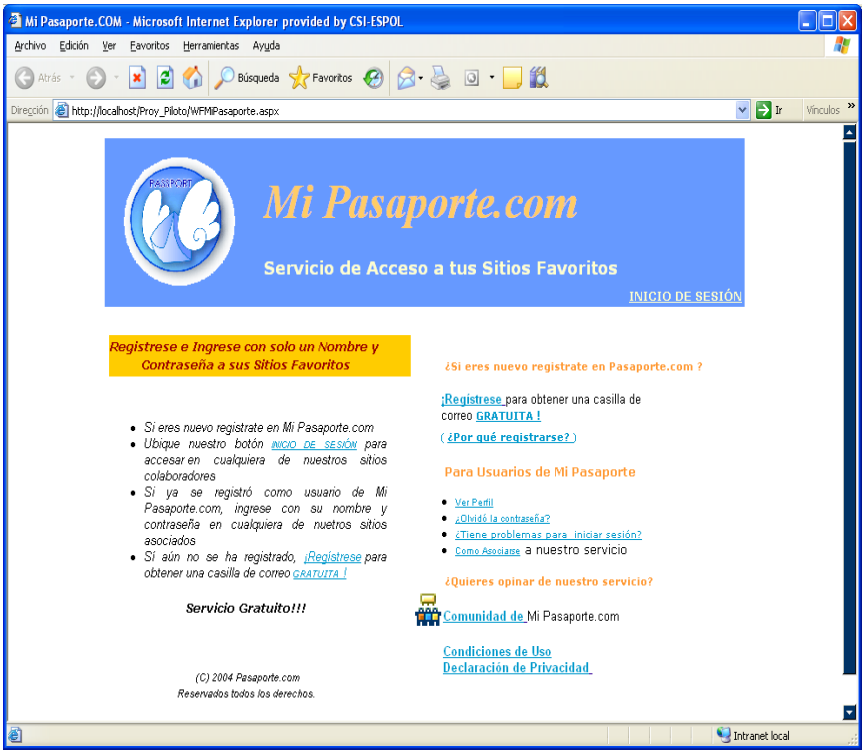


Figura 8: Página principal de Mi Pasaporte

4.1.2 Como obtener una Cuenta Mi P@saporte?

Puede crear una cuenta de inicio de sesión único de 2 forma:

- Registrándose en el sitio Web de Mi P@saporte

- Registrándose en un sitio colaborador de Mi P@saporte que le envía automáticamente a la página de registro de Mi P@saporte.

4.1.3 Como crear una buena contraseña?

Una buena contraseña tiene al menos ocho caracteres, incluye una combinación de letras, números y símbolos y usted no tiene ningún problema para recordarla, pero sí es difícil para los demás adivinarla.

4.1.4 Información que registra Mi P@asaporte

Cuando se registra para obtener una cuenta Passport, se le pedirá que proporcione determinada información personal que se almacenará en el "perfil" de Mi P@saporte. Como se describe a continuación, la cantidad de información solicitada variará en función del

sitio de registro, aunque el perfil de nuestro servicio contiene sólo dos grupos de información requerida:

- **Información del Perfil:** Nombre, apellidos, país o región, ciudad, código postal, género, fecha de cumpleaños, información de cuenta.
- **Información de Cuenta:** Dirección de E-mail, Usuario, password, repetir password, pregunta secreta, respuesta secreta.

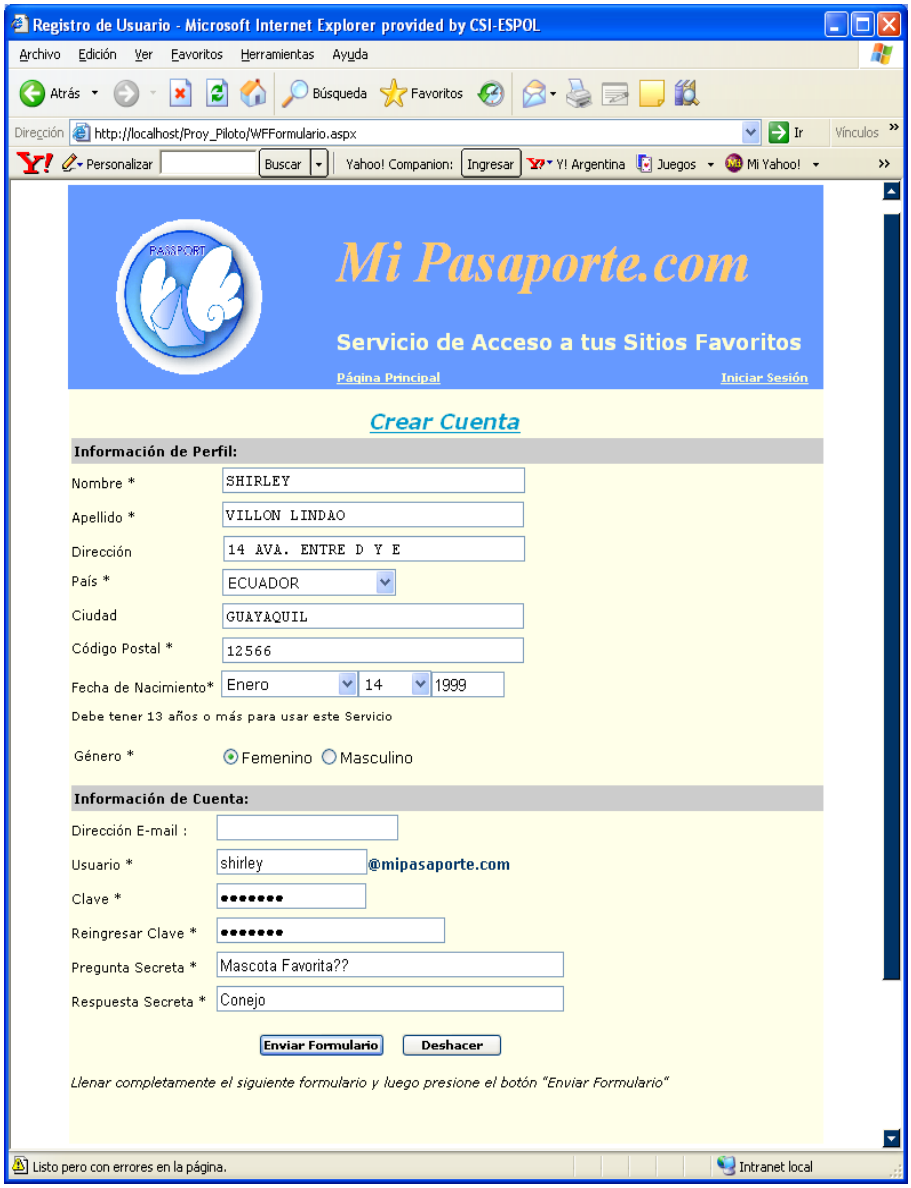


Figura 9: Creación de una Cuenta Passport

Al registrarse para obtener una cuenta de Passport , se le pedirá que cree una contraseña

para su cuenta. Además se le solicitará que proporcione preguntas y respuestas secretas. Estas preguntas y respuestas secretas contribuyen a comprobar su identidad al requerir los servicios de los portales asociados en relación con su cuenta en determinados casos, como por ejemplo, cuando necesite restablecer su contraseña. Por último, algunos sitios pueden precisar un grado de seguridad adicional.

Al registrarse mediante un cuenta Passport , se asocia un identificador único con cada cuenta de Mi P@saporte. El identificador es un número único de 64 bits que la cuenta Passport envía (cifrado) a cada sitio colaborador del servicio Passport en el que inicia sesión. Este identificador único permite que el sitio determine si se trata de la misma persona entre un inicio de sesión y el siguiente.

Mi P@saporte también registra temporalmente inicios de sesión individuales con el propósito de asegurar la eficacia y la seguridad del servicio. La información de estos registros sólo se puede identificar con el número de ID Único de la cuenta y nunca está vinculado a información personal, a no ser que el usuario llame al servicio para solicitar asistencia.

4.2 Inicio de Sesión

El Inicio de Sesión es muy sencillo tal y como pasamos a detallar su uso:

- En el área "¿Ya tienes una casilla de correo?", ingrese sólo un nombre de usuario y una contraseña para iniciar sesión en todos los sitios y servicios colaboradores.
- Busque el botón "Iniciar sesión" en Mi P@saporte y al dar un sólo click nuestro servicio realizara la autenticación para dar permisos de accesos a sus sitios colaboradores.

Figura 10: Inicio de Sesión en Mi P@saporte

4.3 Revocación de Cuentas de Usuarios

Nuestro servicio no posee opción para el cierre de cuentas, pero puede solicitarla poniéndose en contacto con el soporte al cliente de Mi P@saporte. También pueden ser cerradas dejando de usarla por un tiempo. Mi P@saporte está en un "dominio patrocinado" como el descrito anteriormente.

Si intenta registrarse para obtener una cuenta de Mi P@saporte y comprueba que alguien ya ha registrado una cuenta de Mi P@saporte con su dirección de correo electrónico, tiene la opción de ponerse en contacto con soporte al cliente de Mi P@saporte y solicitar que la cuenta de Mi P@saporte que está utilizando su dirección de correo electrónico cambie dicha dirección, con el fin de que poder utilizarla.

Inactividad y eliminación de una cuenta

Nuestro servicio eliminará su cuenta de Mi P@saporte si permanece inactiva durante un periodo prolongado. Se entiende por inactividad la ausencia de uso de inicio de sesión en la cuenta de Mi P@saporte.

Figura 11: Botón Inicio de Sesión de Mip@ssport

Su cuenta Passport se privará de acceso si la cuenta permanece inactiva durante 120 días y, toda la información del perfil o relativa a la cuenta será eliminada.

4.4 Olvido de Contraseñas

En caso de que el cliente olvide su Contraseña el sistema le permite.

Figura 12: Olvido de Contraseña

Si el usuario existe Mi Pasaporte le ayudará a cambiar su contraseña respondiendo la pregunta secreta que ingreso al momento de la apertura de la cuenta Mi Pasaporte, de la siguiente forma:

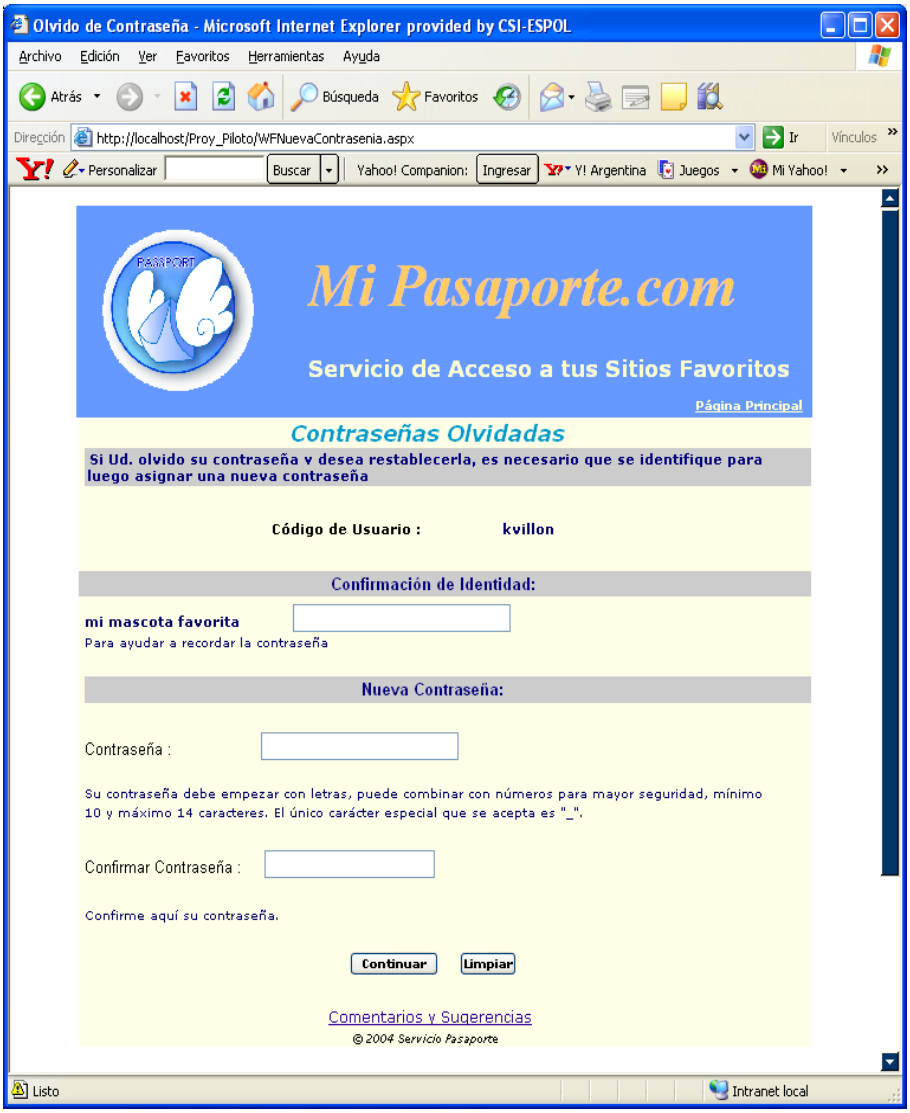


Figura 13: Olvido de Contraseña

En caso de que la nueva contraseña sea aceptada con éxito, Mi Pasaporte le mostrará el mensaje que de transacción exitosa y le permitirá iniciar la sesión con la cuenta creada.

Figura 14: Confirmación de Creación de Cuenta bien registrada

4.5 Renovación de Cuentas de Passport

La aplicación le permite la renovación de cuenta cada 30 días por seguridad de la información. Si el cliente desea la renovación de la cuenta en forma automática, debe indicarlo al momento de Registrar la información requerida por Mi P@saporte. En caso de no indicar esta información Mi P@saporte no realizará la renovación de cuenta en ningún momento, en caso contrario nuestro servicio se encarga de realizar la renovación después de haber transcurrido 30 días y le será indicado al momento de iniciar sesión por primera vez luego de transcurrir el tiempo indicado.

4.6 Configuración de Clientes para validación de Cuentas Mi P@saporte

En un computador se generan archivo al iniciar una sesión, estos archivo son conocidos como cookis del sistema.

Una cookie es un archivo de texto muy pequeño que un sitio Web guarda en el disco duro de su equipo para almacenar la información personal proporcionada o sus preferencias.

Mi P@saporte utiliza cookies cuando inicia sesión en un sitio colaborador. En este archivo se guardan el identificador único, la hora en la que se inició la sesión, cualquier tipo de información del perfil de Mi p@saporte en una cookie cifrada y segura en el disco duro. La cookie permite ir de página en página en el sitio colaborador sin necesidad de iniciar sesión en cada página. Estas cookies se eliminan del equipo cuando se cierra la sesión Mi P@ssport.

Además, Mi P@sporte utiliza cookies para mejorar el inicio de sesión. Por ejemplo, puede almacenar su nombre de usuario en una cookie que permanecerá en el equipo hasta cuando cierre la sesión. Cada sitios y servicios visitados pueden almacenar sus propias cookies en el equipo.

CAPITULO 5

5 Seguridades Adicionales

5.1 Políticas de Seguridad

El servicio de Cuenta Passport se compromete a proteger la seguridad de su información personal. Utilizamos varios procedimientos y tecnologías de seguridad que protegen su información personal, la revelación, el uso y el acceso no autorizados. Por

ejemplo, almacenamos la información personal que nos facilita en sistemas informáticos de acceso limitado, que están ubicados en instalaciones controladas. Al solicitar el envío de la información de Mi P@saporte a un sitio colaborador, éste utiliza tecnologías de seguridad estándar del sector para cifrarla y transmitirla de forma segura por Internet.

Debe escribir la contraseña correcta para tener acceso a la información de .NET Passport . Es su responsabilidad garantizar la seguridad de la contraseña de su cuenta de .NET Passport y no revelar esta información a otros.

La información personal recogida por Mi P@saporte podrá ser almacenada y procesada en cualquier otro país en el que nuestro servicio o sus filiales, subsidiarias y agentes dispongan. Al usar el servicio de Mi P@saporte, otorga su consentimiento para este tipo de transferencia de información fuera de su país. El

servicio se atiene al uso y retención de datos procedentes de nuestros clientes.

USO DE COOKIES

Una cookie es un archivo de texto muy pequeño que un sitio Web guarda en el disco duro de su equipo para almacenar la información personal proporcionada o sus preferencias.

Mi P@saporte utiliza cookies cuando inicia sesión en un sitio colaborador. Este servicio guarda el identificador único, la hora en la que se inició la sesión mediante una cookie cifrada y segura en el disco duro. La cookie permite ir de página en página en el sitio colaborador sin necesidad de iniciar sesión en cada página. Estas cookies se eliminan del equipo cuando se cierra la sesión de Mi P@saporte.

Además, este servicio Passport utiliza cookies para mejorar el inicio de sesión. Por ejemplo, se puede almacenar su nombre de usuario en una cookie que permanecerá en el equipo cuando cierre la sesión. Esta cookie permite que su nombre de usuario se rellene automáticamente, de manera que la próxima vez que inicie sesión, sólo tendrá que escribir la contraseña.

Los sitios y servicios visitados pueden almacenar sus propias cookies en el equipo. .NET Passport le recomienda que se lea la declaración de privacidad de todos los sitios colaboradores para entender las políticas y prácticas relativas a la utilización de cookies. Puede aceptar o rechazar cookies utilizando la configuración del explorador. No obstante, si decide rechazar las cookies, no podrá iniciar la sesión utilizando su .NET Passport .

5.1.1 Administración de Usuarios y Roles

Contraseñas aceptables

Es conveniente que los usuarios elijan claves medianamente resistentes a ataques de diccionario; una contraseña como patata o valencia es un gran agujero de seguridad para la máquina, aunque el usuario que la usa no tenga ningún privilegio especial. Hemos de ver la seguridad como una cadena cuya fuerza depende principalmente del eslabón más débil: si falla éste, falla toda la cadena. Sin embargo, el problema de estas claves es que pueden llegar a ser difíciles de recordar, de forma que mucha gente opta por apuntarlas en el monitor de su estación o en la parte inferior de sus teclados; obviamente, esto es casi peor que el problema inicial, ya que como administradores no podemos controlar estas situaciones la mayor parte de las veces. Podemos (y sería lo

recomendable) recomendar a los usuarios que utilicen combinaciones de mayúsculas, minúsculas, números y símbolos para generar sus claves, pero de forma que la combinación les pueda resultar familiar: por ejemplo, combinar números y letras de la matrícula del coche con algunos símbolos de separación; claves de este estilo podrían ser V#GF&121, @3289?DH o JKnB0322. Obviamente estas claves son más resistentes a un ataque que beatles, pero tampoco son seguras: las acabamos de escribir.

Confidencialidad de las claves

Hemos de concienciar a nuestros usuarios de que las contraseñas no se comparten: no es recomendable 'prestar' su clave a otras personas, ajenas o no al sistema, ni por supuesto utilizar la misma clave para diferentes máquinas. Este último punto

muchas veces se olvida en sistemas de I+D, donde el usuario se ve obligado a utilizar passwords para muchas actividades y tiende invariablemente a usar la misma contraseña; incluso se utiliza la clave de acceso a un equipo Unix para autenticarse en juegos de red (MUDs o IRC) o, lo que es igual de grave, para acceder a equipos Windows, de forma que las vulnerabilidades de seguridad de estos sistemas se trasladan a Unix.

Ejecución de programas

Nunca, bajo ningún concepto, instalar o ejecutar software que no provenga de fuentes fiables; hay que prestar atención especial a programas que nos envíen por correo o por IRC, ya que se puede tratar de programas trampa que, desde borrar todos nuestros ficheros, a enviar por correo una copia del archivo de contraseñas, pueden hacer

cualquier cosa: imaginemos que un 'amigo' nos envía un juego a través de cualquier medio - especialmente IRC - y nosotros lo ejecutamos; incluso disponer del código fuente no es ninguna garantía (>qué usuario medio lee un código en C de, quizás, miles de líneas?). Ese programa puede hacer algo tan simple como rm -rf $HOME/* sin que nosotros nos demos cuenta, con las consecuencias que esta orden implica.

Desconfianza

Hemos de desconfiar de cualquier correo electrónico, llamada telefónica o mensaje de otro tipo que nos indique realizar una determinada actividad en el sistema, especialmente cambiar la clave o ejecutar cierta orden; con frecuencia, un usuario se convierte en cómplice involuntario de un atacante: imaginemos que recibimos una

llamada de alguien que dice ser el administrador del sistema y que nos recomienda cambiar nuestra clave por otra que él nos facilita, con la excusa de comprobar el funcionamiento del nuevo software de correo. Si hacemos esto, esa persona ya tiene nuestra contraseña para acceder ilegalmente a la máquina y hacer allí lo que quiera; hemos de recordar siempre que el administrador no necesita nuestra ayuda para comprobar nada, y si necesita cambiar nuestra clave, lo puede hacer él mismo.

Cualquier actividad sospechosa que detectemos, aunque no nos implique directamente a nosotros, ha de ser notificada al administrador o responsable de seguridad del equipo. Esta notificación, a ser posible, no se ha de realizar por correo electrónico (un

atacante puede eliminar ese mail), sino en persona o por teléfono.

En muchas ocasiones, cuando un usuario nota un comportamiento extraño en el sistema, no notifica nada pensando que el administrador ya se ha enterado del suceso, o por miedo a quedar en ridículo (quizás que lo que nosotros consideramos 'extraño' resulta ser algo completamente normal); esta situación es errónea: si se trata de una falsa alarma, mucho mejor, pero...>y si no lo es?

Respaldos

En este apartado no vamos a hablar de las normas para establecer una política de realización de copias de seguridad correcta, ni tampoco de los mecanismos necesarios para implementarla o las precauciones que hay que

tomar para que todo funcione correctamente; el tema que vamos a tratar en este apartado es la protección física de la información almacenada en backups, esto es, de la protección de los diferentes medios donde residen nuestras copias de seguridad. Hemos de tener siempre presente que si las copias contienen toda nuestra información tenemos que protegerlas igual que protegemos nuestros sistemas.

Un error muy habitual es almacenar los dispositivos de backup en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema: imaginemos simplemente que se produce un incendio de grandes dimensiones y todo el edificio queda reducido a cenizas. En

este caso extremo tendremos que unir al problema de perder todos nuestros equipos - que seguramente cubrirá el seguro, por lo que no se puede considerar una catástrofe - el perder también todos nuestros datos, tanto los almacenados en los discos como los guardados en backups (esto evidentemente no hay seguro que lo cubra). Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de operaciones, aunque en este caso descentralizamos la seguridad y tengamos que proteger el lugar donde almacenamos los backups igual que protegemos la propia sala o los equipos situados en ella, algo que en ocasiones puede resultar caro.

También suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido

(sistemas de ficheros almacenados, día y hora de la realización, sistema al que corresponde...); esto tiene una parte positiva y una negativa. Por un lado, recuperar un fichero es rápido: sólo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada. Sin embargo, si nos paramos a pensar, igual que para un administrador es fácil encontrar el backup deseado también lo es para un intruso que consiga acceso a las cintas, por lo que si el acceso a las mismas no está bien restringido un atacante lo tiene fácil para sustraer una cinta con toda nuestra información; no necesita saltarse nuestro cortafuegos, conseguir una clave del sistema o chantajear a un operador: nosotros mismos le estamos poniendo en bandeja toda nuestros datos. No obstante, ahora nos debemos plantear la duda habitual: si no etiqueto las copias de seguridad, >cómo puedo elegir la que debo restaurar en un momento dado?

Evidentemente, se necesita cierta información en cada cinta para poder clasificarlas, pero esa información nunca debe ser algo que le facilite la tarea a un atacante; por ejemplo, se puede diseñar cierta codificación que sólo conozcan las personas responsables de las copias de seguridad, de forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código sea difícil imaginar su contenido. Aunque en un caso extremo el atacante puede llevarse todos nuestros backups para analizarlos uno a uno, siempre es más difícil disimular una carretilla llena de cintas de 8mm que una pequeña unidad guardada en un bolsillo. Y si aún pensamos que alguien puede sustraer todas las copias, simplemente tenemos que realizar backups cifrados...y controlar más el acceso al lugar donde las guardamos.

5.1.2 Actualización de Software

Es importante mantener la actualización de Softwares a medida que el tiempo transcurra, debido a que frecuentemente se están desarrollando cada vez más tecnologías nuevas para mejorar la eficiencia de los negocios y de las comunicaciones. Al mismo tiempo, las innovaciones tecnológicas ofrecen aún más seguridad a la red, y consecuentemente, más tranquilidad para operar en entornos comerciales de vanguardia. Siempre que las empresas permanezcan a la vanguardia en esta tecnología emergente y se mantengan siempre alertas frente a las amenazas a la seguridad y los peligros, los beneficios de las redes superarán sin duda alguna los riesgos.

5.1.3 Centro de Contingencia

Como herramienta de seguridad es necesario los Centro de Contingencia que serán las

personas quienes dicten los planes de contingencia para la prevención de vulnerabilidad de la información.

Para garantizar la efectividad del operativo el plan de contingencia cuenta con una etapa de preparación donde se prevee realizar fortalecimiento de seguridad para el manejo de información de los clientes.

5.1.4 Seguridad en Sistemas Operativos

Los sistemas de Operativos muchas veces con frecuencia tienen información importante y confidencial de los usuarios. Por lo tanto es muy importante la protección de esa información en contra del uso no autorizado. El Sistema operativo es normalmente solo una porción del total de software que corre en un sistema particular. Como el Sistema Operativo controla el acceso a los recursos del sistema, la

seguridad de los Sistemas Operativos es solo una pequeña parte del problema total de la seguridad en los sistemas de computación, aunque éste viene incrementándose en gran medida. Hay muchas razones para que la seguridad de los Sistemas Operativos reciba especial atención hoy en día.

En el transcurso del tiempo las computadoras se han tornado más accesibles por lo que se tiene un aumento en los riesgos vinculados con la seguridad. Debemos mencionar que a través del tiempo existen ciertos componentes que se van volviendo cada vez más complejos. Ejemplo claro de ello es Internet, la gran red de computadoras, a medida que aumenta su complejidad va tornándose más insegura.

Si tenemos en cuenta que todo software no está libre de fallos, entonces un software

complejo es probable que falle y un porcentaje de estos fallos afecte a la seguridad.

La única manera razonable de probar la seguridad de un sistema es realizar evaluaciones de seguridad en él. Sin embargo, cuanto más complejo es el sistema, más dura se vuelve la evaluación de su seguridad. Un sistema más complejo tendrá más errores relacionados con la seguridad en su análisis, diseño y programación.

CAPITULO 6

6 Conclusiones y Recomendaciones

6.1 Conclusiones

Debido a la importancia que debemos tener presente al acceder a un sitio Web, hemos llegado a la conclusión de que la herramienta puede llegar a brindar un grado de confiabilidad muy alto.

Con Mi P@saporte ofrece facilidad de uso y olvido de contraseñas al intentar un inicio de sesión y sin la necesidad del uso de varias contraseñas. Mi P@saporte

es confiable debido a que brinda privacidad de información a nuestros clientes.

La aplicación desarrollada en entorno Web es fácil en cuanto al manejo debido a que hoy en día existe un sin número de personas que ya están familiarizada con el entorno Web (uso de internet) y al manejo de Cuentas. Mi P@saporte es igual pero con el beneficio que aplica encriptación de la clave del cliente para seguridad de su información.

6.2 Recomendaciones

Con Mi P@saporte.com se puede iniciar sesión en sus sitios colaboradores utilizando su dirección de correo electrónico y una única contraseña para no tener que estar recordando un nombre y una contraseña distinta para cada sitio Web.

Como ya se mencionó anteriormente que con una sola dirección de correo electrónico y una contraseña se

puede ingresar a distintos sitios Web colaboradores, es necesario hacer ciertas recomendaciones al una contraseña:

- No crear contraseñas utilizando una combinación de números o letras consecutivas, o letras adyacentes como "qwerty".
- También se aconseja que utilizar el mismo nombre de usuario, el nombre de personas cercanas o de su cumpleaños como contraseña es algo que nunca debe hacerse.
- Otra cosa que tampoco debe utilizar es palabras que no puedan encontrarse en el diccionario. Los hackers utilizan herramientas sofisticadas para adivinar rápidamente las contraseñas utilizando palabras del diccionario en muchos idiomas, incluso palabras comunes escritas al revés.

- Si usted utiliza una palabra común como contraseña, podría pensar que está protegido si reemplaza las letras de esa palabra con números o símbolos que se

parezcan a las letras que usted pensaría utilizar, como Microsoft o P@ssword. Por desgracia, los hackers también conocen muy bien ese truco

Otros tipos de recomendaciones a tomarse en cuenta después de la creación de una contraseña son:

- **Mantenga en secreto sus contraseñas.** Mantener la seguridad de sus contraseñas significa mantenerlas en secreto. No las proporcione a amigos y no las escriba ni las guarde en su escritorio o en un archivo sin protección en su computadora. Alguien podría entrar en su casa, o quizá alguno de sus hijos podría dejar que algún amigo utilice su computadora o su escritorio, y ese amigo podría no tener las mejores intenciones hablando de su privacidad.

- **Administre sus contraseñas**. Se recomienda que una buena contraseña debe cambiarse cada dos o tres meses. Así como asigna fechas para actualizaciones y limpiezas en su computadora,

debería también asignar fechas periódicas para cambiar sus contraseñas.

- **Monitoree sus cuentas.** En caso de que alguien se robe su contraseña, mientras más rápido lo notifique, menor será el daño que puedan hacer los hackers. Asegúrese de monitorear su cuenta Passport y cuando se de cuenta de cualquier anomalía debe ser notificado inmediatamente para reportar el hecho.

GLOSARIO

CE de Windows 9x.

Nuevo software perteneciente a la familia Microsoft. Windows CE tiene el objetivo de proveer un moderno sistema operativo de plataforma cruzada, multihilado y de tamaño pequeño (cantidad de memoria y de almacenamiento) necesario para albergar al sistema operativo.

Sistemas AIX-Basados.

Sistema hecho por IBM. Plataforma para correcciones suportado para Oracle Database version(s) 8.1.7 (8i) & 8.1.7.x (8i).

Compaq Tru64 UNIX.

El sistema operativo Tru64 producido por HP/Compaq contiene desbordamientos múltiples del almacenador intermediario en bibliotecas de sistema múltiples y binarios. Tru64 ahora se envía con su puesta en práctica de la pila del non-exec permitida por el valor por defecto.

Serie HP-UX.

Hewlett-Packard desarrollo su sistema operativo HP-UX 11i como el sistema operativo UNIX® número 1. Con HP-UX 11i, HP proporciona a los clientes una vía clara y estable hacia el futuro, aportando una completa compatibilidad a nivel binario entre las arquitecturas PA-RISC e Intel® Itanium™. Un amplio número de desarrolladores de software soportan HP-UX, permitiendo a los clientes de HP ejecutar aplicaciones estratégicas que no están disponibles en otros sistemas operativos.

Linux Intel

Servidor estrella fabricado por SUN.

Sol Solaris del HP 9000

Servidores en entorno Sol Solares.

Oracle 9i

Servidor de aplicaciones, red y programación, pues presenta acceso multiusuario para procesamiento y almacenaje de bases de datos de gama alta y en la Web.

Amd.

Nuevo procesador Movile AMD Sempron, para portatiles mas finos y ligeros. AMD pesenta con su tecnología avanzada con el comunicador personal en el internet (PIC).

OLAP proceso analítico en línea

Un sistema OLAP se puede entender como la generalización de un generador de informes. Las aplicaciones informáticas clásicas de consulta, orientadas a la toma de decisiones, deben ser programadas. Atendiendo a las necesidades del usuario, se crea una u otra interfaz.

TPC-C. Plataforma de 32 vías más veloz del mundo. NEX publicó un resultado de benchmark TPC-C que sitúa a Windows Server 2003 y SQL Server 2000 Enterprise Edition a la cabeza de la clasificación de servidores “Online Transaction Processing” (OLTP) de 32 vías más veloces del mundo.

PL/SQL

"Procedural Language/SQL". Es un lenguaje que extiende SQL mediante la incorporación a SQL de construcciones que se encuentran en los lenguajes procedurales, tales como: Variables y tipos, Estructuras de control, Procedimientos y funciones. A través de PL/SQL podemos emplear las estructuras de SQL para manipular datos en ORACLE, y estructuras de flujo para procesar los datos.

T-SQL

Transact-SQL .Procedimiento para generar consulta de insert o update.

VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte

Clustering

Hace referencia al enlace de servidores individuales física y programáticamente y a la coordinación de la comunicación entre ellos, de modo que puedan realizar tareas comunes. Cualquiera de los servidores puede dejar de funcionar, y un proceso denominado de failover automáticamente conmuta la carga de trabajo a otro servidor para proporcionar un servicio continuo.

Offline

Es un status o estado en que se encuentra cualquier acción.

Advanced Server

Añade componentes para soportar aplicaciones críticas. Advanced Server incluye características como equilibrio de carga de red, agrupamiento y un mayor soporte para el multiprocesamiento simétrico.

Datacenter Server

Datacenter Server es un producto especializado de la familia Windows 2000 Server. Datacenter Server está diseñado para proporcionar clientes con soporte hardware y software integrado.

Benchmarks TPC-C

Familia de Servidores Solaris de excelente diseño y avanzada tecnología de la gama PrimePower

Windows 2000 Advanced y Datacenter Server

Familia de Windows. Windows 2000 Advanced Server y Datacenter Server proporcionan tecnologías y servicios de cluster para proporcionar altos niveles de servicio y disponibilidad.

POO

Programación orientada a objetos. La programación orientada a objetos es una evolución de la programación procedural basada en funciones. La POO nos permite agrupar secciones de código con funcionalidades comunes.

Hackers

En general los “hackers” son personas expertas en informática y comunicaciones que intentan penetrar en sistemas informáticos con el fin de obtener información de los mismos, sabotearlos o simplemente (en muchas ocasiones es así) se introducen en estos sistemas por la autosatisfación de mostrar agujeros de seguridad en los mismos. Muchos de ellos, utilizan la red Internet para introducirse en servidores provocando su inutilización o sustituyendo su contenido por otros propios.

WSDL

Web Services Definition Language. Es un documento escrito en XML en el que se describen las operaciones que un servicio ofrece.

SOAP

Simple Object Acess Protocol. Es un lenguaje de mensajera basado en XML, además especifica todas las reglas necesarias para ubicar los servicios Web, y establecer la comunicación

BIBLIOGRAFÍA

1. Digital Document Signing in Java-Based Web Applications

   www.Microsoft® _NET Passport declaración de privacidad.htm.

2. Net Passport

   http://www.Passport

   .net/Consumer/default.asp?lc=3082&lc=3082.

3. Microsoft .Net Passport

   http://www.microsoft.com/latam/net/services/Passport /.

4. Desarrollo Web.com

   http://www.desarrolloweb.com/articulos/1640.php?manual=54

5. Seguridad en servicios web. Autenticación y autorización.

   Interoperabilidad

   http://www.desarrolloweb.com/articulos/1640.php?manual=54

6. Passport .NET se integra a MCP y a sitios seguros de MCT

http://www.microsoft.com/latam/entrenamiento/mcp/mcp/Passport faq.asp

7. Indexo f/es/publicaciones/publicaciones (Comparación de Java VS .Net)
   http://www.icesi.edu.co/es/publicaciones/publicaciones/.

8. SQL Server Worldwide Users Group
   www.mssqlcity.com/Articles/Compare/sql_server_vs_oracle.htm

9. Microsoft
   http://www.microsoft.com/.

10. Security and VPN
    http://www.cisco.com/go/security

11. Seguridad en Sistemas Operativos
    http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGSO200.htm