ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DESARROLLO E IMPLEMENTACIÓN DE UNA INTRANET/ EXTRANET PARA UNA EMPRESA COMERCIALIZADORA DE SOFTWARE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO CON MENCIÓN EN REDES DE INFORMACIÓN

PATRICIA ELIZABETH JÁCOME RAMOS
patty_eliz@yahoo.com
SILVIA PAULINA PAZMIÑO MOYA
Silvia.Pazmino@tcs.ec

DIRECTOR: ING. JUAN HERRERA
Juan.Herrera@leveltch.com.ec

Quito, Septiembre 2007

DECLARACIÓN

Nosotras, Patricia Elizabeth Jácome Ramos y Silvia Paulina Pazmiño Moya, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Patricia Elizabeth Jácome Ramos

Silvia Paulina Pazmiño Moya

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Patricia Elizabeth Jácome Ramos y Silvia Paulina Pazmiño Moya, bajo mi supervisión.

_____

Ing. Juan Herrera

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Nuestros profundos agradecimientos a la Escuela Politécnica Nacional que a través de la Carrera de Ingeniería Informática y por medio de su equipo de profesores nos han formado como profesionales responsables capaces de contribuir al desarrollo del país.

De igual forma hacemos extensivos nuestros agradecimientos al Ingeniero Juan Herrera por su decidida colaboración en la dirección del proyecto. Además de reconocer el apoyo de aquellas instituciones que de alguna manera contribuyeron para hacer posible la realización del mismo.

Un agradecimiento especial dirigimos a nuestros amigos Ibeth, Róbinson y Edison, que con su conocimiento y experiencia nos ayudaron a la consecución del éxito en este propósito.

Patricia Jácome R.
Silvia Pazmiño M.

DEDICATORIA

A nuestros padres, porque con su apoyo incondicional nos han ayudado a culminar este proyecto. Con amor y paciencia nos han alentado para seguir adelante y alcanzar nuestros más grandes sueños y anhelos.

Patricia Jácome R.

Silvia Pazmiño M.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

Las Intranets permiten a una Organización gastar menos tiempo en la búsqueda de información para resolver un problema. La productividad se incrementa a medida que el conocimiento corporativo es más accesible y la información más precisa. Esto lleva a tener empleados mejor informados y con la habilidad de tomar mejores y más rápidas decisiones. Al final, se termina logrando un mayor rendimiento lo que permite incrementar las ganancias en la organización.[1]

Cuando se abre la INTRANET a los clientes o proveedores, se extiende hacia la EXTRANET, es el punto de contacto con el mundo exterior que ofrece la oportunidad de conseguir nuevos clientes y de aumentar la capacidad de servicio a los actuales.

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

Desarrollar e implementar una Intranet / Extranet en una Empresa Comercializadora de Software.

1.1.2 OBJETIVOS ESPECÍFICOS

- Determinar la situación actual de la empresa, en cuanto se refiere a operatividad y procesos que realiza.
- Definir los requerimientos de la Intranet / Extranet.
- Realizar el análisis costo/ beneficio de la solución propuesta.
- Desarrollar e implementar la Intranet / Extranet.
- Definir las políticas de seguridades de la Intranet / Extranet.

1.2 ALCANCE

1.2.1 ANÁLISIS

El proyecto comienza determinando la situación actual de la empresa, en función de estos resultados se definirán los requerimientos en cuanto a su organización desde el punto de vista de los procesos identificados, luego se realizará un estudio de las herramientas de desarrollo con el fin de seleccionar las opciones más adecuadas a los requerimientos y posibilidades de adquisición de la empresa; posteriormente se obtendrá un Análisis Costo / Beneficio de la solución a plantearse.

1.2.2 DISEÑO E IMPLEMENTACIÓN

En la fase de diseño se especificará el diseño lógico y físico que tendrá la Intranet / Extranet. Después se implementará el sistema con los servicios que podrán disponer tanto usuarios internos como externos. Se permitirá la publicación de la información, en la Intranet referente a: Operación y Administración, Recursos Humanos, Capacitación en la Empresa, Difusión y Comunicación; y en la Extranet brindar a los clientes información en línea relacionada con los productos que ofrece la empresa, solicitudes de pedidos de compra y solicitudes de empleo para la selección de personal de la empresa. Finalmente se definirán las políticas de seguridades de la Intranet / Extranet.

1.3 JUSTIFICACIÓN DEL PROYECTO

La empresa en la cual se realizará el diseño de la Intranet / Extranet presenta un alto grado de problemas en el flujo de información interno, mantiene un esquema de red inapropiado que solo permite compartir archivos, además existe una subutilización de los recursos tanto en hardware como en software y no dispone de un medio adecuado de promoción de sus productos y servicios. Se justifica el desarrollo y la implementación del presente proyecto, porque propone una solución eficaz a los inconvenientes descritos anteriormente, que permitirá mejorar los procesos internos y externos de comunicación empresarial, aumentando la accesibilidad a la información tanto al empleado como cliente de

forma inmediata y segura. Actualmente se tienen a disposición herramientas y tecnologías para la implementación de Intranets / Extranets, las cuales han sido ampliamente difundidas y probadas, que ofrecen además un alto índice de rendimiento y gran variedad de aplicaciones, como por ejemplo permitir filtrar y transmitir información confiable utilizando Internet, lo cual abarata los costos de comunicación.

CAPÍTULO 2

FUNDAMENTOS

2.1 INTRANETS/EXTRANETS

2.1.1 INTRANET

Intranet es una infraestructura basada en los estándares y tecnologías de Internet (TCP/IP) que soporta el compartir información mediante la posibilidad de integración con las bases de datos internas de la organización dentro de un grupo bien definido y limitado de usuarios.[2]

Las Intranets están basadas en la arquitectura cliente / servidor. El software cliente es un navegador Web, se ejecuta en una computadora local, y el software servidor está en una Intranet anfitriona. El software cliente y el software servidor no necesitan ejecutarse en el mismo sistema operativo. [3]

Los principales beneficios son:

- Las Intranets son escalables y flexibles porque permite la conexión entre distintas plataformas.
- Hacen más eficientes los procesos de negocios debido a que concentran la información dispersa de la compañía, poniéndola a disposición de todos los individuos de la empresa mejorando los procesos de toma de decisiones, esto ahorra tiempo y dinero.
- Permiten hacer transacciones seguras de actividades entre los sistemas internos de los negocios.
- El acceso a la información es mucho mas fácil, directo y coloquial que con los instrumentos tradicionales, que se traduce en obtención rápida de respuestas.
- El ambiente Web permite al usuario facilidad en el uso de la aplicación, contribuyendo al incremento de la productividad.
- Facilitan la actualización de datos de forma inmediata y automática.
- Mejora el servicio a los clientes e incrementa la potencialidad de nuevos clientes.

2.1.2 EXTRANET

Extranet es una red privada dentro de una organización que utiliza tecnología muy similar a la de Internet pero tiene acceso limitado, esta disponible únicamente a usuarios específicos, tales como clientes, proveedores y socios estratégicos. Esto se realiza por medio de un sistema Web. Entre las ventajas y beneficios que se adquieren al implementar una Extranet se encuentran los siguientes:

- Disponibilidad de contar con un medio permanente las 24 horas del día los 365 días del año para promocionar productos o servicios, distribución de: catálogos, listados y descripciones de productos o servicios, listas de precios, etc.
- Ofrece la oportunidad de ampliar la zona de promoción y conseguir nuevos clientes y de aumentar la capacidad de servicio a los actuales en forma personalizada.
- Capacidad de lanzar ofertas y promociones, así como anuncios y comunicados a clientes interesados directamente en su producto o servicio.

2.2 METODOLOGÍA DE DESARROLLO DE INTRANETS/ EXTRANETS

Aunque los propósitos de las Intranets / Extranets son generales, ninguna es realmente típica. Las personas utilizan la tecnología para diferentes fines. Hay tantas aplicaciones de Intranets / Extranets como tipos de organizaciones y tipos de negocios existen. Lo importante es ver de qué forma se puede potencializar su uso dentro de la empresa.

El desarrollo e implementación de una Intranet / Extranet, tiene analogías con el proceso de construir un sistema informático, por lo tanto se considerarán los fundamentos de Metodologías para el Desarrollo de Software como la guía para la elaboración del proyecto propuesto.

“Una metodología de ingeniería del software es un proceso para producir software de forma organizada, empleando una colección de técnicas y convenciones de notación predefinidas” [4]

En este caso se ha escogido el Análisis Orientado a Objetos (AOO) como la metodología para modelar el sistema en sus etapas de análisis y diseño.

La técnica seleccionada es UML debido a que es un lenguaje gráfico que permite la estandarización de los objetos diseñados y que incluye aspectos conceptuales tales como procesos de negocios y funciones del sistema.

2.2.1 ANÁLISIS ORIENTADO A OBJETOS (AOO)

La esencia del desarrollo orientado a objetos es la identificación y organización de conceptos del dominio de la aplicación, y el objetivo del análisis orientado a objetos es desarrollar una serie de modelos que describan el software de computadora que al trabajar puedan satisfacer un conjunto de requisitos definidos por el cliente.

La popularidad de las tecnologías de objetos ha generado docenas de métodos de AOO desde finales de los 80’s y durante los 90’s. Cada uno de ellos introduce un proceso para el análisis de un producto o sistema. Entre los más ampliamente utilizados se encuentran:

- El método de Booch
- El método de Rumbaugh
- El método de Jacobson

La estandarización de los métodos utilizados anteriormente da como resultado el Lenguaje Unificado de Modelado (UML) que es una recopilación de las mejores características de modelado en un solo método.[5]

2.2.2 VISIÓN GENERAL DE UML

UML es un lenguaje para: visualizar, especificar, construir y documentar los artefactos de un sistema con gran cantidad de software, proporciona un vocabulario y las reglas para combinar palabras de ese vocabulario con el objetivo de posibilitar la comunicación. Un lenguaje de modelado es un lenguaje cuyo vocabulario y las reglas se centran en la representación conceptual y física de un sistema. El lenguaje de modelado UML es por tanto un lenguaje estándar para diseñar los planos del software.[6]

Considerando como artefacto la información que es utilizada o producida mediante un proceso de desarrollo de software.

Para comprender UML se necesita adquirir un modelo conceptual del lenguaje, y esto requiere aprender tres elementos principales: los bloques básicos de construcción de UML, las reglas que dictan como se pueden combinar estos bloques básicos y algunos mecanismos comunes que se aplican a través de UML. Una vez comprendidas estas ideas, se puede leer modelos UML y crear algunos modelos básicos.[7]

2.2.3 CAPTURA DE REQUISITOS COMO CASOS DE USO

El modelo de casos de uso permite que los desarrolladores de software y los clientes lleguen a un acuerdo sobre los requisitos, es decir, sobre las condiciones y posibilidades que debe cumplir el sistema. El modelo de casos de uso sirve como acuerdo entre los clientes y desarrolladores, y proporciona la entrada fundamental para el análisis, el diseño y las pruebas. Un modelo de casos de uso es un modelo del sistema que contiene actores, casos de uso y sus relaciones.

Actores.- El modelo de casos de uso describe lo que hace el sistema para cada tipo de usuario. Cada uno de estos se representa mediante uno o mas actores. Una vez que hemos identificado todos los actores del sistema, tenemos identificado el entorno externo del sistema.

Casos de Uso.- Los casos de uso son gráficos de funcionalidad que el sistema ofrece para aportar un resultado de valor para sus actores, un caso de uso especifica una secuencia de acciones que el sistema puede llevar a cabo interactuando con sus actores.

Relaciones.- Representa la interacción entre los objetos.[8]

2.2.4 ANÁLISIS

El lenguaje que utilizamos en el análisis se basa en el modelo de objetos conceptual, que es llamado modelo de análisis. El modelo de análisis nos ayuda a refinar los requisitos y nos permite razonar sobre los aspectos internos del sistema. El modelo de análisis también nos ayuda a estructurar los requisitos y nos proporciona una estructura centrada en el mantenimiento, en aspectos tales como la flexibilidad ante los cambios y la reutilización.

2.2.4.1 Modelo de Análisis

El modelo de análisis se representa mediante un sistema de análisis que denota el paquete de más alto nivel del modelo, las clases utilizadas en este modelo representan abstracciones de subsistemas y posiblemente capas completas del diseño del sistema. Dentro de este modelo, los casos de uso se describen mediante clases de análisis y sus objetos, y esto se representa mediante colaboraciones que se denominan realizaciones de caso de uso-análisis. Las clases utilizadas se describen a continuación:

Clases de Interfaz.- Se utilizan para modelar la interacción entre el sistema y sus actores. Esta interacción a menudo implica recibir información y peticiones de los usuarios y los sistemas externos.

Clases de Entidad.- Se utilizan para modelar información que posee una larga vida y que es a menudo persistente. Las clases de entidad modelan la información y el comportamiento asociado de algún fenómeno o concepto, como una persona, un objeto del mundo real, o un suceso del mundo real.

Clases de Control.- Representan coordinación, secuencia, transacciones, y control de otros objetos y se usan con frecuencia para encapsular el control de un caso de uso en concreto. Las clases de control también se utilizan para representar derivaciones y cálculos complejos, como la lógica del negocio, que no puede asociarse con ninguna información concreta, de larga duración, almacenada por el sistema.

Diagramas de Colaboración.- En los diagramas de colaboración se muestra la interacción entre objetos creando enlaces entre ellos y añadiendo mensajes a esos enlaces. El nombre de un mensaje debería denotar el propósito del objeto invocante en la interacción con el objeto invocado. [9]

2.2.5 DISEÑO

En el diseño se modela el sistema y se encuentra su forma para que soporte todos los requisitos incluyendo los requisitos no funcionales y otras restricciones que se le suponen. Una entrada esencial en el diseño es el resultado del análisis, esto es, el modelo de análisis. El modelo de análisis proporciona una comprensión detallada de los requisitos. Y lo que es más importante, impone una estructura del sistema que se debe conservar lo más fielmente posible cuando se de forma al sistema.[10]

2.2.5.1 Realización de Caso de Uso-Diseño

Una realización de caso de uso – diseño es una colaboración en el modelo de diseño que describe como se realiza un caso de uso específico, o como se ejecuta, en términos de clases de diseño y sus objetos. Una realización de caso de uso – diseño proporciona una traza directa a una realización de caso de uso – análisis. Una realización de caso de uso – diseño proporciona una realización física del caso uso_ análisis para la que es trazado, y también gestiona muchos requisitos no funcionales capturados del caso de uso- análisis. Por consiguiente, una realización de caso de uso – diseño puede, como pueden las clases diseñadas, posponer el manejo de algunos requisitos hasta las subsiguientes actividades de implementación anotándolas como requisitos de implementación en la realización.

2.2.5.2 Diagramas de Colaboración

En el análisis se prefiere mostrar diagramas de colaboración. Ya que el objetivo fundamental es identificar requisitos y responsabilidades sobre los objetos, y no identificar secuencias de interacción detalladas y ordenadas cronológicamente (para eso se utilizarán en cambio diagramas de secuencia).

En los diagramas de colaboración se muestran las interacciones entre los objetos creando enlaces entre ellos y añadiendo mensajes a esos enlaces. El nombre de un mensaje debe denotar el propósito del objeto invocante en la interacción con el objeto invocado. [11]

2.2.5.3 Diagramas de Secuencia

Para crear un diagrama de secuencia se debe comenzar por el principio del flujo del caso de uso y después seguir ese flujo paso a paso, decidiendo que objetos del diseño y en que interacciones de instancias de actores son necesarias para realizar cada paso. En la mayoría de los casos los objetos se ajustan de manera natural a la secuencia de interacciones de la realización de caso de uso. Se debe observar lo siguiente sobre los diagramas de secuencia:

- El causante de la invocación del caso de uso es un mensaje de una instancia, de un actor hacia un objeto del diseño.
- Cada clase del diseño identificada en el paso anterior debe tener al menos un objeto del diseño participante en el diagrama de secuencia.
- Los mensajes que realiza el caso de uso se envían entre líneas de vida de los objetos.
- La secuencia en el diagrama es la principal preocupación, ya que la realización de caso de uso – diseño, es la entrada principal para la implementación del caso de uso.
- Se utilizarán etiquetas y el flujo de sucesos – diseño para completar los diagramas de secuencia.
- El diagrama de secuencia debe tratar todas las relaciones del caso de uso que realiza. [12]

2.3 SEGURIDADES EN INTRANETS/EXTRANETS

La seguridad informática comprende un conjunto de mecanismos confiables que garanticen estos principios:

- *Confidencialidad*.- Garantizar que los datos no sean comunicados incorrectamente, es decir que lleguen al destinatario final deseado, y que en caso de ser interceptados, no se pueda conocer el mensaje.
- Integridad.- Proteger los datos para evitar cambios no autorizados.
- *Disponibilidad*.- Garantizar que los recursos estén disponibles cuando se necesiten.
- *Autenticación*.- Confianza en la identidad de usuarios.
- *No repudio*.- Que el destinatario de la información no pueda negar el haberlos recibido.
- Verificación.- Comprobar que los mecanismos de seguridad estén correctamente implementados

La seguridad también implica el establecimiento de procedimientos y políticas de protección ante incidentes, malos manejos, desastres naturales para lo cual se necesita tener planes de: backups, control de configuración, control de medios (cintas magnéticas, discos, etc.). Recuperación ante desastres y planes de contingencia.

El grado de seguridad que se considera adecuado para una empresa está en función del valor de la información que debe protegerse, las amenazas a las que está sujeta esta información y la exposición a riesgos que la compañía está dispuesta a aceptar. Además se debe considerar los costos de hardware, software, red, mantenimiento y educación adicionales, así como costos de procesamiento en los equipos.

2.3.1 CONFIDENCIALIDAD

Confidencialidad es la propiedad de seguridad de un objeto que evita que su existencia se conozca y/o que su contenido se sepa, por lo tanto la información no se proporcionará o revelará a individuos, entidades o procesos no autorizados.

Este término se utiliza con más frecuencia junto con la criptografía, que se utiliza para proteger la información que se transmite entre los nodos de una red. La información cifrada se ha codificado de manera que no se pueda comprender fácilmente en caso de ser interceptada. La confidencialidad, en su sentido más amplio, extiende la filosofía de control de acceso y de esta manera evita la revelación no sólo de los datos propiamente dichos, sino también de la identidad de la operación que un usuario está llevando a cabo.

2.3.2 INTEGRIDAD

La integridad es el estado que existe cuando los datos informáticos son los mismos que los datos de los documentos fuente y no se han alterado o destruido accidental o intencionadamente. Los servicios de integridad aseguran que un problema no existe ya que comprueban que el contenido de un mensaje no se ha modificado y que, en caso de que se transfiera una secuencia de mensajes, ésta se ha conservado. Esto es especialmente importante cuando los datos se transmiten a través de la red y no pueden protegerse con ninguno de los servicios de seguridad del sistema operativo. La integridad se consigue combinando criptografía, funciones hash y firmas digitales.

2.3.3 DISPONIBILIDAD

La disponibilidad de los datos es parte primordial de la seguridad, no es necesario preocuparse de la integridad de los datos si no se puede tener acceso a éstos. A continuación algunos factores que influyen en la disponibilidad de los datos y pueden agruparse en las siguientes categorías:

- Seguridad física
- Redundancia

- Reparación de emergencia

2.3.3.1 Seguridad Física

Todos los equipos informáticos deben permanecer en un lugar seguro, tomando en cuenta la temperatura y la humedad del ambiente. No se debe tener los servidores o equipos que manejen información importante a la vista pública, ya que para el caso de ser robados no se necesita ningún conocimiento informático para sustraerlos o dañarlos.

2.3.3.2 Redundancia

Tolerancia a errores, consiste en suministrar componentes duplicados que permitan la disponibilidad de un sistema incluso aunque uno o más de esos componentes no funcionen correctamente. En particular se clona los dispositivos de hardware, por ejemplo los discos duros, fuentes, procesadores, etc. De manera similar pueden redundarse sistemas de archivos a nivel de software.

2.3.3.3 Reparación de Emergencia

Se los considera una extensión de la filosofía de redundancia. Si un intruso ha sido capaz de dañar los datos de un entorno, los procedimientos de reparación de emergencia deben poder devolver el sistema a su estado de última configuración válida con una pérdida mínima de datos.

2.3.4 AUTENTICACIÓN

Autenticación es el proceso de obtener las credenciales de identificación de un usuario, como nombre y una contraseña, y validar esas credenciales consultando a alguna autoridad como una base de datos. Si las credenciales son válidas, la entidad que las ha presentado se considera una identidad autenticada. Un proceso adjunto es la autorización que es el proceso que determina si la identidad tiene acceso a un recurso específico. La autenticación se consigue mediante el uso de los certificados y firmas digitales.

2.3.5 NO REPUDIO

Denegación por parte de una de las entidades involucradas en una comunicación de su participación en la totalidad o en parte de la comunicación.

Este concepto hace referencia a un mecanismo utilizado para demostrar la identidad del remitente de un mensaje específico. Es una extensión de la autenticación, pero se utiliza generalmente para fines legales. Un ejemplo sería una aplicación de comercio electrónico cuyo mecanismo utilizó un destinatario para probar ante terceros (juez o jurado) que la negación de un remitente acerca del envío de un mensaje era falsa. El no repudio se consigue mediante los certificados y la firma digital.

Existen cuatro situaciones principales en las que se da el sin rechazo:

1. Prueba de remitente (origen). Protege al destinatario en caso de que el remitente niegue que ese usuario envió los datos.
2. Prueba de envío. Protege al remitente de las dudas suscitadas por otra persona acerca de si el remitente envió o no los datos.
3. Prueba de entrega. Protege al remitente o al proveedor de servicios de las dudas suscitadas por otra persona acerca de si los datos se enviaron o no a su destino correcto.
4. Prueba de recepción. Protege al remitente ante la negación del destinatario acerca de la recepción de los datos.

2.3.6 TIPOS DE ATAQUES

2.3.6.1 Ataques Malintencionados

Se refieren a actos encubiertos por personas que desean dañar el sistema o impedir que otros usuarios lo utilicen. A continuación se muestran algunos ejemplos:

- **Los ataques de denegación de servicio (DOS)** causan un impacto negativo en el tiempo de respuesta de un sistema o lo bloquean completamente.

- **Los ataques de piratas informáticos**. pueden intentar descifrar contraseñas o cambiar el contenido de un mensaje durante su transmisión. El motivo suele ser simplemente demostrar que son capaces de superar una barrera de código que pretendía ser indestructible y parte del desafío reside en su anonimato.
- **Los ataques por beneficio personal**. En este caso, los agresores intentan penetrar en las redes con el fin de robar o cambiar datos. Por ejemplo personas que intentan obtener acceso a los números de tarjetas de crédito, que buscan información acerca de los planes o productos de la competencia y desvían las transferencias de fondos electrónicos a otras cuentas.
- **Software Malicioso**
  - **Los virus**. un virus informático es un fragmento de código que se duplica automáticamente y se adjunta a otro fragmento de código. El virus busca entre los archivos internos o de los clientes, programas ejecutables no infectados para los que el cliente o el usuario tienen privilegios de escritura de seguridad. El virus infecta el archivo al insertar código en el archivo de programa seleccionado. Cuando se ejecuta un programa infectado con un virus, éste asume inmediatamente el control para buscar e infectar otros programas y archivos.
  - **Caballos de Troya**: los caballos de Troya son códigos ocultos en un programa, como un juego o una hoja de cálculo, que parece inofensivo durante su ejecución pero tiene efectos colaterales ocultos. Cuando se ejecuta el programa, parece funcionar como espera el usuario, pero en realidad destruye, daña o altera información en segundo plano. Es un programa por sí mismo y no necesita ningún programa huésped en el que incrustarse
  - **Gusanos**: Es un programa autocontenido e independiente que es diseñado generalmente para propagarse o reproducirse por si mismo dentro de sistemas infectados y busca los mecanismos para atacar otros sistemas. La diferencia entre un virus y un gusano es que el virus no es un programa independiente. Sin embargo existen

muchas nuevas versiones en que pierde la diferencia entre gusano y virus.

3.1.1.1 Ataques no Intencionados

Se refiere a usuarios que accidentalmente elimina archivos importantes del sistema operativo es el tipo de individuo que realiza ataques no intencionados, por ejemplo, que cada administrador tenga como mínimo dos cuentas y sólo use la cuenta administrativa con dispositivos de mayor seguridad para ejecutar tareas administrativas con el fin de prevenir accidentes

2.3.7 ENCRIPTACIÓN

Proteger información es un proceso que debe realizarse con algoritmos probados e implementados de la forma en que fueron concebidos. Los algoritmos de encriptación se dividen en simétricos y asimétricos.

2.3.7.1 Encriptación Simétrica

Se usa para almacenar información crítica que deberá poder descifrarse, y un único usuario hará todo el proceso. Nadie más tendrá acceso a la llave con que se encriptará y desencriptará la información. Dentro de los algoritmos de encriptación simétrica podemos encontrar los siguientes, algunos más seguros que otros:

- DES (Digital Encryption Standard): Utiliza una llave de 56 bits. 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.
- 3DES (Three DES o Triple DES): Este funciona aplicando tres veces el proceso con tres llaves diferentes de 56 bits. La importancia de esto es que si alguien puede descifrar una llave, es casi imposible poder descifrar las tres y utilizarlas en el orden adecuado. Hoy en día es uno de los algoritmos simétricos más seguros.

- 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.
- AES (Advanced Encryption Standard): este algoritmo, también conocido como Rijndael. Aun no es un estándar, pero es de amplia aceptación a nivel mundial. Junto a 3DES es de los más seguros. Este último se utiliza cuando hay necesidad de compatibilidad. AES 128 es aproximadamente 15% más rápido que DES, y AES 256 sigue siendo más rápido que DES.

Cualquiera de estos algoritmos utiliza los siguientes dos elementos. Ninguno de los dos debe pasarse por alto ni subestimar su importancia:

IV (Vector de inicialización): Esta cadena se utiliza para empezar cada proceso de encriptación. Un error común es utilizar la misma cadena de inicialización en todas las encriptaciones. En ese caso, el resultado de las encriptaciones es similar, pudiendo ahorrarle mucho trabajo a un hacker en el desciframiento de los datos. Tiene 16 bytes de largo.

Key (llave): Esta es la principal información para encriptar y desencriptar en los algoritmos simétricos. Toda la seguridad del sistema depende de donde este esta llave, como esté compuesta y quien tiene acceso. El largo de las llaves depende del algoritmo. La llave de encriptación es una serie de caracteres, de determinado largo, que se utiliza para encriptar y desencriptar la información que se quiere proteger. Existen llaves privadas y públicas.

Para obtener la llave del algoritmo, dado que una cadena de caracteres generada por un humano en un formulario es considerada poco variada debido a que los caracteres utilizados son pocos (a->z, A->Z, 0->9), se le aplica un proceso de variación con la clase PasswordDeriveBytes y se le pide un resultado de 32 bytes.

Esto nos retorna una llave con caracteres variados, ideal para la encriptación. PasswordDeriveBytes utiliza Hash para generar la salida.

El IV cumple un rol pequeño, pero muy importante. El único motivo por el cual existe es para apoyar el proceso de encriptación, permitiendo exactamente que ocurra la variación del resultado del proceso de encriptación. El IV no debe considerarse como una segunda llave, por que no lo es. Es una ayuda y por lo mismo, no es un dato que haya que esconder, si no que basta con almacenarlo para que cuando se vaya a desencriptar se utilice el mismo IV que se utilizó en la encriptación. En el ejemplo, el IV se retorna como parte del resultado de la encriptación y se genera cada vez que se realiza un encriptación. Su largo es de 16 bytes para el algoritmo de Rijndael.

Es importante considerar que en los algoritmos simétricos se utiliza la misma llave para encriptar y desencriptar. En los algoritmos asimétricos se verá que existen dos llaves, una pública para encriptar y una privada para desencriptar.[13]

2.3.7.2 Encriptación Asimétrica

La encriptación asimétrica permite que dos personas puedan enviarse información encriptada, sin necesidad de compartir la llave de encriptación. Se utiliza una llave pública para encriptar el texto y una llave privada para desencriptar. A pesar de que puede sonar extraño que se encripte con la llave pública y desencripte con la privada, el motivo para hacerlo es el siguiente: si alguien necesita que le envíen la información encriptada, deja disponible la llave pública para que quienes le desean enviar algo lo encripten. Nadie puede desencriptar algo con la misma llave pública. El único que puede desencriptar es quien posea la llave privada, quien justamente es el que recibe la información encriptada.

Los algoritmos de encriptación asimétrica más conocidos son:

- RSA (Rivest, Shamir, Adleman)
  Creado en 1978, hoy es el algoritmo de mayor uso en encriptación asimétrica. Tiene dificultades para encriptar grandes volúmenes de

información, por lo que es usado por lo general en conjunto con algoritmos simétricos.

- Diffie-Hellman (& Merkle)
  No es precisamente un algoritmo de encriptación sino un algoritmo para generar llaves públicas y privadas en ambientes inseguros.
- ECC (Elliptical Curve Cryptography)
  Es un algoritmo que se utiliza poco, pero tiene importancia cuando es necesario encriptar grandes volúmenes de información.
- Mientras más larga sea la llave, más seguro será. La relación con los algoritmos simétricos no es directa. En este caso, una llave de 1024 bits de RSA es equivalente en seguridad a una de 75 bits de un algoritmo simétrico. [14]

2.3.7.3 Encriptación Asimétrica + Simétrica

Debido a que la encriptación asimétrica es casi 1000 veces más lenta que la simétrica, cuando la información a encriptar es mucha, se utiliza una combinación de algoritmos. El algoritmo simétrico se utiliza para encriptar la información y el asimétrico para encriptar la llave del algoritmo simétrico con que se encriptó la información. Entonces, el proceso es mucho más rápido. Esta técnica se utiliza hoy en **SSL** en la negociación entre el navegador del cliente y el servidor. En cada ida y vuelta al servidor se generan nuevas llaves y se realiza todo el proceso. También es utilizada por Windows en la encriptación de los archivos.

Otro motivo para utilizar esta encriptación combinada es la necesidad de encriptar textos largos. La encriptación asimétrica además de ser ineficiente en tiempo, tiene limitaciones de tamaño. El tamaño máximo depende del largo de la llave. Estas limitantes nos obligan a utilizar el método combinado. [15]

2.3.7.4 Hash de Información

Se emplea cuando se necesita almacenar o enviar información crítica de forma segura, pero que no requerirá ser desencriptada para su validación, o que es

extremadamente importante verificar que no haya sido modificada en el camino. Es en esencia un algoritmo.[16]

2.3.8 FIREWALLS

Son un tipo de seguridad muy efectiva en redes. Intentan prevenir los ataques de usuarios externos a la red interna. Tienen múltiples propósitos:

- Restringir la entrada a usuarios.
- Prevenir los ataques.
- Restringir los permisos de los usuarios a puntos bien controlados.

Un firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accedidos dentro de ésta por los que están fuera, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

EL firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración, desafortunadamente, este sistema no pude ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Un firewall es vulnerable, él no protege de la gente que esta dentro de la red interna, éste trabaja mejor si se complementa con una defensa interna.

- Perímetro en defensa
- Firewalls Personales

Se lo puede considerar como un método más protección de la red, separándola de otra red en la cual no se confía; puede ser descrito como un par de mecanismos: uno que existe para bloquear el tráfico, y otro que existe para permitirlo.

2.3.9 VPN’S

La intranet es esencialmente una red restringida, pero ante la necesidad de que usuarios remotos se conecten a la red interna con total seguridad, se recurre a las VPN´s, que son una red privada que se extiende, mediante un proceso de encapsulación y encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte (Internet).

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública, entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte. Todo esto es implementado por medio de los firewalls y los sistemas operativos tanto del servidor como de los clientes.

Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el Point-to-Point Protocol, también conocido como PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN), que permite la creación de un túnel virtual que garantiza la confidencialidad e integridad de los datos transmitidos.

La principal solución utilizada hasta el momento es el establecimiento de Redes Privadas Virtuales (VPN's) que consiguen confidencialidad en las comunicaciones sobre un canal público gracias a los protocolos IPSec e IKE.[17]

CAPÍTULO 3

ANÁLISIS DE FACTIBILIDAD

En la etapa de análisis se procede a realizar el estudio de la situación actual de la empresa determinando sus requerimientos, además se realiza un análisis costo / beneficio que permitirá definir la factibilidad del proyecto.

3.1 SITUACIÓN ACTUAL

Misión

Ayudar a pequeñas y medianas empresas con soluciones informáticas para la gestión de negocios.

Visión

Ser líder en el desarrollo de soluciones informáticas para la gestión de negocios de pequeñas, medianas y grandes empresas del mercado nacional con proyección internacional en los próximos cinco años.

3.1.2 ORGANIGRAMA ESTRUCTURAL

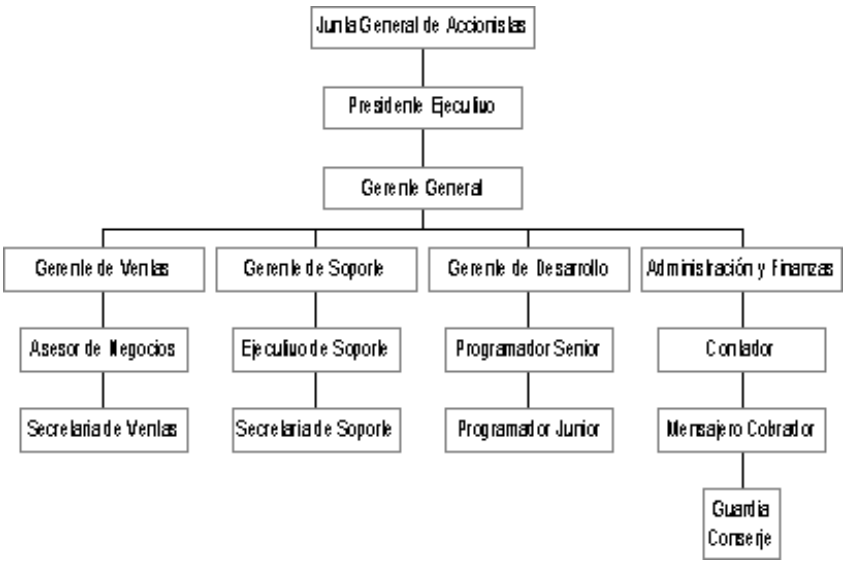

Figura 3-1: Organigrama Estructural
Fuente: Emcosoft \ RRHH

3.1.3 DIAGRAMA DE MACRO PROCESOS

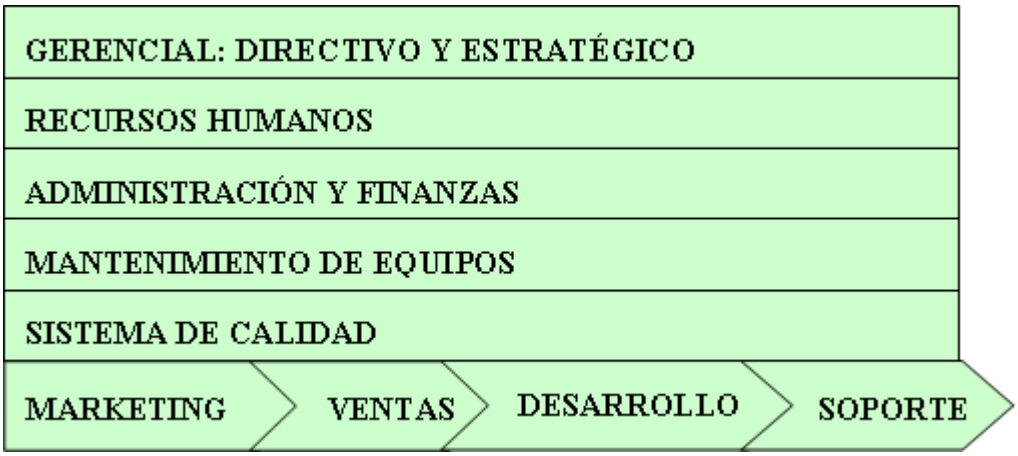

Figura 3-2: Diagrama de Macroprocesos
Fuente: Emcosoft \ RRHH

Las actividades de la empresa se describen en un esquema correspondiente a la cadena de valor, en la figura anterior se distinguen dos tipos de actividades básicas en la empresa: las de “LINEA”, normalmente representadas en la parte inferior del esquema y que tienen que ver directamente con los procesos de creación de valor, y las de “SOPORTE”, en las que las anteriores se apoyan para coordinarse, compartir información, etc.

3.1.4 DESCRIPCIÓN DE PROCESOS

3.1.4.1 Proceso de Marketing

Define responsabilidades, actividades y políticas para la promoción de los productos y servicios al cliente.

3.1.4.2 Proceso de Ventas

Define responsabilidades, actividades y políticas para el eficiente proceso de ventas; además evalúa el grado de cumplimento por parte de la empresa con los requerimientos del cliente.

3.1.4.3 Proceso de Desarrollo

Establece las normas y actividades para la correcta elaboración de software en las distintas fases del diseño y desarrollo. Define responsabilidades, actividades y

políticas para el eficiente proceso de diseño, desarrollo y mantenimiento de software.

El software de la empresa, es revisado en etapas adecuadas. Estas revisiones permiten evaluar la capacidad de los resultados para cumplir con los requisitos, identificar problemas y proponer acciones necesarias. Las revisiones son hechas por personal competente relacionado con el área de desarrollo.

3.1.4.4 Proceso de Soporte

Define responsabilidades, actividades y políticas para el eficiente proceso de soporte al cliente. Se evalúa el grado de satisfacción del cliente con respecto al cumplimiento de sus requerimientos. Esta evaluación es hecha parcialmente en Soporte. La información generada por esta evaluación es usada como elemento de entrada para la revisión del SGC (Sistema de Gestión de Calidad) por parte de la Presidencia Ejecutiva.

3.1.4.5 Proceso Gerencial: Dirección y Estratégico

Establece la estrategia y dirección de la empresa, controla la ejecución de proyectos y procesos, otorga recursos.

La Empresa Comercializadora de Software planifica los procesos necesarios para la realización del producto. Esta planificación se sustenta en el establecimiento de Objetivos de Calidad y de las necesidades de los clientes. Todo esto se gestiona en los procesos de Marketing y Ventas. Este conjunto de necesidades de los clientes constituyen los requisitos del producto. Impulsa el mejoramiento continuo de los procesos de SGC usando para ello las directrices dadas en la Política y Objetivos de Calidad, los informes de resultados de auditorías, los resultados de la operación de los procesos, los resultados de la revisión por la dirección y las acciones preventivas y correctivas tomadas.

3.1.4.6 Proceso de Recursos Humanos

Definir responsabilidades, actividades y políticas para la gestión de los Recursos Humanos.

3.1.4.7 Proceso de Administración y Finanzas

El Contador de la empresa, emite los cheques para que se realice las compras de materiales y productos necesarios para la ejecución de las actividades que se realizan en la empresa, luego los jefes de área respectiva evalúan y seleccionan a sus proveedores de acuerdo a los requerimientos de la empresa.

3.1.4.8 Proceso de Mantenimiento de Equipos

La empresa mantiene en condiciones apropiadas su infraestructura para lograr la conformidad del producto con los requisitos especificados. Esta adecuación de la infraestructura se logra con el adecuado mantenimiento e instalación de los equipos.

3.1.4.9 Proceso de Control de Calidad

Define responsabilidades, actividades y políticas para la gestión del mejoramiento, auditorias, administración de documentos y control de producto no conforme, para lo cual se ha establecido un procedimiento de Auditorias Internas, éste procedimiento describe la forma como la empresa planifica y es llevada a cabo por personal capacitado e independiente de los procesos que se van a auditar. Los resultados son usados como elemento de entrada para la revisión por parte de la Presidencia Ejecutiva.

3.1.5 ANÁLISIS DE LA INFRAESTRUCTURA TECNOLÓGICA DISPONIBLE

3.1.5.1 Hardware

- Se dispone de dos servidores Compaq Proline ML350 G3. distribuidos de la siguiente forma: uno para el servidor de dominio, y otro para la base de datos.

- Un servidor Compaq Proline ML350 G2 para de Internet y correo electrónico.

- Las estaciones clientes están conformadas por equipos clones (23) y portátiles Compaq (4) y Toshiba (3) los clones corresponden a procesadores Pentium IV y Centrino y los equipos portátiles son y Pentium III, y Pentium IV.

- La empresa cuenta en la actualidad con un sistema de cableado estructurado certificado categoría 5.

3.1.5.2 Software

- Para los servidores se cuenta con licencias Windows 2000 Server.

- En las estaciones: Windows 2000 Professional y Windows XP, Office 2000. La versión de Internet Explorer es la 6.0. Además cuenta con el licenciamiento de los siguientes programas: Clipper, Alaska, Visual Studio 6.0, Adobe Acrobat 6.0 Profesional, los cuales utiliza para el desarrollo de las aplicaciones que comercializa.

- La empresa cuenta con un ERP “Enterprise 4.0.1” que corre sobre SQL Server 2000 con las respectivas licencias.

Según lo expuesto anteriormente, se evidencia que la empresa dispone de infraestructura tecnológica que puede ser utilizada en forma más eficiente.

3.2 REQUERIMIENTOS DE LA EMPRESA

3.2.1 Proceso de Marketing

Publicitar los productos y servicios que la empresa ofrece

Proporcionar una guía para llegar al cliente con la información adecuada de los productos y servicios de la empresa, dando la factibilidad de realizar pedidos de productos.

Dar a conocer información publicitaria de la empresa

Mediante la difusión de información con carácter promocional de la empresa, se puede dar a conocer la razón de ser de la organización, así como dar respuesta a las preguntas más frecuentes que se realizan.

Establecer la comunicación con el cliente

- Para los interesados en trabajar en la empresa, permitir registrar solicitudes de empleo que permita hacer selección de personal.
- Dar la posibilidad de establecer una comunicación directa con la empresa para solicitar una demostración de alguno de los productos promocionados.
- Evaluar el grado de satisfacción del cliente con respecto al cumplimiento de sus requerimientos post venta comercial.

3.2.2 Proceso de Ventas

Establecer contactos para realizar demostraciones de los productos.

Cuando se atienden las llamadas de los clientes, se detecta y registra las necesidades del cliente a través del dialogo y se asigna un Asesor de Negocio. Las citas de los clientes son registradas con la siguiente información: nombre del cliente, dirección, teléfonos, fecha y hora de la cita, nombre del asesor de negocios asignado, descripción de la necesidad del cliente.

Disponer de la información necesaria para acudir a las citas de trabajo

Cuando la persona responsable asigna a un determinado Ejecutivo de Ventas para asistir a una demostración, el ejecutivo necesita tener conocimiento de la información necesaria para organizar su agenda de trabajo como por ejemplo: hora y fecha de la cita; nombre, dirección y teléfono del cliente.

Disponer de los formatos para la negociación de los productos y servicios

Una vez realizada la demostración del producto y siendo satisfactoria la negociación, es necesario tener disponible la respectiva documentación para la preparación de los respectivos documentos como: Cotizaciones, Condiciones

Comerciales, Contrato de Licencia, Solicitud de Implementación, Orden de Producción, Nota de Pedido.

3.2.3 Proceso de Soporte

Asignar un Ejecutivo de Soporte para la Implementación y Capacitación

El Departamento de Ventas entrega a Soporte una carpeta con los datos generales del nuevo cliente, en dicha carpeta se encuentra los siguientes documentos: Nota de Pedido, Condiciones Comerciales, Copia de Factura, Orden de Producción, Hoja de Garantía, Licencia y Solicitud de Implementación. Soporte asigna un técnico y le coordina una cita directamente con la persona responsable por parte del cliente.

Soporte atiende las llamadas de los clientes que requieren asesoría en los sistemas ya implementados, detecta las necesidades del cliente a través del diálogo y asigna un técnico coordinándole una cita con la persona responsable por parte del Cliente.

Registrar las Órdenes de Trabajo

El Ejecutivo de Soporte asiste a las oficinas del cliente y entrega un servicio personalizado de soporte técnico. Al finalizar la visita el técnico de Soporte llena la Orden de Trabajo en la cual detalla: nombre del cliente, el nombre del ejecutivo, las actividades realizadas, la hora de entrada y de salida de las oficinas del cliente.

Disponer de la información necesaria para acudir a las citas de trabajo

Cuando la persona responsable asigna a un determinado técnico para asistir a una cita y dar solución a algún requerimiento, el técnico necesita tener conocimiento de la información necesaria para organizar su agenda de trabajo como por ejemplo: hora y fecha de la cita; nombre, dirección y teléfono del cliente.

Disponer de la información necesaria de los trabajos realizados por cada cliente

Como diferentes técnicos atienden los requerimientos de cada cliente, es necesario tener disponible la respectiva documentación de los trabajos realizados para facilitar el conocimiento de la operación del cliente por cualquier técnico que deba acudir para dar solución a los nuevos requerimientos.

3.2.4 Proceso de Recursos Humanos

Disponer de los formatos del bienestar del personal

Solicitudes de Vacaciones, Aviso de Enfermedad, Licencia por Maternidad, Forma para reportar Gastos de Presentación, adicionalmente el calendario de vacaciones y días de descanso

Descripción de puestos y responsabilidades

Especificando el nombre del cargo solicitado, descripción del cargo, tareas típicas, requisitos del puesto, tiempo máximo de contratación.

Disponer de la información de los aspirantes

El personal responsable de la contratación de personal necesita tener disponible la información de los currículums de los aspirantes cuando se de la necesidad de cubrir una vacante y establecer contacto con los aspirantes pre seleccionados.

Disponer de información relativa a los empleados

Es necesario publicar la información referente a la historia laboral de los empleados.

Difundir la información acerca de la organización estructural de la empresa

3.2.5 Proceso de Operación y Administración

Disponer de la información relativa a los procesos establecidos como normativos de la empresa

Disponer ***de la información relativa a la Difusión y Comunicación*** como: revista de la empresa, comunicados de prensa, Reportes Anuales, Folletos y Hojas de Especificaciones.

Tener la posibilidad de actualizar automáticamente la información de las novedades acontecidas en la empresa

Disponer de la información recopilada en Capacitaciones

Con la finalidad de mantener disponible toda la información en capacitaciones publicar los respectivos Manuales de Capacitación y Presentaciones didácticas de los cursos tomados.

3.3 ANÁLISIS DE LAS HERRAMIENTAS PARA LA CONSTRUCCIÓN PARA LA INTRANET / EXTRANET

Con el propósito de obtener una solución óptima y acorde a los requerimientos de la empresa Comercializadora de Software en cuanto a la construcción de la Intranet / Extranet se realizará un análisis de las herramientas disponibles en el mercado, en cuanto se refiere a:

3.3.1 PLATAFORMAS DE DESARROLLO

Con el fin de elegir la plataforma tecnológica a utilizar para la implementación del proyecto optamos por hacer un estudio entre dos plataformas (J2EE y .NET), para lo cual se analizarán algunos aspectos explicando cómo se comportan ambas plataformas con respecto a las diferentes necesidades del sistema como:

- Herramientas de Desarrollo
- Portabilidad
- Transaccionalidad
- Seguridad
- Escalabilidad

En el siguiente cuadro se exponen varios criterios de comparación entre las plataformas.

3.3.1.1 Cuadro Comparativo.

CARACTERÍSTICAS	.NET	J2EE
Herramientas de Desarrollo	Visual Studio .NET Los Lenguajes de programación que utiliza son: Visual C# .NET, Visual Basic .NET, C++ , Visual J# .NET(para lograrlo utiliza CLS Common Language Specification	Se requieren múltiples productos: Editor de código HTML, DreamWeaver de Macromedia ó FrontPage. Editor de código Java como JBuilder de Borlan o Netbeans Forte de Sun, Visual Café de WebGain, Visual Age for Java de IBM El lenguaje de programación es JAVA
Portabilidad (posibilidad de ejecutar las aplicaciones desarrolladas en cualquier sistema operativo y/o máquina del mercado)	.NET sólo está preparada para ejecutarse sobre plataformas Microsoft Windows.	Como J2EE es adoptado por varios fabricantes, una misma aplicación será portable entre los distintos sistemas siempre que mantengamos la solución del mismo vendedor. Sin embargo estos productos son portables en todos los sistemas.
Transaccionalidad (es la forma como desarrolladores gestionan las transacciones, puede ser manual o automático (dejarle la gestión al contenedor)	El contenedor es el CLR	El contenedor es el EJB
Seguridad	Los servicios de autenticación y autorización son proporcionados mediante el sistema operativo y sus archivos de identificación.	La funcionalidad de autenticación y autorización es proporcionada por Sun mediante JAAS (Java Authentication and Authorisation Service), basado en PAM.
Escalabilidad (Es la capacidad de un sistema para soportar más carga de trabajo, usualmente debida al aumento de usuarios que lo utilizan)	Ofrece métodos como la carga balanceada que permite a un cluster de servidores (varios servidores) colaborar y dar un servicio de forma simultánea.	Ofrece métodos como la carga balanceada que permite a un cluster de servidores (varios servidores) colaborar y dar un servicio de forma simultánea

Tabla 3-1: Cuadro Comparativo .NET vs. J2EE
Fuente http://www.deltablog.com/2005/06/08/net-vs-j2ee/

3.3.1.2 Conclusiones

- En cuanto a portabilidad con J2EE existe el problema de que es un estándar y no un producto en sí. Este hecho, que facilita la adopción de esta tecnología por parte de varios fabricantes, también conlleva que las implementaciones de J2EE no son 100% compatibles entre sí, ya que cada vendedor ha realizado su propia interpretación del estándar. En definitiva, pasar de una implementación J2EE a otra requerirá de modificaciones en el código de la aplicación y la portabilidad se pierde en gran parte. La solución de Microsoft .NET siempre funcionará mejor que la basada en J2EE, porque tanto Windows como .NET son productos de Microsoft, lo que asegura una mayor integración.
- .NET Soporta múltiples lenguajes, J2EE solamente soporta el lenguaje (Java).
- .NET hace todo de forma mucho más automática y simple que J2EE, tiene muchos asistentes que facilitan el trabajo con la plataforma, en J2EE hay muchas cosas que aprender para sacarle provecho a la plataforma (Lenguaje Java, AWT, Swing, JDBC, JAR, JavaDocs, Java Servlets, JSP, Java Beans, JSF) entre otros, lo cual para un desarrollador de poca o mediana experiencia puede ser complicado.
- J2EE en sus implementaciones requiere de mayores recursos, tanto económicos como humanos, que Microsoft .NET, aunque presenta la ventaja de su portabilidad, su madurez y el apoyo que le ofrecen empresas como IBM, Oracle o Sun. En general sus clientes serán las grandes corporaciones que actualmente mantienen sistemas muy heterogéneos, entre ellos las administraciones públicas.
- Según un estudio estadístico se concluye que J2EE necesita más líneas de código que .NET para realizar la misma funcionalidad. El estudio lo realizó la compañía **Software Productivity Research** publicado en: http://www.gotdotnet.com/team/compare/petshop.aspx.

3.3.2 SISTEMAS OPERATIVOS

Los sistemas operativos proporcionan una plataforma de software encima de la cual otros programas puedan funcionar, asegura que los programas y usuarios que están funcionando al mismo tiempo no interfieran entre ellos, también es responsable de la seguridad, asegurándose de que los usuarios no autorizados no tengan acceso al sistema.

Las aplicaciones se programan para que funcionen sobre un sistema operativo particular, por tanto, la elección del sistema operativo determina en gran medida las aplicaciones que se pueden utilizar.

A continuación se describen algunos de ellos:

3.3.2.1 Windows Server 2003

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de Redes privadas virtuales (VPN) (o acceso remoto al servidor).
- Controlador de Dominios (mediante Active Directory).
- Servidor WINS.

Funcionalidades

Directorio Activo.

Tiene la capacidad de renombrar dominios, la posibilidad de redefinir el esquema, de desactivar tanto atributos como definiciones de clase en el esquema, la selección múltiple de objetos sobre los cuales realizar cambios simultáneamente, y la de establecer relaciones de confianza en bosques cruzados, evitando problemas con políticas de usuarios y grupos.

Administración.

A través de la Consola de Gestión de Políticas de Grupo (GPMC) se proporcionan herramientas y servicios entre como Windows Management Instrumentation (WMI), Resultant Set of Policy (RsoP) y la nueva tecnología de Instalación Remota (RIS), con cuya implementación los usuarios pueden disponer de sus aplicaciones y datos sin importar desde donde se conecten a la red corporativa.

Seguridad.

Permite gestionar la autenticación y autorización de usuarios, el soporte del protocolo Kerberos V5, las mejoras en la autenticación de clientes SSL, la gestión de credenciales (incluyendo claves y certificados X.509), el Internet Connection Firewall y la seguridad mejorada del servidor Web. Encriptar la información para mantenerla segura dentro y fuera de la organización (gracias a los Servicios de Gestión de Derechos Digitales). La integración con Passport y el mantenimiento de relaciones de confianza entre bosques cruzados (procedentes de socios o compañías colaboradoras) permite compartir credenciales y acceso a datos entre diferentes organizaciones.

Internet Information Services mejora la seguridad, fiabilidad y rendimiento. Las aplicaciones Web en ejecución están aisladas una de la otra, permitiéndose la monitorización y administración de aplicaciones así como cambios de configuración en línea, reduciendo el tiempo que precisan los administradores para reiniciar servicios con el fin de mantener las aplicaciones operativas. Con el IIS 6.0 la replicación de configuraciones de servicio Web en diferentes servidores es automatizada permitiendo a los administradores reducir el tiempo de implementación.

Clustering.

Con características avanzadas de recuperación ante fallos y balanceo de carga, ofrecen la máxima disponibilidad 7x24. Integrándose en el Directorio Activo (en el que cada cluster es visto como un objeto "virtual") y con soporte tanto de 32 como de 64 bit, en Microsoft Windows Server 2003 se ha incrementado de 4 a 8 el número máximo de nodos por cluster, disponiendo así el administrador de más opciones para garantizar el servicio para las necesidades de la empresa.

Networking & Comunicaciones.

Con ayuda de la Resultant Set of Policy se puede analizar el impacto de la implementación de políticas de red y comunicaciones, simplificando así la resolución de problemas.

Mediante los servicios de Instalación Remota, las herramientas para migración de configuraciones de usuarios, el nuevo Windows Installer (con sopor te de aplicaciones de 64 bit, así como de firmas digitales y CLR), los Software Update Services (SUS) para testear las actualizaciones de Windows Update antes de ser aplicadas en la organización, se logra una mejor gestión centralizada de recursos y servicios.

Terminal Services.

Permite disponer de aplicaciones Windows e incluso de los propios escritorios Windows en cualquier dispositivo. Ofrecen nuevas opciones para la implementación de aplicaciones, un acceso más eficiente a los datos con conexiones de menor ancho de banda, mayor número de usuarios concurrentes, y mediante Session
Directory proporciona el soporte necesario para el balanceo de carga de red.

Existe una edición de Microsoft Windows Server 2003 para satisfacer las necesidades de cada organización:

- ***Web Edition Diseñado.-*** Para los servicios y el hospedaje Web.
- ***Standard Edition.-*** El más versátil de todos, ofrece un gran número de servicios útiles para empresas de cualquier tamaño.
- ***Enterprise Edition.-*** Para empresas de mayor tamaño que la Standard Edition.
- ***Datacenter Edition.-*** Para empresas que requieran bases de datos más escalables y un procesamiento de transacciones de gran volumen. [18]

Requerimientos

Procesador: Procesador a 133 MHz o superior para equipos basados en x86; 733 MHz para equipos basados en Itanium; hasta ocho procesadores compatibles en la versión de 32 bits o 64 bits.

Memoria: 128 MB de RAM mínimo; máximo: 32 GB para equipos basados en x86 con la versión de 32 bits y 64 GB para equipos basados en Itanium con la versión de 64 bits.

Hard Disk: 1,5 GB de espacio disponible en disco equipos basados en x86; 2 GB para equipos basados en Itanium; se necesita espacio adicional si se instala en una red.

3.3.2.2 Linux Fedora Core 6

Fedora es la distribución heredera más directa de Red Hat, es un sistema operativo de propósito general y basado exclusivamente en software libre.

Fedora dispone de tres repositorios fundamentales:

- Core: en el cual se encuentran los paquetes esenciales.
- Extras: en el cual se encuentran los paquetes más utilizados o demandados.
- Updates: en el cual se encuentran las actualizaciones periódicas.

Funcionalidades

Administración

Cuenta con el instalador gráfico Anaconda para facilitar la instalación del sistema y que también tiene soporte para IPv6.19

El Stateless Linux permite al administrador de sistemas mantener una instalación sincronizada e idéntica con el método de: instalación original en una máquina maestra y repeticiones de esta instalación en máquinas esclavo, las que nunca deberán se actualizadas o reconfiguradas individualmente.

Seguridades

Provee capacidades integradas de tarjetas inteligentes para autenticación segura.

Utiliza SELinux que es herramienta gráfica para la solución de problemas.

Clustering

Esta versión introduce una nueva herramienta, la **lvm2-cluster**, para manejar volúmenes clúster con facilidad.

Navegabilidad

El paquete mozilla fue eliminado. Para una funcionalidad equivalente se usa firefox como navegador web y thunderbird como cliente de correo.

Servidor Web

Fedora Core 6 incluye la versión 2.2 del servidor HTTP Apache.

Base de Datos

Fedora provee **MySQL** 5.0 y PostgreSQL 8.1

Requerimientos

Procesador: Ordenador Pentium o equivalente; 200 MHz o mayor para sistema en modo texto; 400 MHz Pentium II o mayor para sistema en modo gráfico.

Memoria: 128 MB mínimo para sistema en modo texto; 256 MB mínimo para sistema en modo gráfico.

Hard Disk: 620 MB para instalación mínima; 1.1 GB para instalación servidor; 2.3 GB para sistema de escritorio personal; 6.9 GB instalación completa.

3.3.2.3 Cuadro Comparativo de Precios

Producto	Precio (USD $)
Linux Fedora Core 6	Sin costo
Windows 2003 Server	727.53

Tabla 3-2: Cuadro Comparativo de Precios
Fuentes: Linux: http://fedoraproject.org/es/index;
Windows: Akros

3.3.2.4 Conclusiones

- Se ha seleccionado el sistema operativo Windows 2003 Server debido a la amplia gama de funciones de servidor que dispone.

- Windows 2003 Server es un sistema operativo ampliamente probado y recomendado en el mercado.

- La infraestructura de la red actual de la organización está basada en Windows, de manera que existirá una mejor integración con Windows 2003 Server, y con las mejoras que presenta con Active Directory.

3.3.3 SERVIDORES DE BASES DE DATOS

Parte de una solución integral para el manejo de tres capas constituye el servidor de base de datos, el cual permite extraer, consolidar, integrar, resumir, analizar, compartir información de la empresa en forma confiable y segura. Uno de los aspectos más importantes que se analiza es la capacidad para manejar concurrencia y bloqueo de datos.

Las siguientes tablas muestran las características de Microsoft SQL 2005.

3.3.3.1 SQL 2005 Enterprise Edition

CARACTERÍSTICA	DESCRIPCIÓN
Soporte para .NET Framework	Se puede desarrollar funciones, procedimientos y triggers en lenguajes como C# y VB.NET.
Tecnologías XML	Soporta el almacenamiento de documentos XML, especificación de consultas con XML y devolución de resultado de consultas como documentos XML.
ADO.NET Versión 2.0	ADO .NET supone una evolución de los métodos de acceso y manipulación de datos, para conseguir una mayor escalabilidad y flexibilidad.
Mejoras en Transact-SQL	Manejo de errores, consultas recursivas
Servicios de Notificación	Permiten construir aplicaciones de notificación capaces de expedir información personalizada en el momento en que se genera.
Servicios Web	Los desarrolladores pueden crear servicios Web en la capa de base de datos, convirtiendo a SQL Server en un servidor HTTP. Esta capacidad supone un nuevo modelo de acceso a los datos para aplicaciones basadas en Web Services.
Soporte para Xquery	Permiten la manipulación de objetos XML en la capa de datos, así como un nuevo juego de herramientas de creación de Xquery.
Mejoras en Seguridad	Separa a los usuarios de los objetos, proporciona un acceso muy granular y un mejor control de los accesos a los datos. Además, todas las tablas del sistema se implementan ahora como Vistas, lo que redunda en un mayor control sobre los objetos de sistema de la Base de Datos.

Tabla 3-3: Características SQL 2005
Fuente: http://www.microsoft.com/spain/sql/productinfo/features/top30features.mspx

CARACTERÍSTICA	EXPRESS	WORKGROUP	STANDARD	ENTERPRISE	COMENTARIOS
Número de CPU	1	2	5	Ilimitado	Es compatible con procesadores multinúcleo
RAM	1 GB	3 GB	Ilimitado	OS Max	Memoria limitada a un máximo compatible con el sistema operativo
Tamaño de la base de datos	4 GB	Ilimitado	Ilimitado	Ilimitado	
Partición	No	No	No	Si	Compatibilidad para bases de datos a gran escala
Operaciones de índice paralelo	No	No	No	Si	Procesamiento paralelo de operaciones de indexación
Vistas indexadas	No	No	No	Si	Se admite la creación de vista indexada en todas las ediciones. La correspondencia de vista indexada por el procesador de consulta sólo se admite en la Enterprise Edition.

Tabla 3-4: Escalabilidad y Rendimiento de SQL
Fuente: http://www.microsoft.com/spain/sql/productinfo/features/compare-features.mspx

CARACTERÍSTICA	EXPRESS	WORKGROUP	STANDARD	ENTERPRISE	COMENTARIOS
Auditoría, autenticación y autorización avanzadas	Si	Si	Si	Si	
Cifrado de datos y administración de claves	Si	Si	Si	Si	Cifrado de datos incorporado para lograr seguridad avanzada de datos
Analizador de prácticas más adecuadas	Si	Si	Si	Si	Explora su sistema para garantizar que se sigan las prácticas más adecuadas recomendadas
Integración con Microsoft Baseline Security Analyzer	Si	Si	Si	Si	Explora su sistema para verificar vulnerabilidades comunes de seguridad
Integración con Microsoft Update	Si	Si	Si	Si	

Tabla 3-5: Seguridad en SQL
Fuente: http://www.microsoft.com/spain/sql/productinfo/features/compare-features.mspx

Requerimientos	Express	Workgroup
Sistema Operativo	• Windows XP Home Edition** • Windows Server 2003 Web Edition4 (Express únicamente)	• Windows XP Professional** • Windows XP Media Edition** • Windows XP Tablet Edition** • Windows 2000 Professional*
Memoria	512 MB (se recomienda 512 MB o más; 1 GB como máximo)	512 MB (se recomienda 1 GB o más; 3 GB como máximo)
Disco Duro	350 MB de espacio disponible en el disco duro para la instalación completa	350 MB de espacio disponible en el disco duro para la instalación completa

Tabla 3-6: Requerimientos de SQL
Fuente: http://www.microsoft.com/spain/sql/productinfo/features/compare-features.mspx

Precios Server 2005	Licencia por procesador	Server plus User/Device CALs
	Precio	Precio
Express Edition	Libre	Libre
Compact Edition	Libre	Libre
Workgroup Edition	$ 3,899	$739 con 5 Workgroup CALs
Standard Edition	$ 5,999	$1,849 con 5 CALs
Enterprise Edition	$ 24,999	$13,969 con 25 CALs

Tabla 3-7: Precios Referenciales SQL
Fuente: http://www.microsoft.com/spain/sql/productinfo/features/compare-features.mspx

3.3.3.2 ORACLE

Aplicaciones Administrativas de Oracle

- Oracle se basa en la tecnología cliente/ servidor para la gestión de Bases de Datos, para su utilización es necesario la instalación de la herramienta servidor por ejemplo (Oracle8i) y posteriormente para acceder a la base de datos desde otros equipos con herramientas de desarrollo como Oracle Designer y Oracle Developer, que son las herramientas de programación sobre Oracle.

- Oracle soporta datos alfanuméricos, así como también textos sin estructura, imágenes, audio y video.

- Soporta 17 idiomas, corre en más de 80 arquitecturas de hardware y software distinto sin cambiar una sola línea de código debido a que más del 80% de los códigos internos de Oracle son iguales a los establecidos en todas las plataformas de sistemas operativos.
- Versiones de Oracle:
    - **Oracle 5 y Oracle 6**: fueron las dos primeras versiones de Oracle.
    - **Oracle 7:** La base de datos relacional componentes de Oracle Universal Server. Posee además las versiones 7.1, 7.1.2, y 7.1.3.
    - **Oracle 8:** Soporta aplicaciones de procesamiento de transacciones on line (OLTP) y de data warehousing.

- **Oracle Fail Safe:** Protege al sistema de caída de entornos Cluster Windows NT. Este producto es para que el sistema operativo Windows NT disponga de una mayor oferta de soluciones en entornos cluster.
- **Oracle Universal Server:** Con soporte completo de Web, mensajería y datos multimedia. [20]

Producto	Usuario Nombrado	Update, Licencia y Soporte	Licencia por procesador	Update, Licencia y Soporte
	(USD $)	(USD $)	(USD $)	(USD $)
Base de Datos:				
• Estándar Edition One	149.00	32.78	4,995.00	1,098.90
• Estándar Edition	300.00	66.00	15,000.00	3,300.00
• Enterprise Edition	800.00	176.00	40,000.00	8,800.00
Data WareHouse:				
• Express Server	800.00	176.00	40,000.00	8,800.00
• Express Analizer	800.00	176.00	n/a	n/a
• Express Object	5,000.00	1,100.00	n/a	n/a
Internet Aplication Server:				
• Standard Edition One	149.00	32.78	4,995.00	1,098.90
• Standard Edition	200.00	44.00	10,000.00	2,200.00
• Enterprise Edition	600.00	132.88	30,000.00	6,600.00
• Business Intelligence	400.00	88.00	20,000.00	4,400.00

Tabla 3-8: Precios Oracle a Diciembre 2006
Fuente: http://www.oracle.com/corporate/pricing/eplext.pdf

Oracle Database Standard Edition One. - Este producto está orientado a empresas pequeñas, para poder utilizar esta versión, el equipo sobre el que va a ser instalado no puede contar con capacidad para más de dos procesadores. Actualmente existe para Windows, Unix y Linux. Como se puede apreciar en la tabla, el costo de este producto es de $4,995 por procesador (máximo dos), o de $149 por usuario (mínimo 5).

Oracle Database Standard Edition.- Este producto cuenta con las mismas características que la versión Standard Edition One, pero esta puede ser configurada en un equipo con capacidad hasta 4 procesadores, el costo es de $15,000 por procesador (máximo 4) ó de $300 por usuario (mínimo 5).

Oracle Database Enterprise Edition.- Orientado a empresas grandes o que requieren características especiales, puede ser configurado sin restricción de procesadores, y su costo es de $40,000 por procesador o de $800 por usuario (mínimo 25 usuarios por procesador instalado).

Funciona en más plataformas que la Estándar e incluye mejoras en el manejo de redes, administración, características de Data Warehousing. También tiene otras opciones para funciones especiales tales como integración con datos a sistemas de información geográfica, sonido y video.

Opciones de Oracle Database Enterprise Edition

Real Application Cluster.- Su finalidad es poder tener múltiples servidores soportando a la misma base de datos, tiene un costo de USD $20,000 por procesador, o de USD $400 por usuario nombrado.

El número de procesadores o usuarios a licenciar debe ser igual al número de procesadores o usuarios licenciados para Oracle Enterprise Edition.

Partitioning.- Una opción que permite administrar las tablas grandes de la base de datos en diferentes tablespaces, para ayudar al rendimiento de la base de datos. Su costo es de USD$10,000 por procesador o USD $200 por usuario.

Aplicaciones para Mantenimiento

Oracle Packs.- Diagnostic, Tunning, Change Management, Configuration Management son características adicionales que permiten facilitar la administración del motor de base de datos Oracle, así como potenciar su rendimiento. El costo de cada uno de estos 4 paquetes es de $3,000 por procesador o de $60 por cada usuario.

3.3.3.3 Cuadro Comparativo de Precios

Producto	Precio (USD $)
Microsoft SQL 2005	897.07
Oracle	727.53 (por usuario)

Tabla 3-9: Cuadro Comparativo de Precios
Fuente: http://www.oracle.com/corporate/pricing/eplext.pdf

3.3.3.4 Conclusiones

- Del análisis realizado anteriormente concluimos que se utilizará SQL Server 2000. Entre las razones por las cuales se optó por este producto se encuentran: el proyecto utiliza como fuente, los datos replicados de la base SQL SERVER 2000 del ERP (Enterprise Resource Planning) propio de la empresa, adicionalmente su costo es accesible, es el más adecuado para el tamaño de la empresa y los costos indirectos como por ejemplo el soporte técnico especializado es más fácil de conseguir.

- La administración es más intuitiva y fácil debido a la interfaz gráfica y gran cantidad de asistentes disponibles para ejecutar tareas de administración.

- SQL Server tiene mejor integración, compatibilidad con .NET de Microsoft que es la herramienta seleccionada para el desarrollo.

3.3.4 SERVIDORES WEB

Un servidor Web es un programa, que tiene la función de permitir desarrollar y administrar sistemas de hospedaje de sitios, lo que hace un servidor es atender las solicitudes que se piden vía Internet.

3.3.4.1 IIS Internet Information Services 6.0

IIS engloba un conjunto de herramientas destinadas al control de servicios de Internet como el Web, FTP, correo y servidores de noticias. Además incluye el soporte necesario para la creación de páginas dinámicas.

- Incorpora servicios como (HTTP, HTTPS), SMTP, NNTP, ejecuta páginas ASP, PHP (si se instalan las librerías de PHP). Incluye ASP.NET, WebDav y una gestión de la ejecución de las aplicaciones y, rendimiento Web mejorado. También incorpora una nueva forma de administrar las extensiones de servidor a través de Web.[21]

- Una de las formas que tiene IIS de asegurar los datos es mediante SSL (Secure Sockets Layer). Esto proporciona un método para transferir datos entre el cliente y el servidor de forma segura, permitiendo también que el servidor pueda comprobar al cliente antes de que inicie una sesión de usuario.

- IIS tiene integrado el protocolo Kerberos v5.

- El almacenamiento de certificados se integra ahora con el almacenamiento CryptoAPI de Windows. Se puede utilizar el administrador de certificados de Windows para hacer una copia de seguridad, guardar y configurar los certificados.
- Autenticación implícita que permite a los administradores autenticar a los usuarios de forma segura a través de servidores de seguridad y Proxy.

- Permite impedir que aquellos usuarios con direcciones IP conocidas obtengan acceso no autorizado al servidor, permitiendo especificar la información apropiada en una lista de restricciones.

- La administración de la seguridad del servidor IIS se realiza base de asistentes para seguridad. Se pueden definir permisos de acceso en

directorios virtuales e incluso en archivos, de forma que el asistente actualizará los permisos NTFS para reflejar los cambios. Si se trabaja con entidades emisoras de certificados, es posible gestionar la lista de certificados de confianza (CTL, Certificate Trust List) con el asistente para CTL.[22]

3.3.4.2 Apache

- Permite restringir determinados sitios Web, conexiones seguras a través de SSL, configuración de módulos de programación.

- Apache permite manejar mensajes de error altamente configurables, bases de datos de autenticación.

- Permite la restricción a determinados sitios Web.

- Falta de una interfaz gráfica que ayude en su configuración.

- Tomcat funciona con cualquier servidor Web con soporte para servlets y JSPs. Incluye el compilador Jasper, que compila JSPs convirtiéndolas en servlets. El motor de servlets del Tomcat a menudo se presenta en combinación con el servidor Web Apache.

- Tomcat puede funcionar como servidor Web. Opera en entornos de desarrollo poco exigentes en términos de velocidad y de manejo de transacciones. Dado que Tomcat fue escrito en Java, funciona en cualquier sistema operativo que disponga de la máquina virtual.

- Tomcat lo desarrollan y lo mantienen miembros de la Apache Software Foundation y voluntarios independientes. Los usuarios disponen de libre acceso a su código fuente. Las primeras distribuciones de Tomcat fueron las versiones 3.0.x. Las versiones más recientes son las 5.x, que

implementan las especificaciones de Servlet 2.4 y de JSP 2.0. En las versiones 4.x, Jakarta Tomcat utiliza el contenedor de servlets.

3.3.4.3 Cuadro comparativo

Característica	Apache Tomcat 1.3.19	Internet Information Services
Empresa distribuidora	Apache Software Foundation	Microsoft
Precio	Libre	Incluido en las versiones de Windows NT, 2000, 2003 Server
Sistema operativo	Unix, todas las versiones de Windows	Todas las versiones de Windows para servidores
Integración con Proxy	Necesita herramienta adicional	Si
Protocolo de seguridad	SSL, configuración de módulos de programación	SSL (Secure Sockets Layer), Integrado Kerberos v5 Administración de estados de conexión
Autenticación de usuarios	Integración con LDAP	Mediante servidores de seguridad y Proxy.
Almacenamiento de certificados	Integración con SSL	CryptoAPI de Windows, para hacer una copia de seguridad, guardar y configurar los certificados.
Requisitos mínimos de hardware	Aproximadamente 12 MB durante la instalación, y 3 MB una vez instalado.	512 MB y 40 MB en disco.

Tabla 3-10: Cuadro Comparativo IIS vs. Apache
Fuente: http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch08.html
http://httpd.apache.org/docs/2.2/faq

Requerimientos de sistema para instalar Apache

Como mínimo de condiciones para el óptimo funcionamiento del servidor se necesita de un mínimo aproximado de 12 megas durante la instalación y 3 megas para instalarlo.

3.3.4.4 Comparativo de Precios

IIS es un servicio incorporado en el Sistema Operativo Windows 2000 Server y Apache es software libre.

3.3.4.5 Conclusión

Los dos servidores Web analizados se encuentran altamente difundidos en el mercado y ofrecen casi las mismas funcionalidades, pero en concordancia con la plataforma seleccionada, se concluye que IIS es la opción indicada para el presente caso.

3.3.5 SERVIDORES DE CORREO ELECTRÓNICO

3.3.5.1 Exchange Server 2003

Exchange 2003 es el servidor de correo electrónico y colaboración de Microsoft diseñado para ayudar a los negocios a comunicarse en forma más eficaz. Exchange 2003 ofrece acceso móvil, remoto y de escritorio al correo electrónico con avanzada seguridad y privacidad; menor costo total de propiedad a través de los servicios proporcionados por Microsoft Windows Server™ 2003; alta confiabilidad y sorprendente rendimiento; colaboración basada en el correo electrónico; y fácil actualización, implementación y administración.[23]

Las principales características son:

- Internet Information Services (IIS) proporciona todos los servicios basados en protocolos Web en Exchange, así como formularios Web y soporte para DAV (Distributed Authoring and Versioning), Control de Versiones y Autoría Distribuida.

- El cliente de Exchange Outlook, se conecta con el servidor Exchange sobre una conexión HTTP segura, mediante IIS 6.0 que proporciona un nuevo medio de comunicación llamado “RPC (Remote Procedure Call) mediante el protocolo MAPI”, permitiendo a los usuarios conectarse directamente al servidor de Exchange a través de Internet, sin necesidad de establecer un túnel de red privada virtual (VPN).

- IIS proporciona a Exchange soporte para protocolos de acceso como POP3, IMAP4 y SMTP.

- Windows proporciona el servicio de directorio Active Directory, del cual depende Exchange para mantener la información de usuarios, enrutamiento de mensajes, validación de accesos y funciones de lectura y escritura mediante protocolo LDAP.

- Exchange Server 2003 graba la información sobre el servicio de Instantáneas de Volumen de Windows Server 2003, permitiendo reducir

los tiempos de backup y recuperación para los entornos de mensajería. Esto permite reducir el número de servidores Exchange en los entornos informáticos.

- Exchange Server 2003 está previsto solo ejecutarse sobre un servidor Windows Server 2003.

- Cuando se instala Exchange Server 2003 se deshabilita los ISAPIs (Internet Server Application Programming Interfaces) por defecto. Para que un archivo ejecutable pueda interactuar con peticiones desde IIS, necesita estar escrito con ISAPI. El deshabilitar ISAPI por defecto supone que en una instalación por defecto de Windows Server 2003, IIS solo será capaz de devolver archivos HTML estáticos.

- Exchange 2003 permite acceso a Outlook Web Access (OWA), mediante esta opción los usuarios podrán hacer Bloqueo de archivos adjuntos, crear reglas de gestión de mensajes en el servidor y leer y enviar mensajes firmados digitalmente creándose una firma que se incluye automáticamente en todos los mensajes de correo electrónico.

- Del lado del Servidor, se pueden configurar diferentes funciones para evitar el spam.

- Implementando un servicio de lista de bloqueo en tiempo real que contiene listas de direcciones IP de orígenes conocidos como correo no deseado. Así los administradores de Exchange 2003, pueden mantener una lista de direcciones IP de envío para los mensajes de correo electrónico que siempre se acepten o siempre se rechacen.

- Para ayudar a bloquear gran parte del correo no deseado que los usuarios reciben, es el control acerca de qué mensajes reciben y de quiénes también. El filtro no distingue ningún remitente o tipo de mensaje en particular. El control de los mensajes se basa en el

contenido del mensaje y se utiliza un análisis avanzado de su estructura para determinar la probabilidad de que el usuario considere el mensaje como correo deseado o no. Se pueden hacer 2 tipos de filtrado: el de remitentes, el cual examina el campo de cada mensaje de correo entrante y lo compara con una lista de remitentes bloqueados; y el de destinatarios, para bloquear los mensajes de correo electrónico dirigidos a destinatarios no válidos (direcciones que no existen en el servicio de directorio Active Directory de Windows) o a direcciones de correo electrónico restringidas.

- Con Exchange Intelligent Message Filter, los usuarios de Exchange 2003 pueden clasificar cada mensaje de correo entrante según la probabilidad de ser correo deseado o no, de acuerdo con las características controladas por Smart Screen, que ayuda a filtrar el correo antes de llegar a la bandeja de entrada del usuario. La base de datos utilizada para almacenar las características se actualiza con nueva información de patrones del origen de la muestra, haciendo que el filtro sea más eficaz y actual. El filtro inteligente de mensajes utiliza esta base de datos para reconocer modelos de mensajes legítimos y no legítimos, permitiendo llevar a cabo una evaluación más precisa de la legitimidad de un mensaje de correo electrónico entrante.

Características Generales:

- Compatibilidad de Seguridad de protocolo Internet (IPSec).
- Autenticación Kerberos
- Solicitudes firmadas de Protocolo ligero de acceso a directorios (LDAP) para el servicio de directorio Active Directory.
- Modo de aplicaciones dedicado y seguridad de Servicios de Internet Information Server (IIS) 6.0.

Correo Electrónico

- Listas de distribución restringidas a usuarios autenticados

- Listas seguras y de bloqueo en tiempo real
- Filtrado de destinatarios de entrada
- Filtrado y protección avanzados de mensajes de correo electrónico no deseado (requiere Outlook 2003)
- API de detección de virus 2.5 (requiere software antivirus de terceros)
- Bloqueo de datos adjuntos en Microsoft Office Outlook Web Access
- Mejoras de permisos de carpetas públicas para usuarios desconocidos

Outlook Web Access

- Acceso HTTP desde Outlook 2003
- Compatibilidad con exploradores cHTML (teléfonos i-Mode)
- Compatibilidad con exploradores xHTML (Protocolo de aplicaciones inalámbricas [WAP] 2.0)

Administración

- Habilitación de autorización mediante cookies
- Jerarquía de envío de carpetas públicas
- Informes automáticos de errores[24]

Requerimientos del sistema para Exchange 2003 Enterprise Edition

Componente	Requerimiento	Recomendación
Procesador	Intel Pentium o procesador compatible de 133-megahercios (MHz) o capacidad superior	Intel Pentium o procesador compatible de 733-MHz
Sistema operativo*	• Microsoft Windows® 2000 Server, Windows 2000 Advanced Server o Windows 2000 Datacenter Server con SP3 o versión posterior • Microsoft Windows Server™ 2003, Standard Edition; Windows Server 2003, Enterprise Edition; o Windows Server 2003, Datacenter Edition	Windows Server 2003 para 32 Bits
Memoria	256 megabytes (MB) de RAM	512 MB de RAM
Espacio disponible en disco duro	Requiere de: • 500 MB en el disco duro en que instale Exchange 2003 • 200 MB en la unidad del sistema	Requiere de: • 500 MB en el disco duro en el que instale Exchange 2003 • 200 MB en la unidad del sistema

Tabla 3-11: Requerimientos Exchange
Fuente: www.microsoft.com/spain/technet

3.3.5.2 SendMail

- SendMail es el agente de transporte de correo en los sistemas UNIX. Aunque actúa principalmente como MTA (Mail Transport Agent, su función es transferir los mails a su destino), también puede ser utilizado como MUA (Mail User Agent, su función es la creación de mails) aunque no posee interfaz de usuario.

- Recoge los mails provenientes de un MUA como el, Eudora o provenientes de un MTA como el mismo SendMail. Reparte los mails basándose en la información de la dirección del destinatario contenida en la cabecera.

- Si el mail es local enviará el mail al programa de reparto local de mails.

- Si el mail no es local, SendMail utiliza el DNS para determinar el host al que debe ser enviado el mail. Para transferir el mensaje, iniciará una sesión SMTP con el MTA de dicho host.

- Si no es posible mandar el mail a su destino (porque la maquina receptora esta desconectada, o está muy lenta), SendMail almacena los mails en una cola de correo, y vuelve a intentar el envío del mail un tiempo después. Si el mail no puede ser enviado tras un tiempo razonable, el mail será devuelto a su autor con un mensaje de error. SendMail debe garantizar que cada mensaje llegue correctamente a su destino, o si hay error este debe ser notificado.

- SendMail ofrece compatibilidad entre usuarios distintos, para ello reformatea el mail antes de pasarlo a la siguiente máquina, según reglas de reescritura. Según el tipo de conexión que posea una máquina, o según el agente de transporte al que vaya dirigido el mail,

se cambian los formatos de las direcciones del remitente y del destinatario, se cambian algunas líneas de la cabecera del mail.

- Permite el uso de "alias" entre los usuarios del sistema, lo que permite crear y mantener listas de correo entre grupos.

- Las funciones del SendMail deben ser configuradas y variarán de unos sistemas a otros. Para configurarlas se usa el fichero de configuración de SendMail.

- Aunque no posee interfaz de usuario, SendMail como agente de usuario (MUA) permite el envío directo de mails a través de un ejecutable, el cual lee su entrada estandard hasta encontrar un end-of-file (EOF) o una línea que contenga únicamente un punto ("."), en ese momento manda una copia de ese mensaje a cada una las direcciones destino que se le habrán pasado previamente en la línea de comandos. SendMail determina cómo enrutar un mensaje, de acuerdo a la información que posee en su fichero de configuración.

- SendMail como MTA se queda como proceso residente (demonio) escuchando el puerto 25, admitiendo y realizando conexiones SMTP cuando sea invocado, Cuando reciba una petición de conexión, creará un proceso hijo que se encargará de ello, mientras el proceso padre seguirá escuchando el puerto 25.

3.3.5.3 Cuadro Comparativo de Precios

Producto	Precio (USD $)
Exchange 2003	2732,51
SendMail	libre

Tabla 3-12: Cuadro Comparativo de Precios
Fuente: Akros

3.3.5.4 Conclusiones

- En coherencia con el sistema operativo seleccionado y por la compatibilidad e integración, se ha seleccionado Exchange Server 2005, como servidor de correo electrónico.

- El proceso de actualización del sistema hacia Exchange Server 2005 se beneficiará con las ventajas de integración que presenta Active Directory.

3.3.6 SERVIDORES FIREWALLS O CORTAFUEGOS

El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñado para proteger las fuentes de información. Un firewall en general es un programa que restringe las conexiones TCP/IP. Los firewalls perimetrales, los más clásicos, hacen de pasarela entre una red local de una organización e Internet. Dejan entrar y salir sólo el tráfico que definan los administradores de la red, y habitualmente hacen traducción de direcciones de red (NAT - también llamado "enmascaramiento") y escanean el tráfico en busca de virus y otros programas maliciosos.

3.3.6.1 Internet Security And Acelerator Server

(ISA SERVER2004)

- Seguridad de nivel corporativo.
- Arquitectura multicapa: permite filtrado de paquetes, filtrado de circuitos, y aplicación.
- Inspección de paquetes a nivel de datos (Stateful Inspection): analiza los comandos dentro de los protocolos de aplicación y los datos, verifica el tráfico VPN, HTTP, FTP, SMTP, POP3, DNS, conferencia H.323, difusión multimedia y RPC. Además controla el estado de la conexión, incluyendo el uso los protocolos de nivel IP.

- Publicación en servidor seguro: permite impersonar el servidor de publicación, añadiendo una capa de seguridad.
- VPN integrado: permite un control muy granular sobre los recursos y protocolos a los que los usuarios de VPN pueden acceder.
- Transparencia de firewall: SecureNAT sustituye una dirección IP válida de Internet por una dirección IP interna, sin necesidad de software cliente ni configuración adicional.
- Autenticación de usuario reforzada.: Los usuarios se pueden validarse contra la base de datos de usuarios local en el propio firewall, el Directorio Activo o mediante RADIUS (Remote Authentication Dial-In User Service)
- Puente SSL a SSL: para servidores Web que requieren acceso de cliente autentificado y cifrado, El servidor ISA Server 2004 desencripta el flujo SSL, realiza la inspección de datos y después vuelve a encriptar los datos y los redirige al servidor de publicación Web.
- La política FTP de ISA Server 2004 se puede configurar para admitir descargas desde o hacia la red corporativa utilizando FTP, o bien limitando el acceso de los usuarios a descargas FTP en sentido entrante.
- Se pueden configurar una o más redes, cada una con una relación distinta con las otras.
- Cifrado obligatorio para conexiones seguras con Exchange usando RPC al impedir que las credenciales del usuario y los datos se intercambien en formatos no encriptados.
- Se pueden volcar los logs a una base de datos SQL emplazada en otra máquina dentro de la red interna.
- Los sitios Web publicados se protegen de accesos no autenticados al exigir que el firewall ISA Server 2004 autentifique al usuario antes de que la conexión se reenvíe al sitio Web publicado. Así se evita que usuarios no autenticados puedan acceder al servidor Web publicado y originar ataques.
- ISA Server 2004 puede autenticar conexiones remotas utilizando el sistema de autentificación bifactorial SecurID. Con esto se consigue un

alto grado de seguridad en la validación, ya que el usuario debe “saber” algo y “tener” algo para conseguir el acceso al servidor Web publicado.

- Imposición de la política de uso de Internet controlando el acceso por usuario, grupo, aplicación, destino, planificación, y tipo de contenido.

Cache Web

- Cache de Web de alto rendimiento: cache en RAM rápido y un cache a disco optimizado para proporcionar el mejor rendimiento posible en la navegación Web.
- Cache planificado: La cache se puede precargar con contenidos de sitios Web completos siguiendo una planificación temporal.
- Cache jerárquico: permitiendo configurar una jerarquía de cache, encadenando matrices de máquinas, de modo que los clientes pueden acceder al cache más próximo.

Gestión simplificada.

- Control de acceso basado en políticas: Se puede controlar el acceso de entrada y salida a nivel de usuario, grupo, aplicación, dirección de origen y destino, contenido y planificación temporal. Los asistentes de Políticas de Firewall permiten especificar qué sitios y contenidos pueden accederse, si un protocolo concreto es accesible en comunicación entrante o saliente, y permitir o denegar la comunicación entre direcciones IP específicas, utilizando protocolos y puertos concretos.
- Gestión simplificada: permite copiar toda la configuración del firewall a un archivo XML, de gran ayuda para normalización y respaldo.
- Integración con Directorio Activo: potenciar la base de datos de usuarios almacenada en el Directorio Activo para validar tanto el acceso entrante como el saliente a través del firewall.
- Paneles de tareas en formato gráfico: simplifican la navegación y configuración de las tareas más frecuentes del firewall.

Gestión remota

- Registro de actividad, informes y alertas
- Gestión a nivel de usuario

Plataforma extensible

- Amplio soporte para aplicaciones y productos de otros fabricantes, por ejemplo, se pueden aplicar filtros para impedir el paso de virus de última generación, o la descarga de scripts Java o controles ActiveX hacia el interior de redes seguras
- Proporciona documentación completa del API y ejemplos paso a paso para desarrollar nuevos filtros Web o de aplicación, snap-ins para consolas MMC, herramientas de informes, comandos en formato script, gestión de alertas y otras muchas utilidades.

3.3.6.2 Symantec Firewalls

"Desde avanzadas soluciones de software hasta appliances únicos de seguridad integrada, la familia firewall y VPN de Symantec ofrece a las organizaciones la flexibilidad de escoger el nivel adecuado de protección de red que requieran."[25]

De la amplia gama de productos tanto en hardware y software que Symantec ofrece haremos hincapié en los que se adaptan al tamaño de la empresa:

- Symantec ™Enterprise Firewall.- proporciona protección de firewall rápida y segura, de inspección completa, una tecnología de firewall que de forma predeterminada protege contra ataques a nivel de las aplicaciones o de la red. Suministra el alto rendimiento que requieren las redes actuales permitiendo que el tráfico autorizado fluya de forma rápida y segura en la empresa.
- Symantec ™Enterprise VPN.- Altamente seguro y fácil de administrar, Symantec Enterprise VPN utiliza tecnología única de análisis ProxySecured para monitorear y controlar el tráfico. Constituye una forma poderosa de establecer vínculos encriptados seguros entre oficinas, usuarios móviles y socios.

- El appliance Symantec ™ Firewall //VPN.- proporciona una seguridad estricta del perímetro de la red ya que sólo permite el acceso a Internet de aplicaciones y usuarios autorizados. Una familia de appliances multifuncionales que ofrece tres modelos para satisfacer las necesidades de seguridad y trabajo en red de ubicaciones remotas y oficinas. El modelo que nos aplicaría corresponde al Symantec Enterprise FW/VPN modelos 100/200/200R, aunque el firewall no hace filtrado de contenido, requiere antivirus y el IDS es limitado.
- Antivirus for Microsoft Internet Security and Acceleration (ISA) Server. - soporta tráfico SMTP, HTTP/FTP recomendado para empresas de tamaño pequeño a mediano soporta plataforma Windows 2000 Server, Advanced Server, Windows Server 2003, Solaris, y Red Hat Linux.
- Enterprise VPN 7.0 .- Una red privada virtual segura y fácil de administrar, de alto rendimiento, que reduce los gastos administrativos, al mismo tiempo que protege los activos corporativos y las transacciones comerciales, tiene licencia para 50 usuarios, admite el algoritmo AES (Estándar de Cifrado Avanzado), e incluye:

  - Servidor VPN ProxySecured.- que permite que las organizaciones extiendan sus redes más allá del firewall de la empresa, sin correr riesgos, porque ofrece exploraciones ProxySecured de la VPN en los servidores y protección de firewall personal en las estaciones de trabajo. Es una solución VPN/firewall basada en estándares, que permite conexiones de alta velocidad y seguras con Internet (disminuyendo así los costos de conexión), y que mejora la integración con los socios comerciales dando acceso rápido y seguro a la información a trabajadores móviles, clientes y oficinas remotas.
  - **La tecnología de exploración ProxySecured controla el tráfico.-** Symantec Enterprise VPN es el único servidor de VPN que incluye exploraciones ProxySecured de las conexiones IPSec, permitiendo así que los administradores vigilen y controlen el tráfico de entrada y de salida, tanto a nivel de las aplicaciones, como a nivel de la red.

Para mejorar la seguridad en las estaciones de trabajo e impedir ataques a la red con base a la dirección IP, su firewall integrado cuenta con la posibilidad de configurar el bloqueo automatizado de puertos y otras capacidades continuas de endurecimiento del sistema que protegen las redes en todos los puntos posibles de entrada.

- **Firewall independiente para una fácil integración**.- Symantec Enterprise VPN es una solución de seguridad completamente integrada que reduce los costos de administración del acceso remoto. Diseñado para asistir tanto a las empresas con redes altamente sofisticadas, como a las que sólo requieren protección básica de correo electrónico y navegación por la Web, es un componente de seguridad esencial para el mundo conectado electrónicamente de hoy en día. Gracias a la configuración y conexión de un paso de los clientes Symantec Enterprise VPN, el despliegue y la administración son sencillos. Y como su operación es independiente de las arquitecturas de firewall, se integra fácilmente en las redes ya existentes e interactúa con muchas otras variedades de firewall. Para evitar que el firewall se encargue de tareas de cifrado que pueden sobrecargar el CPU y crear obstrucciones, el servidor Symantec Enterprise VPN se puede instalar en otro servidor separado del Symantec Enterprise Firewall.[26]

3.3.6.3 Firewalls de las Series Cisco

- Cisco PIX 501 Firewall: desarrollado para empresas pequeñas, es un producto de seguridad plug and play muy confiable, ideal para ambientes de banda ancha. Realiza inspección stateful, basada en el algoritmo de Seguridad Adoptivo (ASA), soporta sobre 100 aplicaciones predefinidas, servicios y protocolos para control de acceso flexible. Permite acceso a VPN usando estándares IKE/IPSec. Switch integrado que permite a múltiples usuarios compartir una conexión de banda

ancha. Como firewall bloquea los controles Active X que crean muchos problemas potenciales a los clientes de la red e incluso a los servidores.

- Características de hardware.- chasis compacto para escritorio, con procesador de 133 MHz, 16 MB en RAM y 8 MB de memoria flash, interfaz Ethernet, un puerto para Internet y 4 para LAN, puerto para consola de acceso administrativo. 60 Mbps de texto claro atravesando el firewall, 4.5 Mbps atravesando la VPN con AES128/SHA-1 o 3 Mbps con 3DES/SHA-1.
- Características de software.- versión 6.1 que incluye un Cisco PIX Device Manager (PDM) para administración intuitiva basada en Web. Soporta hasta 10 hosts activos pero son ampliables con su respectiva licencia. Soporta hasta 10 accesos remotos o puntos VPN.[27]

3.3.6.4 Conclusiones

- Se ha seleccionado ISA Server como Servidor Firewall porque integra en una sola aplicación múltiples productos de seguridad como software antivirus y firewalls en las estaciones de trabajo en red y remotas, haciendo que la estrategia de desplegar, instalar, administrar y actualizar los productos de seguridad disminuya los gastos de administración y soporte.
- Para protegernos mejor de las complejas amenazas de Internet, necesitamos una solución manejable que incluya una gama de complejas tecnologías de seguridad con administración integrada.

3.4 ANÁLISIS COSTO BENEFICIO

Las Intranets/Extranets son una alternativa muy apreciable porque aprovechan los actuales sistemas de información incluyendo la infraestructura de redes, computadores personales, servidores y las aplicaciones de sistemas existentes, lo que reduce su costo de inversión.

La viabilidad de un proyecto depende siempre de un análisis de rentabilidad exhaustivo que refleje entre otros datos la recuperación de la inversión realizada.

Para esto se procede en primer lugar a la revisión de datos históricos de la situación general de la empresa

3.4.1 DATOS HISTÓRICOS

A través del Departamento de Administración y Finanzas de la empresa se han obtenido los datos de la situación financiera de la empresa de los 5 años anteriores (2003-2007). Estos datos históricos nos muestran las siguientes políticas:

- El incremento de las ventas de los paquetes de software es de un promedio de 10% anual.
- Los precios de venta por paquetes de software se incrementan en un promedio de 2% anual.
- Los costos de comercialización de paquetes de software no son constantes, tienen un incremento del 2% el primer año, un 3% el segundo año y un 6% los dos siguientes. Tabla Situación Financiera sin Proyecto

Situación Financiera sin Proyecto					
Período	Año 2003	Año 2004	Año 2005	Año 2006	Año 2007
Unidades Vendidas	360	396	436	479	527
Precio (USD $)	1,070.00	1,091.40	1,113.23	1,135.49	1,158.20
Costo (USD $)	470.00	479.40	493.78	523.41	554.81
% Incremento Costo		2%	3%	6%	6%

Tabla 3-13: Situación Financiera sin Proyecto
Fuente: EMCOSOFT. Departamento Financiero

La variación del costo de desarrollo y comercialización dio como resultado una variación de la utilidad de la empresa. La misma que seguía generando utilidades pero en menor porcentaje cada año, hasta el año 2007 que generó una utilidad notablemente menor con relación a años anteriores. Tabla Estado de Resultados Históricos.

Estado de Resultados Históricos	Año 2002	Año 2003	Año 2004	Año 2005	Año 2006
Ventas (USD $)	385,200.00	432,194.40	484,922.12	544,082.62	610,460.69
(-)Costo de Ventas (USD $)	169,200.00	189,842.40	215,091.44	250,796.62	292,428.86
(=)Utilidad Bruta en Ventas (USD $)	216,000.00	242,352.00	269,830.68	293,286.00	318,031.84
(-)Gastos Operacionales (USD $):					
• Gastos de Administración (USD $)	207,318.02	228,049.82	250,854.80	275,940.28	303,534.31
• Gastos de Comercialización (USD $)	3,852.00	4,501.94	5,029.22	5,620.83	6,284.61
• Depreciaciones (USD $)	3,250.00	3,250.00	3,250.00	3,250.00	3250.00
• Amortizaciones (USD $)	150.00	150.00	150.00	150.00	150.00
TOTAL GASTO (USD $)	214,570.02	235,951.77	259,284.03	284,961.11	313,218.92
UTILIDAD OPERACIONAL (USD $)	1,429.98	6,400.23	10,546.65	8,324.89	4,812.92
(+-)MOV. FINANCIERO:					
(-)Intereses Pagados (USD $)	-3,062.50	-2,450.00	-1,837.50	-1,225.00	-612.50
(=)Utilidad Neta (USD $)	-1,632.52	3,950.23	8,709.15	7,099.89	4,200.42
(-) 36,25% Imp. Y Particip. (USD $)	0.00	1,432.16	3,157.50	2,574.06	1,522.86
(=)UTILIDAD DESPUÉS DE IMP. Y PARTICIP (USD $):	-1,632.52	2,518.08	5,551.65	4,525.82	2,677.56

Tabla 3-14: Estado de Resultados Históricos
Fuente: EMCOSOFT. Departamento Financiero

3.4.2 INVERSIÓN

3.4.2.1 Inversión en Software

Para el cálculo de las inversiones se toma en cuenta los paquetes adicionales que deben comprarse para la implementación de la Intranet / Extranet en lo referente a software, en base a lo que dispone actualmente la empresa, especificado en el "Análisis de la Infraestructura Tecnológica Disponible", punto 3.1.5.2.

Software	Unidades	Costo Unitario (USD $)	Costo Total (USD $)
Sistema Operativo Windows 2003 Server	2	727.53	1,455.06
Servidor de Correo Electrónico Exchange Svr. 2007 Spanish OLP NL	1	707.51	707.51
Exchange Standard CAL 2007 Spanish OLP NL Device CAL	30	67.50	2,025.00
ISA Server Std Ed 2006 Spanish OLP NL 1 Proc	2	1,311.50	2,623.00
Visual Studio Pro 2005 Spanish OLP NL	1	542.36	542.36
SQL Svr. Standard Edtn. 2005 Win 32 Spanish OLP NL Qualified	1	896.07	896.07
Total (USD $):			**8,249.00**

Tabla 3-15: Inversión en Software
Fuente: Akros

NOTA: Estos valores son referenciales en el mercado y están proyectados a tres años incluidas las renovaciones de licencias.

3.4.2.2 Inversión en Hardware

Para la inversión el Hardware se considera utilizar equipos con garantía técnica, que garantice su óptimo funcionamiento y respaldo en caso de fallas.

Hardware	Unidades	Costo Unitario (USD $)	Costo Total (USD $)
Servidor Proliant ML150 G4 ▪ Procesador Intel Xeon Core Duo 3.06 Ghz ▪ Memoria 512MB ▪ 2 Hdd modelo SCSI de 34.4 GB ▪ Tarjeta de red Giga Ethernet	2	1,413.44	2,826.80
Total (USD $):			**2,826.80**

Tabla 3-16: Inversión en Hardware
Fuente: Akros

3.4.2.3 Inversión en Personal de Desarrollo.

Constituyen las inversiones y gastos necesarios para desarrollar el proyecto que se ha estimado estará concluido, en un período de 6 meses y con esta condición se realizará el cálculo para determinar el valor total.

Personal de Desarrollo	Personas	Valor Mensual (USD $)	Valor Semestral (USD $)
Programador	2	500.00	6,000.00
Web Master	1	500.00	3,000.00
Total (USD $):			**9,000.00**

Tabla 3-177: Inversión en Personal de Desarrollo
Fuente: Las Autoras

Inversión	Valor (USD $)
Inversión de Software de Sistemas	8,249.00
Inversión de Hardware	2,828.80
Inversión de Personal para Desarrollo	9,000.00
Total (USD $):	**20,077.80**

Tabla 3-188: Inversión Total
Fuente: Las Autoras

3.4.3 PROYECCIONES

Por medio de la implementación del proyecto se pretende subir la productividad de la empresa atacando al factor de los “Costos de Ventas”, que por datos históricos observados en la tabla 3-13 “Estado de Resultados Históricos” crecen notoriamente.

Con la implantación del proyecto la empresa pretende controlar el incremento de los costos con relación a las ventas y al precio, para así lograr mantener el equilibrio costo-beneficio.

Partiendo de los datos históricos proporcionados por Departamento Financiero y con las premisas facilitadas por la Gerencia de la empresa se han elaborado proyecciones a 3 años del funcionamiento y operación de la misma con la implantación del nuevo proyecto, para lo cual se realizó la proyección del *Estado de Resultados* a 3 años incluyendo los costos de inversión y nuevo personal para el proyecto. Las premisas para elaborar la proyección son las siguientes:

- La inversión del proyecto se estima en USD $20,077.80 con un Capital de Trabajo para operar de USD $10,000.00.
- El porcentaje de las ventas crece un 10% con relación al año anterior, y el último año crece en un 1% adicional, es decir al 11%
- El precio, por políticas de la empresa crece un 2% cada año y al igual que el promedio de unidades vendidas, el último año proyectado crece un 1% adicional, es decir un 3% en relación al anterior.
- Se financiará alrededor del 50% del proyecto con un préstamo bancario y la diferencia como inversión propia.

- El proyecto se basa en incrementar la productividad de la empresa mediante el ahorro de los “Costos de Ventas” en los que está incurriendo, ya que por datos históricos tienen un crecimiento desordenado y no acorde con el crecimiento de las ventas y del precio.
- El proyecto busca mantener un incremento lógico del costo en un 3% constante durante los próximos años y al igual que las ventas y el precio, crecer un 1% adicional en el último año estimado. Tabla situación Financiera con Proyecto.

Período	Año 2007	Año 2008	Año 2009
Unidades Vendidas	580	638	708
Precio (USD $)	1,181.37	1,204.99	1,241.14
Costo (USD $)	571.46	588.60	612.15
% Incremento Costo	3%	3%	4%

Tabla 3-199: Situación Financiera con Proyecto
Fuente: Las Autoras

Al momento de lograr equilibrar los costos, la empresa genera un incremento constante de la utilidad lo que demuestra un mejor uso de sus recursos, cumpliendo así el objetivo del proyecto. Tabla Proyecciones.

Estado de Resultados Proyectado	Año 2007	Año 2008	Año 2009
Ventas (USD $)	684,936.90	768,499.20	878,625.14
(-)Costo de Ventas (USD $)	331,321.89	375,387.71	433,347.57
(=)Utilidad Bruta en Ventas (USD $)	353,615.00	393,111.49	445,277.57
(-)Gastos Operacionales (USD $):			
• Gastos de Administración (USD $)	324,569.64	357,026.60	392,729.26
• Gastos de Comercialización (USD $)	20,049.37	20,884.99	21,986.25
• Depreciaciones (USD $)	3,250.00	3,250.00	3,250.00
• Amortizaciones (USD $)	150.00	150.00	150.00
TOTAL GASTO (USD $)	348,019.01	381,311.60	418,115.52
UTILIDAD OPERACIONAL (USD $)	5,596.00	11,799.90	27,162.05
(+-)MOV. FINANCIERO:			
Intereses Ganados			
(-)Intereses Pagados (USD $)	-1,800.00	-1,200.00	-600.00
(=)Utilidad Neta (USD $)	3,796.00	10,599.90	26,562.05
(-) 36,25% Imp. Y Particip. (USD $)	1,376.24	3,842.99	9,630.07
(=)UTILIDAD DESPUÉS DE IMP. Y PARTICIP (USD $):	2,419.76	6,756.90	16,931.98

Tabla 3-20: Proyecciones
Fuente: Las Autoras

A partir de estas proyecciones se debe efectuar el cálculo del Flujo Efectivo Operacional, que se requiere para realizar el cálculo de los índices de rentabilidad como el TIR (Tasa Interna de Retorno), el VAN (Valor Actual Neto), y el PRI (Periodo de Recuperación de la Inversión), índices utilizados generalmente en la industria para reflejar la viabilidad de un proyecto. [28]

3.4.3.1 Cálculo del Flujo de Efectivo Operacional (FEO).

Se realiza éste cálculo para saber la liquidez real de la empresa, puesto que en el Estado de Resultados Proyectados se incluyen valores que no constituyen erogación de efectivo real como las amortizaciones y las depreciaciones, y que deben sumarse a la utilidad para los cálculos de los índices. Tabla Flujo Efectivo Operacional.

FEO	Año 2007	Año 2008	Año 2009
(+)Utilidad (USD $)	2,419.76	6,756.90	16,931.98
(+)Depreciación (USD $)	3,250.00	3,250.00	3,250.00
(+)Amortización (USD $)	150.00	150.00	150.00
Total (USD $):	5,819.76	10,156.90	20,331.98

Tabla 3-21: Flujo Efectivo Operacional
Fuente: Las Autoras.

Para el cálculo de los índices se debe considerar también la amortización del financiamiento dentro del mismo período de 3 años lo que nos da el valor real de los flujos de efectivo que utilizaremos. Tabla Valor Real del Flujo Efectivo

		Año 2007	Año 2008	Año 2009
FEO (USD $)		5,819.76	10,156.90	20,331.98
Inversión (USD $) (USD $)	-20,077.80			10,000.00
Capital de Trabajo K (USD $)	-10,000.00			
Financiamiento (USD $)	15,000.00	-5,000.00	-5,000.00	-5,000.00
Flujo Actualizado (USD $)	-15,077.80	819.76	5,156.90	25,331.98

Tabla 3-222: Valor Real del Flujo de Efectivo
Fuente: Las Autoras

Para el estudio financiero de éste proyecto se tomará en cuenta una Tasa de Descuento del 15%. Esta tasa es el valor que se desea obtener por la inversión, está compuesta por el promedio entre el Costo financiero del endeudamiento

(13%), y la rentabilidad mínima que el inversionista desea obtener en este proyecto (17%). Todos estos datos son ingresados en las fórmulas de los cálculos financieros por medio de una hoja de Excel y se obtiene los siguientes resultados.

3.4.4 ÍNDICES

3.4.4.1 Tasa Interna de Retorno (TIR)

Mide el retorno de la inversión, utilizando la proyección de los flujos para compararlo con una determinada Tasa de Descuento. El resultado de éste cálculo es un porcentaje que si es superior a la Tasa de Descuento el proyecto se torna aceptable, se estaría ganando más de lo esperado, lo que se conoce como utilidades extraordinarias. Tabla 3-23 “Índices”.

Al interpolar los porcentajes extremos del VAN un positivo y un negativo se obtiene la Tasa Interna de Retorno

$TIR= i_1 – [(i_1-i_2) (VAN_1 /(VAN_{1-} VAN_2)]$

i_1= tasa de descuento que hace positivo al VAN

i_2= tasa de descuento que hace negativo al VAN

VAN_1= Valor Actual Neto positivo

VAN_2= Valor Actual Neto negativo

3.4.4.2 Valor Actual Neto (VAN)

Refleja el valor actual de la empresa utilizando los flujos de efectivo proyectados tomando en cuenta una tasa de descuento. Para que un proyecto sea aceptable utilizando la técnica del VAN, este resultado debe ser positivo. Tabla 3-23 “Índices”.

La fórmula es la siguiente:

$$VAN = \sum [(FEO) / (1+ K)^n] – I$$

Flujo de caja del periodo sobre 1+ la tasa de descuento elevado a la n (cada período) – inversión

Índices	Valores
Valor Actual (USD $)	21,268.38
Valor Actual Neto (VAN) (USD $)	6,190.58
KP (Tasa de descuento)	15%
Tasa Interna de Retorno (TIR)	30.43%

Tabla 3-233: Índices
Fuente: Las Autoras

3.4.4.3 Período de Recuperación de la Inversión (PRI)

Es el tiempo real en el que de acuerdo a la proyección de los flujos vamos a recuperar la inversión. De acuerdo al análisis el resultado es 2 años 4.3 meses. Valor obtenido de las siguientes operaciones: primero se divide para 12 del valor del Flujo Anual del año 3 (período en que la Inversión por Recuperar dejará de ser negativa) para conseguir las correspondientes mensualidades y posteriormente se divide el valor de la Inversión por Recuperar del año 2 para estas mensualidades.

CÁLCULO DEL PERÍODO REAL DE RECUPERACIÓN (PRR)			INVERSIÓN POR RECUPERAR (USD $)
	FLUJO (USD $)		
AÑO	ANUAL	ACUMULADO	-15,077.80
1	819.76	8,601.13	-14,258.04
2	5,156.90	18,338.62	-9,101.14
3	25,331.98	29,234.99	16,230.84

Tabla 3-244: Período Real de Recuperación
Fuente: Las Autoras.

3.5.4 CONCLUSIONES

El análisis muestra los siguientes resultados:

VAN: USD $6,190.58. Es un valor positivo superior a las expectativas de la inversión, lo que demuestra que es un proyecto viable.

TIR: 30.43%. Al compararla con la tasa de descuento del 15%, éste resultado muestra que es un proyecto viable, que supera las expectativas del inversionista por lo que se recomienda su implantación.

PRI: 2 años 4.3 meses. Es un tiempo de recuperación consecuente con el tipo de proyecto, se tendrá la capacidad de contar con un retorno de inversión que permitirá aumentar el costo de oportunidad (utilidad).

3.5 PLANTEAMIENTO DE LA SOLUCIÓN RECOMENDADA

La solución que se plantea es implementar una Intranet / Extranet que permita mejorar la operatividad de la empresa por medio de un sistema WEB que contempla las siguientes características:

3.5.1 TECNOLOGÍA

Se propone desarrollar el sistema en entorno de tres capas: **páginas WEB con tecnología ASP.Net** (Active Server Pages) para el lado del *Cliente*, componentes **desarrollados en Visual Basic y C# para la encriptación de datos** e IIS (Internet Information Server) para la capa *Intermedia* y Microsoft SQL Server 2000 como motor de bases de datos para la capa *de Datos*. En el lado del cliente es necesario disponer de Internet Explorer 6.0 o superior. Se instalará automáticamente con el sistema operativo, esto facilitará la tarea de implementación de terminales nuevas.

3.5.2 HERRAMIENTAS DE DESARROLLO

Se plantea utilizar el conjunto de tecnologías orientadas a la implementación de aplicaciones para Internet, como Visual Studio.Net para el desarrollo de páginas activas (ASP.NET) programando componentes desarrollados en Visual Basic.NET y C#, y la utilización de Crystal Reports para la creación de reportes, además de los lenguajes HTML y Java Script para que el sistema interactúe con el cliente.

3.5.3 BASE DE DATOS

Se utilizará un Servidor de Base de Datos Relacional Microsoft SQL Server 2000, que proporciona soporte para un conjunto de ventajosas características: facilidad de instalación y utilización.

3.5.4 PORTABILIDAD

Otro beneficio de la aplicación es que podrá correr sobre otros browsers como Mozilla Firefox o Netscape 7.0.

3.5.5 SEGURIDAD

La concepción modularizada de todo el sistema permitirá asignar a cada usuario los procedimientos que le corresponden por sus responsabilidades y permisos, al nivel de usuarios y funciones.

La seguridad está implementada den tres niveles, la primera es por medio de la utilización de DMZ según Figura 4-33 “Diseño Físico”, constituida con ISA Server, la segunda es la petición por el lado del cliente de páginas Web seguras por medio del protocolo SSL configurado en el servidor Web IIS si y solo si el usuario se ha autenticado previamente, y la tercera es la encriptación de los datos enviados a la base de datos a través de algoritmos de encriptación.

Los accesos estarán controlados por inicios de sesión de usuario que evita la manipulación no autorizada de páginas intermedias tales como las que existen en el historial del navegador o explorador de Internet.

3.5.6 COMUNICACIÓN

Al estar desarrollado en tecnología Web usa un cliente liviano que puede trabajar sobre una red LAN en el caso de los usuarios locales, ó por medio Internet, ya sea módem y línea telefónica, wireless, enlace dedicado, etc. Por donde se levantará conexiones VPN o solicitudes https.

3.5.7 IMPLEMENTACIÓN

En las terminales de trabajo, sólo será necesaria la instalación del sistema operativo, el cual incluye el explorador de Internet, además de Adobe Reader.

Para el caso de los servidores se requieren configuraciones específicas de las funciones que realizarán.

CAPÍTULO 4

DESARROLLO E IMPLEMENTACIÓN DE LA INTRANET/ EXTRANET

4.1 ANÁLISIS Y DEFINICIÓN DE REQUERIMIENTOS

4.1.1 CAPTURA DE REQUERIMIENTOS COMO CASOS DE USO

El siguiente diagrama muestra el sistema de forma general en una vista de nivel 1.

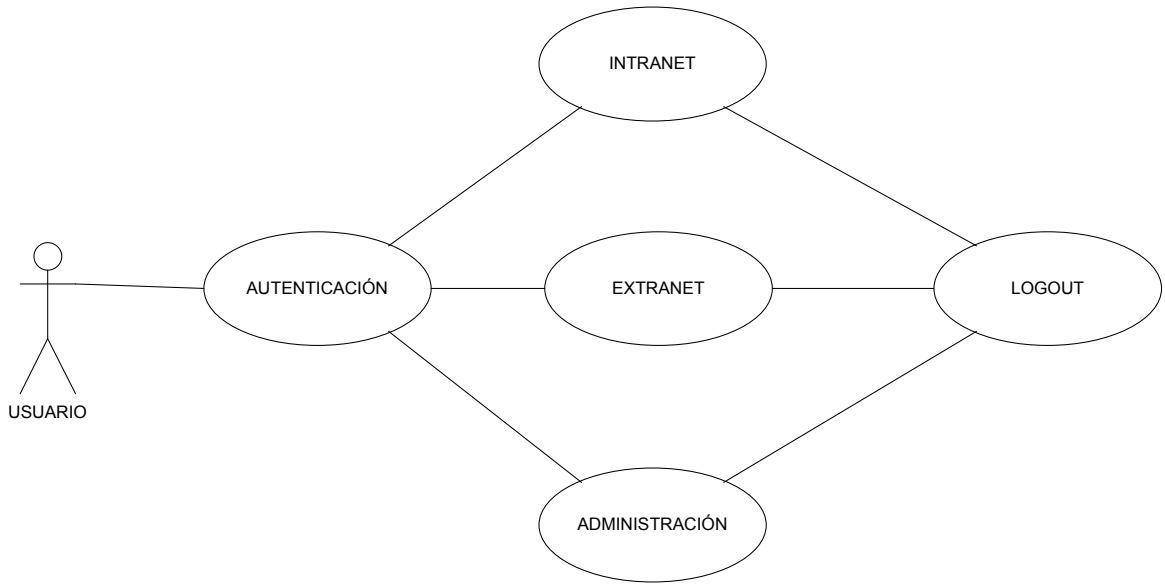

Figura 4-1: Diagrama de Casos de Uso de Nivel 1: Sistema
Fuente: Las Autoras

4.1.1.1 Diagrama de Casos de Uso: Autenticación

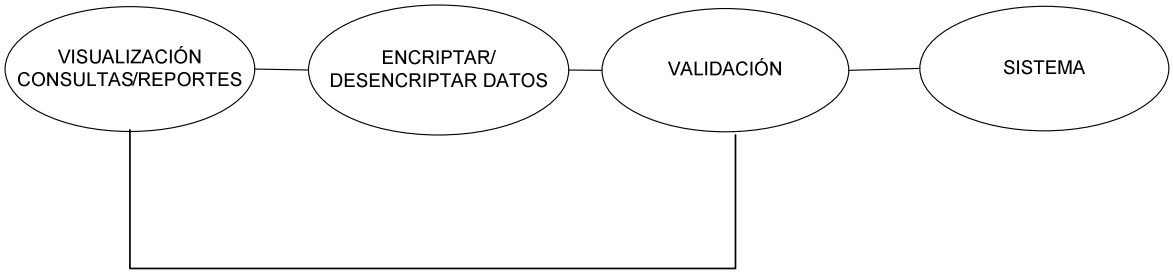

Figura 4-3: Diagrama de Casos de Uso de Nivel 2: Autenticación
Fuente: Las Autoras

4.1.1.2 Diagramas de Casos de Uso: Intranet

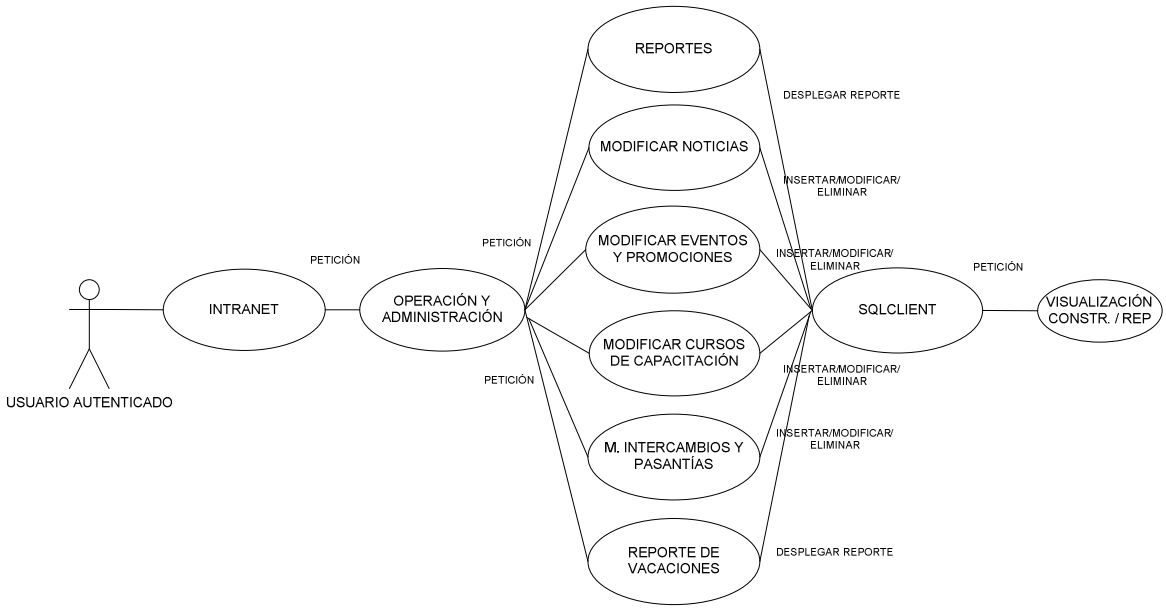

Figura 4-4: Diagrama de Casos de Uso de Nivel 2: Intranet / Operación y Administración
Fuente: Las Autoras

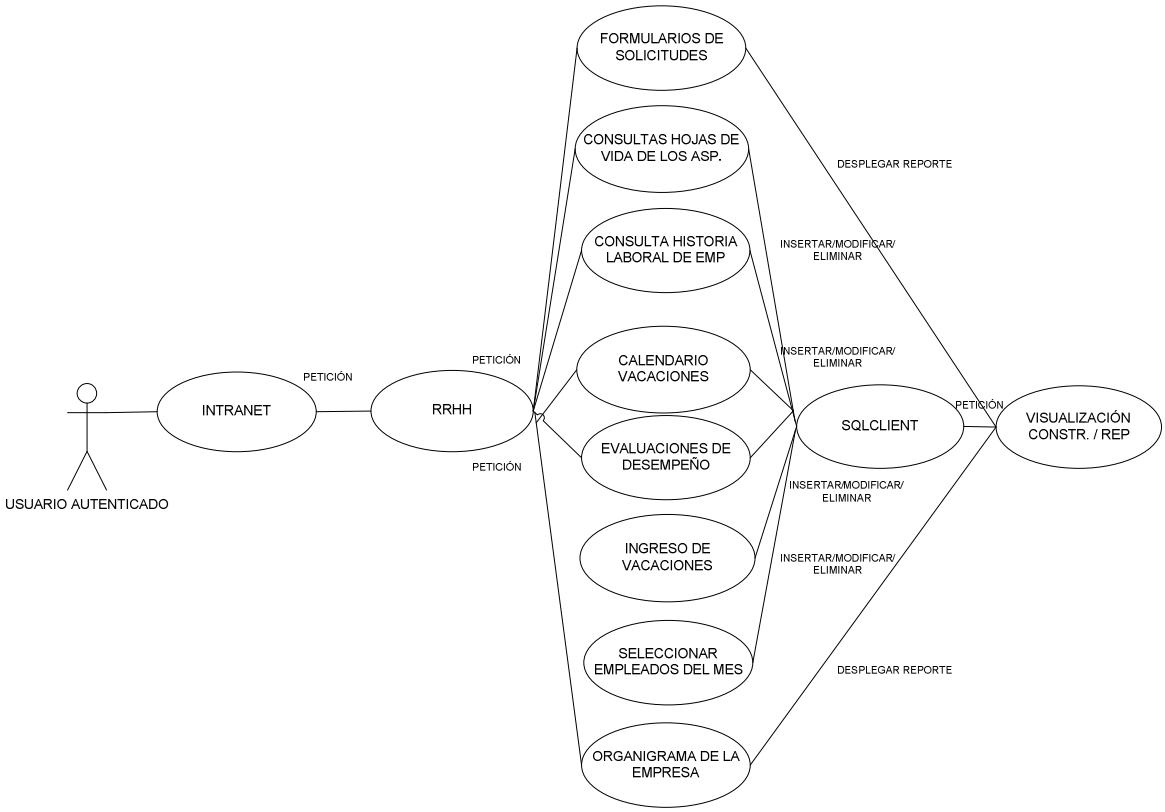

Figura 4-5: Diagrama de Casos de Uso de Nivel 2: Intranet / RRHH
Fuente: Las Autoras.

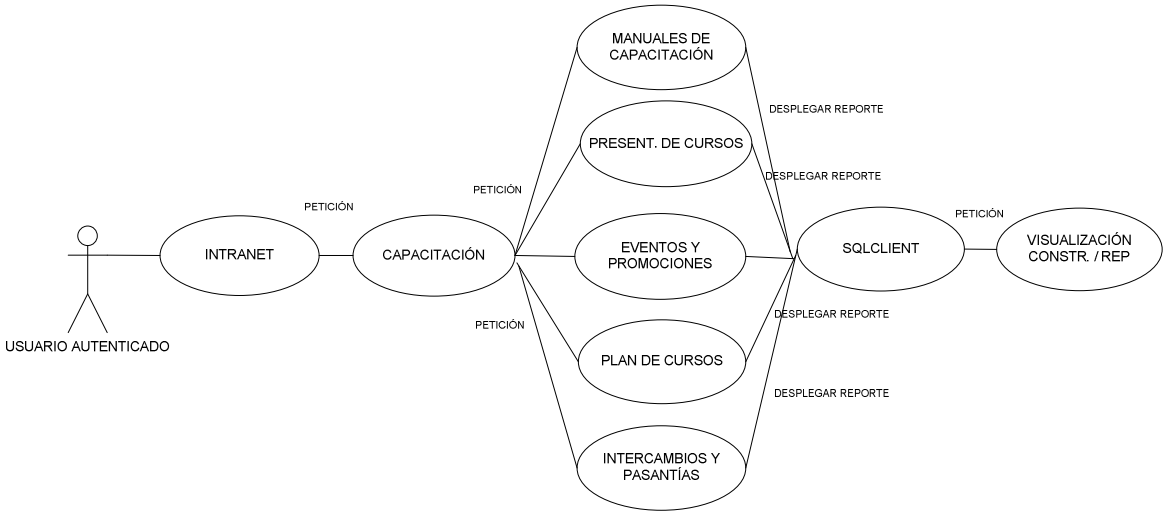

Figura 4-6: Diagrama de Casos de Uso de Nivel 2: Intranet / Capacitación
Fuente: Las Autoras

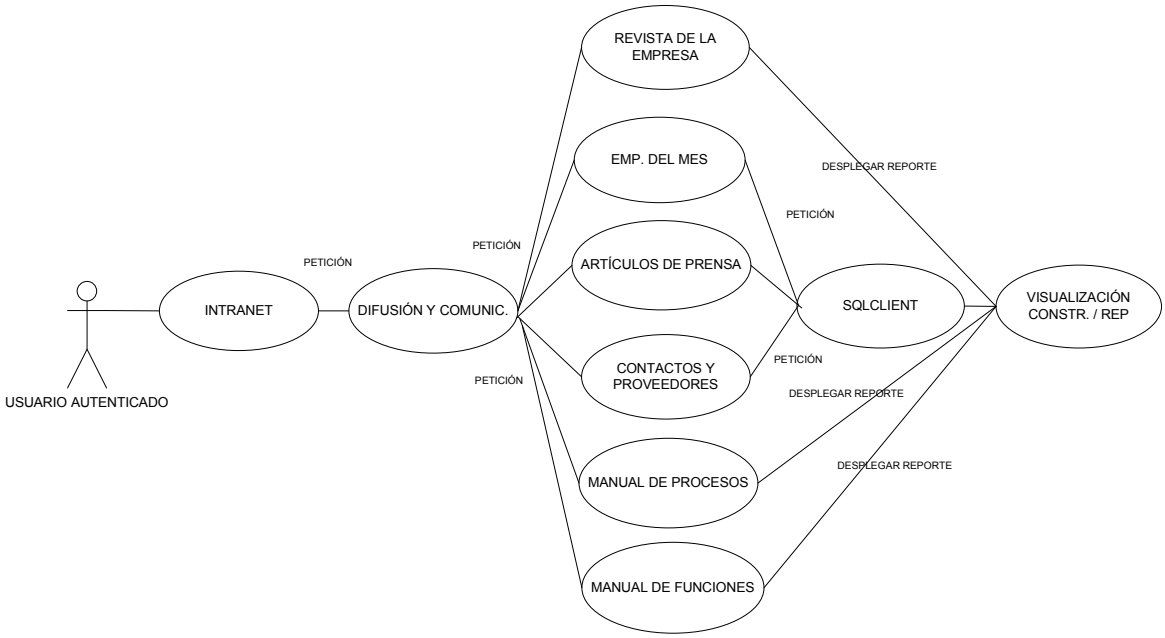

Figura 4-7: Diagrama de Casos de Uso de Nivel 2: Intranet / Difusión y Comunicación
Fuente: Las Autoras.

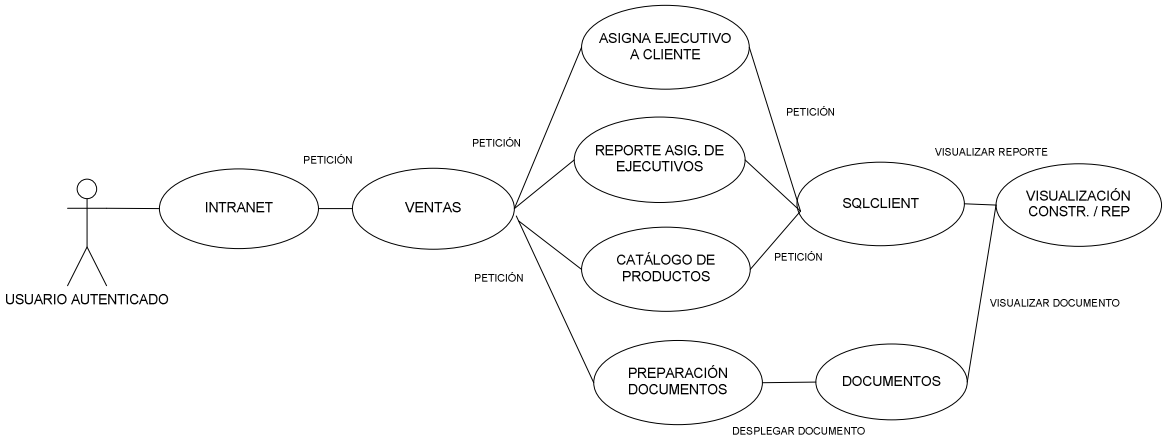

Figura 4-8: Diagrama de Casos de Uso de Nivel 2: Intranet / Ventas
Fuente: Las Autoras

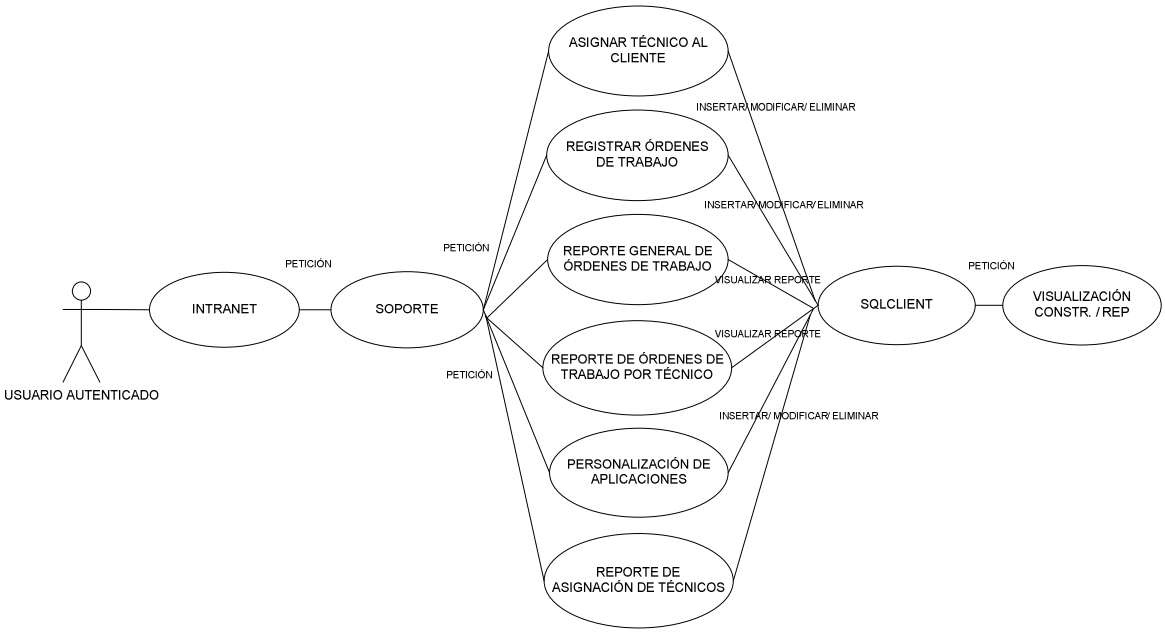

Figura 4-9: Diagrama de Casos de Uso de Nivel 2: Intranet / Soporte
Fuente: Las Autoras.

4.1.1.3 Diagrama de Casos de Uso: Extranet

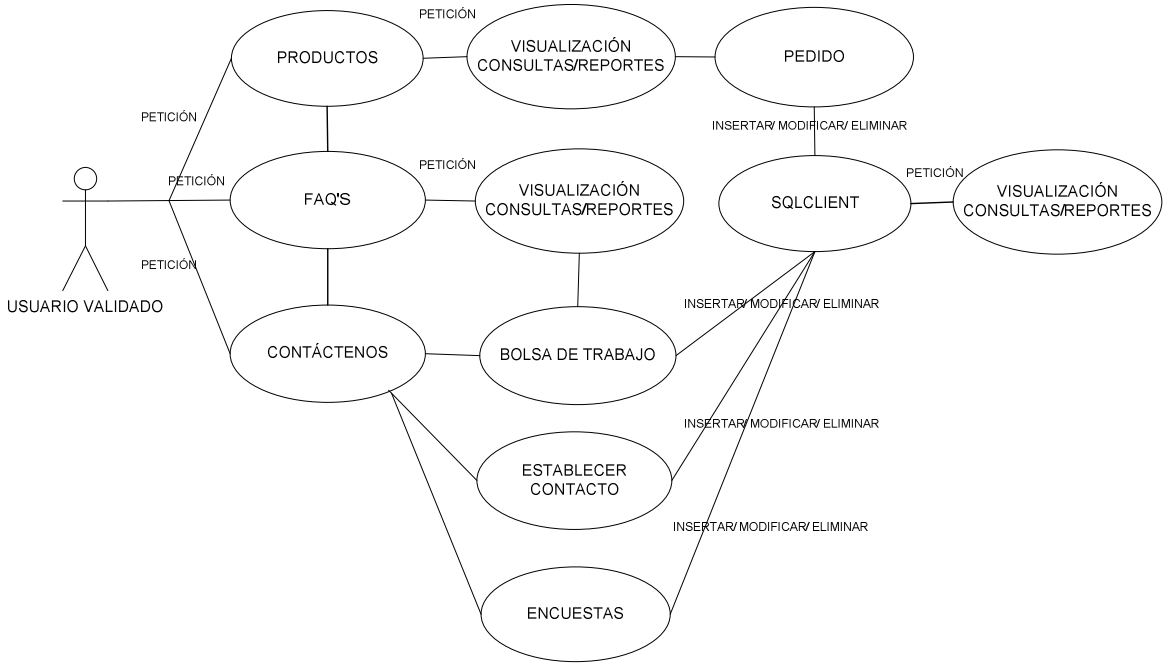

Figura 4-10: Diagrama de Casos de Uso de Nivel 2: Extranet
Fuente: Las Autoras

4.1.1.4 Diagrama de Casos de Uso: Administración

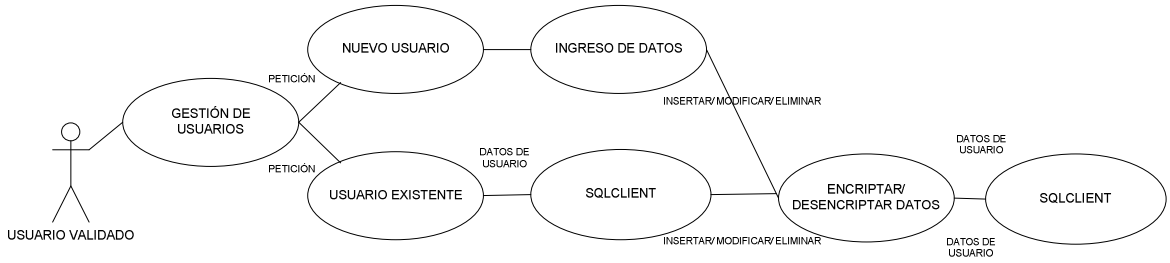

Figura 4-11: Diagrama de Casos de Uso de Nivel 2: Administración
Fuente: Las Autoras.

4.1.2 ANÁLISIS

4.1.2.1 Diagrama de Colaboración: Autenticación

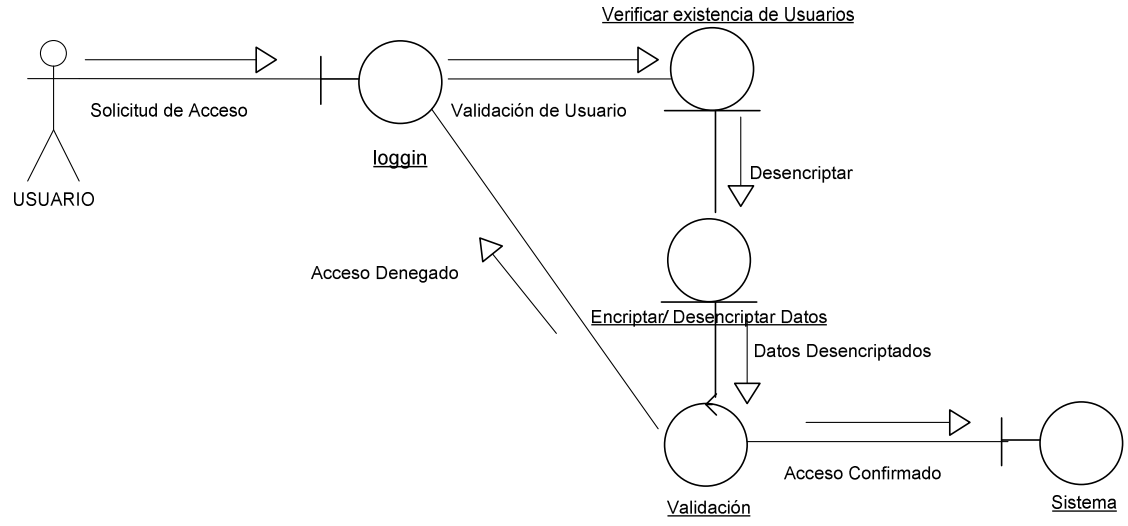

Figura 4-12: Diagrama de Colaboración Caso de Uso: Autenticación
Fuente: Las Autoras.

4.1.2.2 Diagramas de Colaboración: Intranet

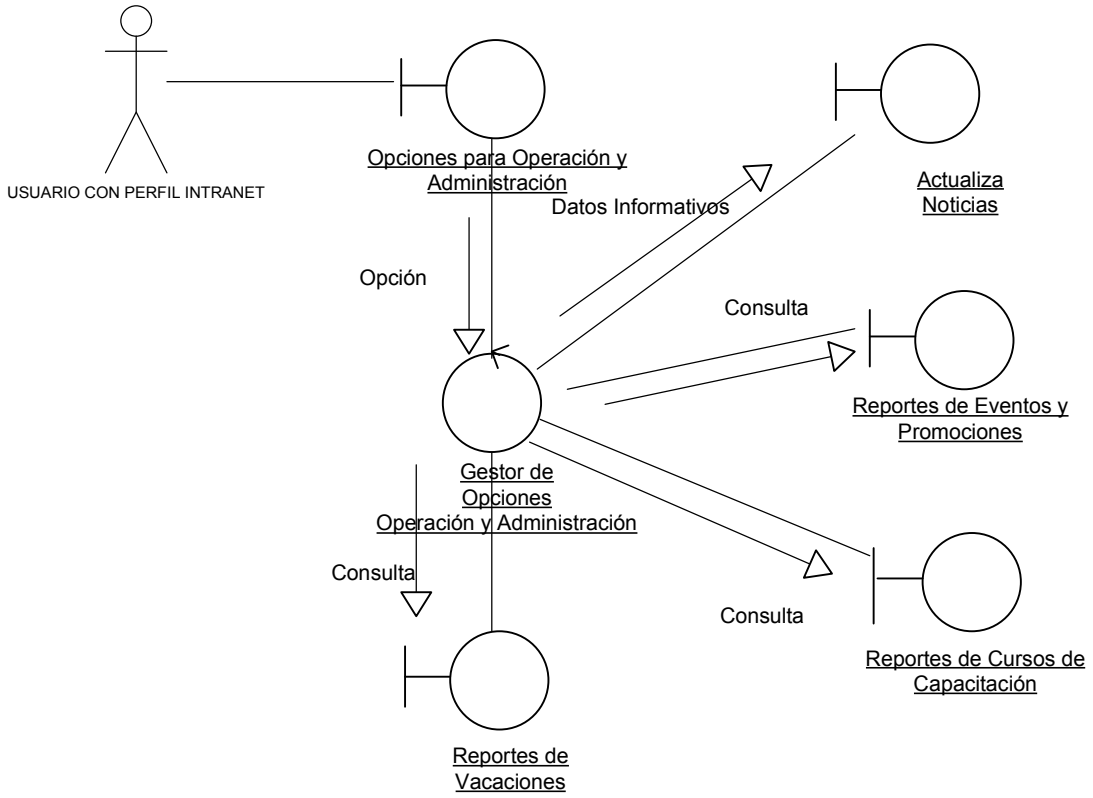

Figura 4-13: Diagrama de Colaboración Caso de Uso: Intranet / Operación y Administración
Fuente: Las Autoras

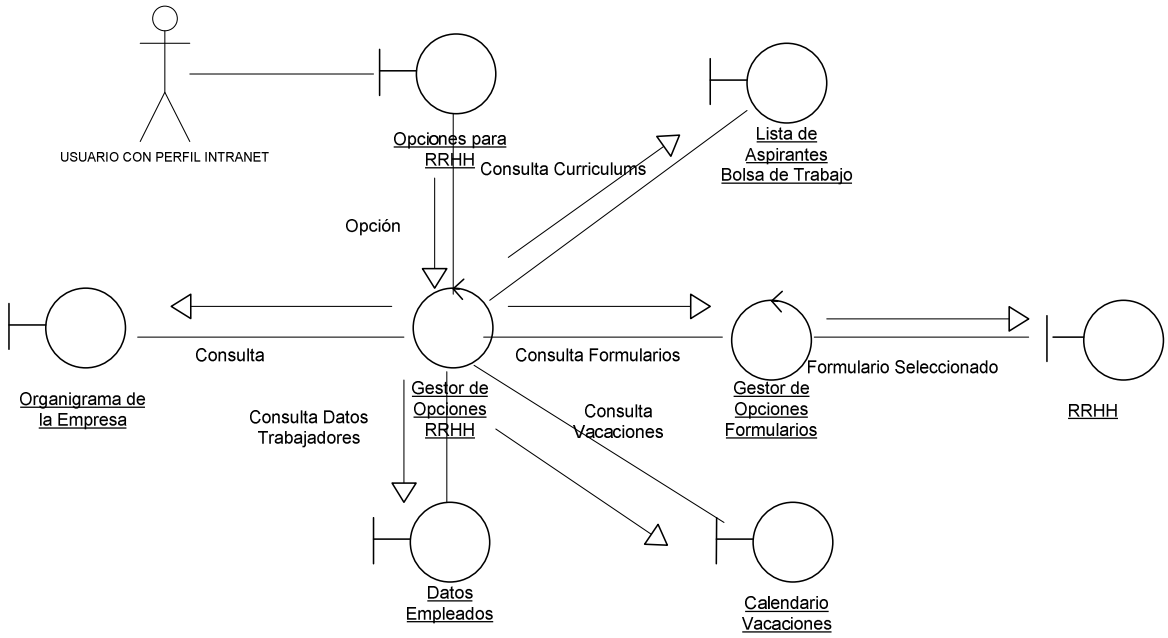

Figura 4-14: Diagrama de Colaboración Caso de Uso: Intranet / RRHH
Fuente: Las Autoras.

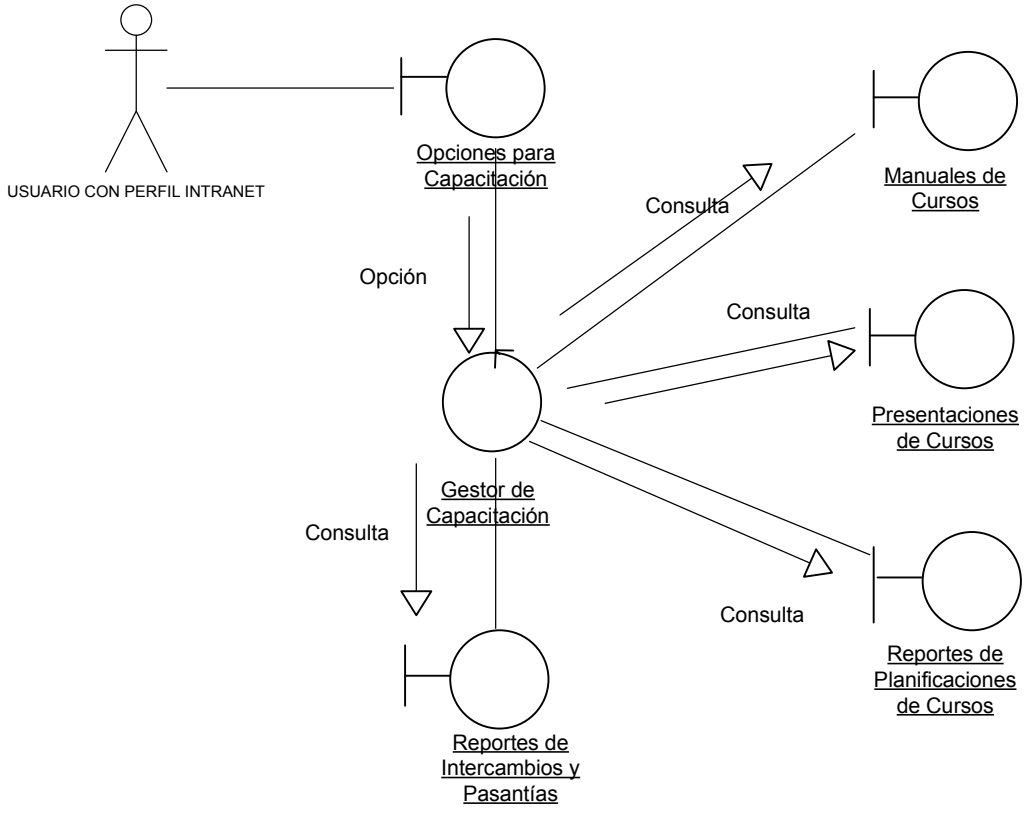

Figura 4-15: Diagrama de Colaboración Caso de Uso: Intranet / Capacitación
Fuente: Las Autoras.

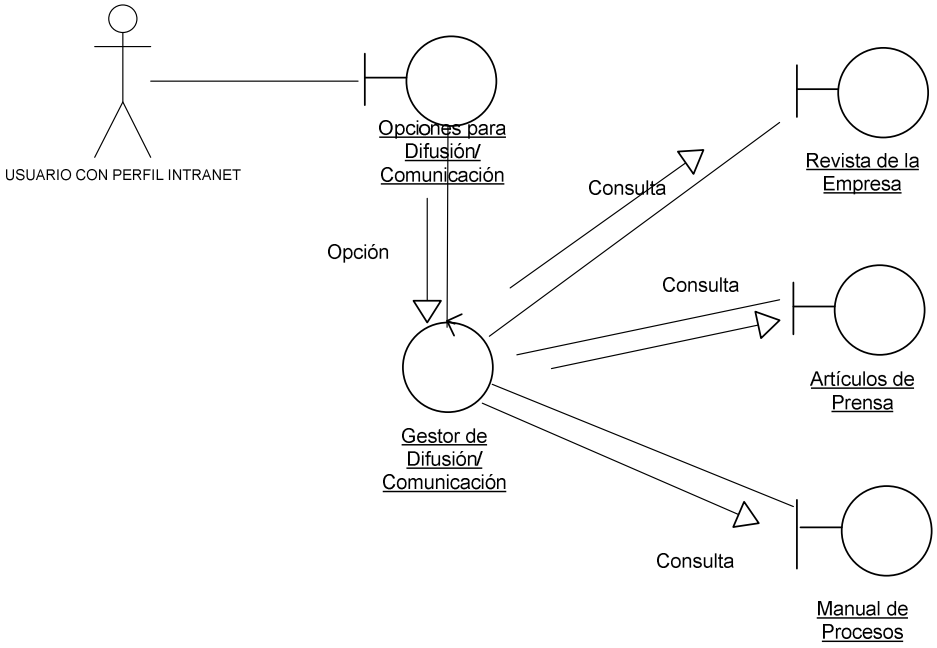

Figura 4-16: Diagrama de Colaboración Caso de Uso: Intranet / Difusión y Comunicación
Fuente: Las Autoras

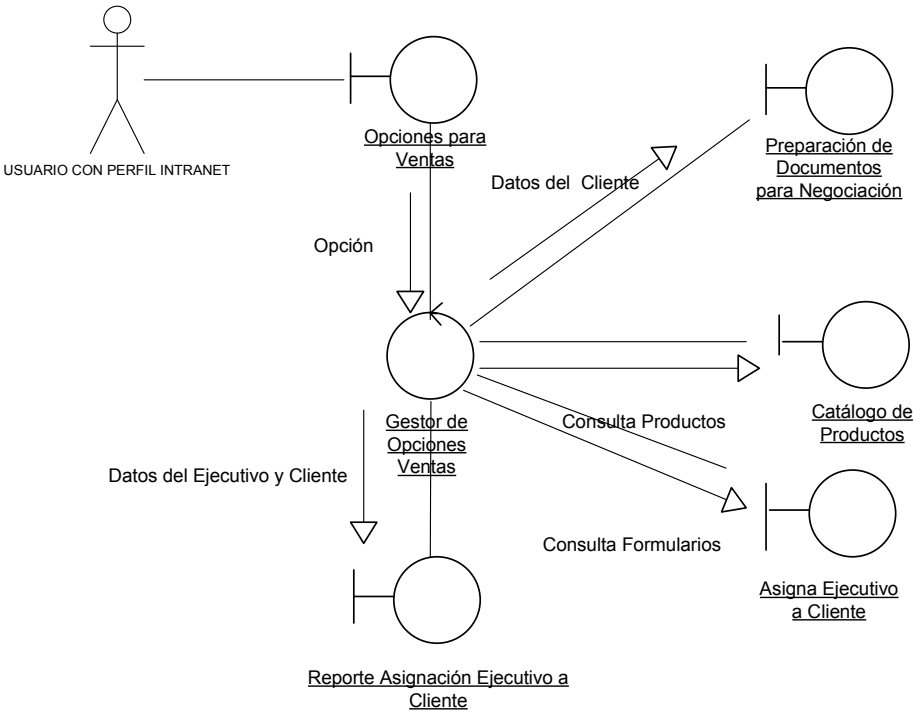

Figura 4-17: Diagrama de Colaboración Caso de Uso: Intranet / Ventas
Fuente: Las Autoras.

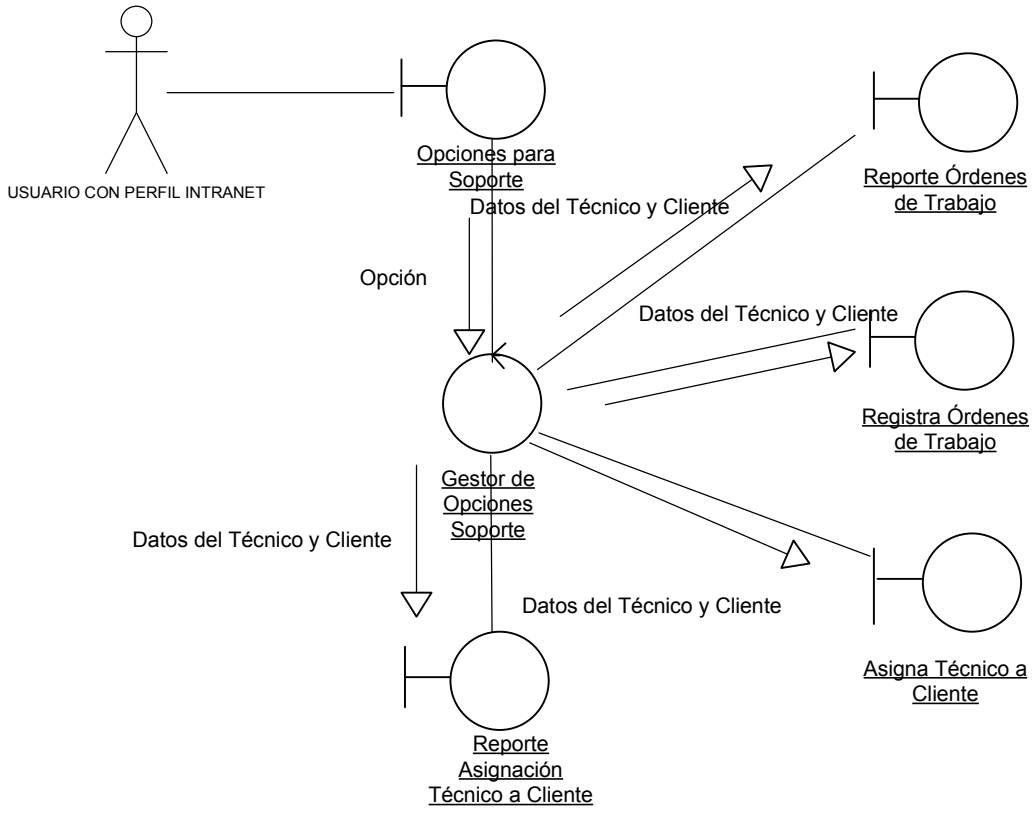

Figura 4-18: Diagrama de Colaboración Caso de Uso: Intranet / Soporte
Fuente: Las Autoras

4.1.2.3 Diagramas de Colaboración: Extranet

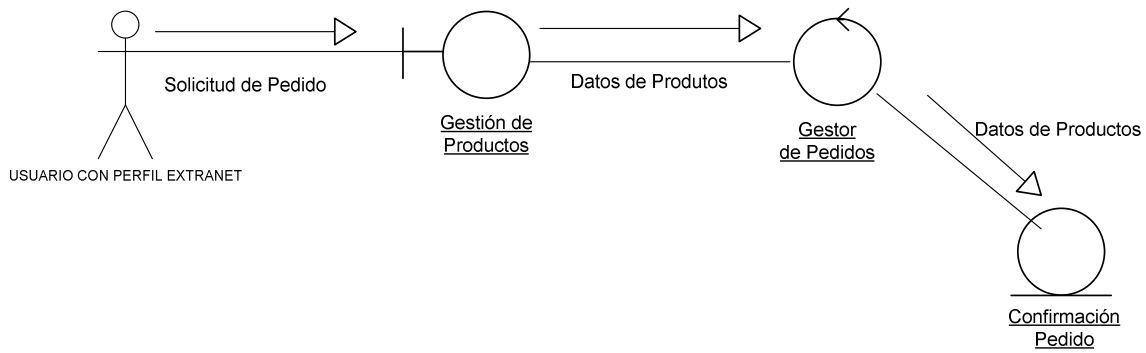

Figura 4-19: Diagrama de Colaboración Caso de Uso: Extranet / Productos
Fuente: Las Autoras.

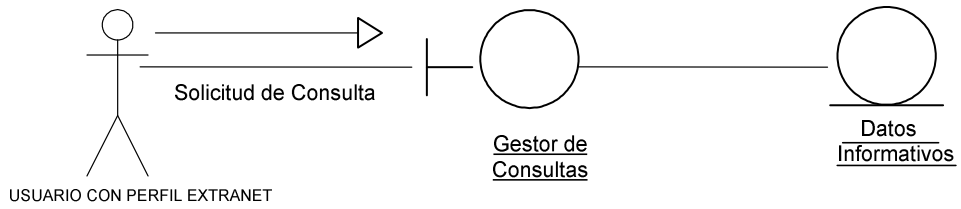

Figura 4-20: Diagrama de Colaboración Caso de Uso: Extranet / Faq's
Fuente: Las Autoras.

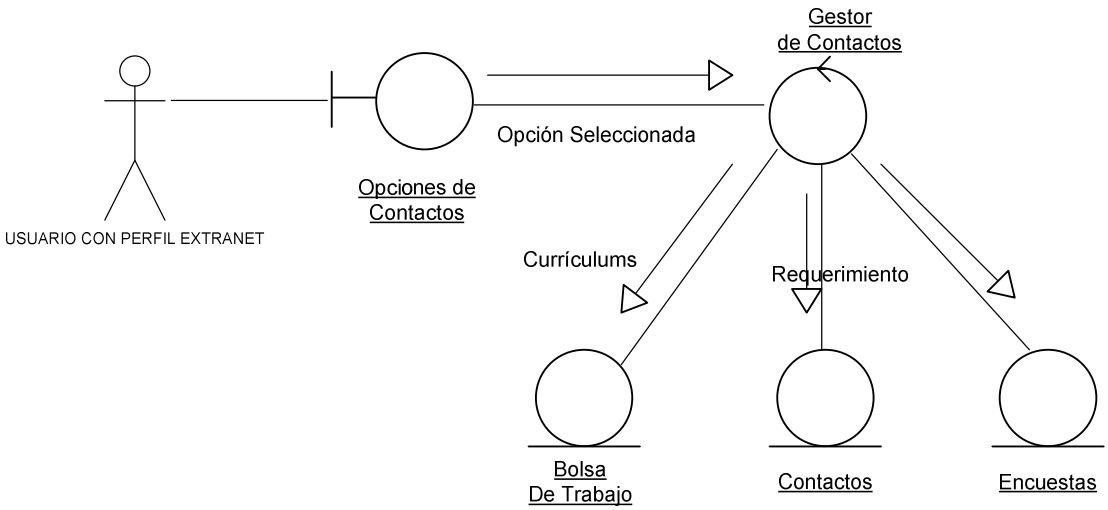

Figura 4-21: Diagrama de Colaboración Caso de Uso: Extranet / Contáctese con Nosotros
Fuente: Las Autoras.

4.1.2.4 Diagrama de Colaboración: Administración

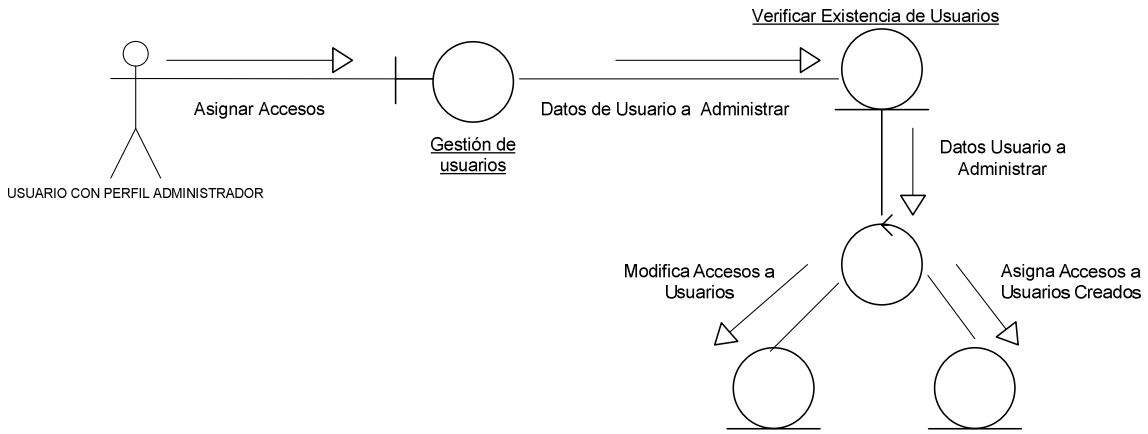

Figura 4-22: Diagrama de Colaboración Caso de Uso: Administración
Fuente: Las Autoras.

4.2 DISEÑO DE LA SOLUCIÓN

4.2.1 DISEÑO LÓGICO

4.2.1.1 Diagrama de Secuencia: Autenticación

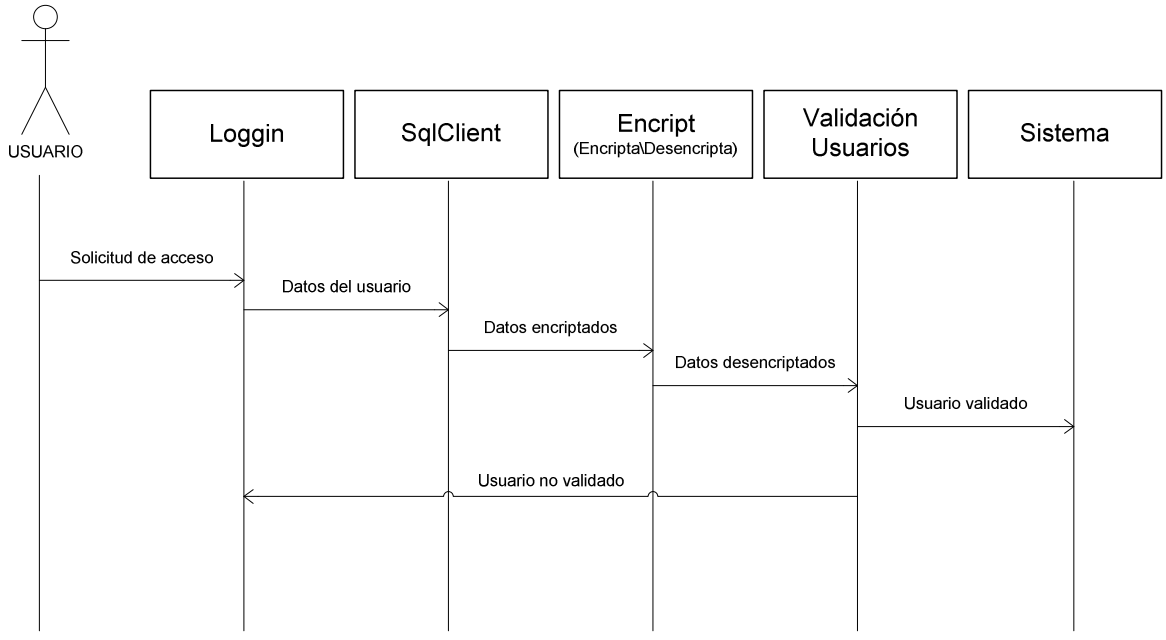

Figura 4-23: Diagrama de Secuencia Caso de Uso: Autenticación
Fuente: Las Autoras.

4.2.1.2 Diagramas de Secuencia: Intranet

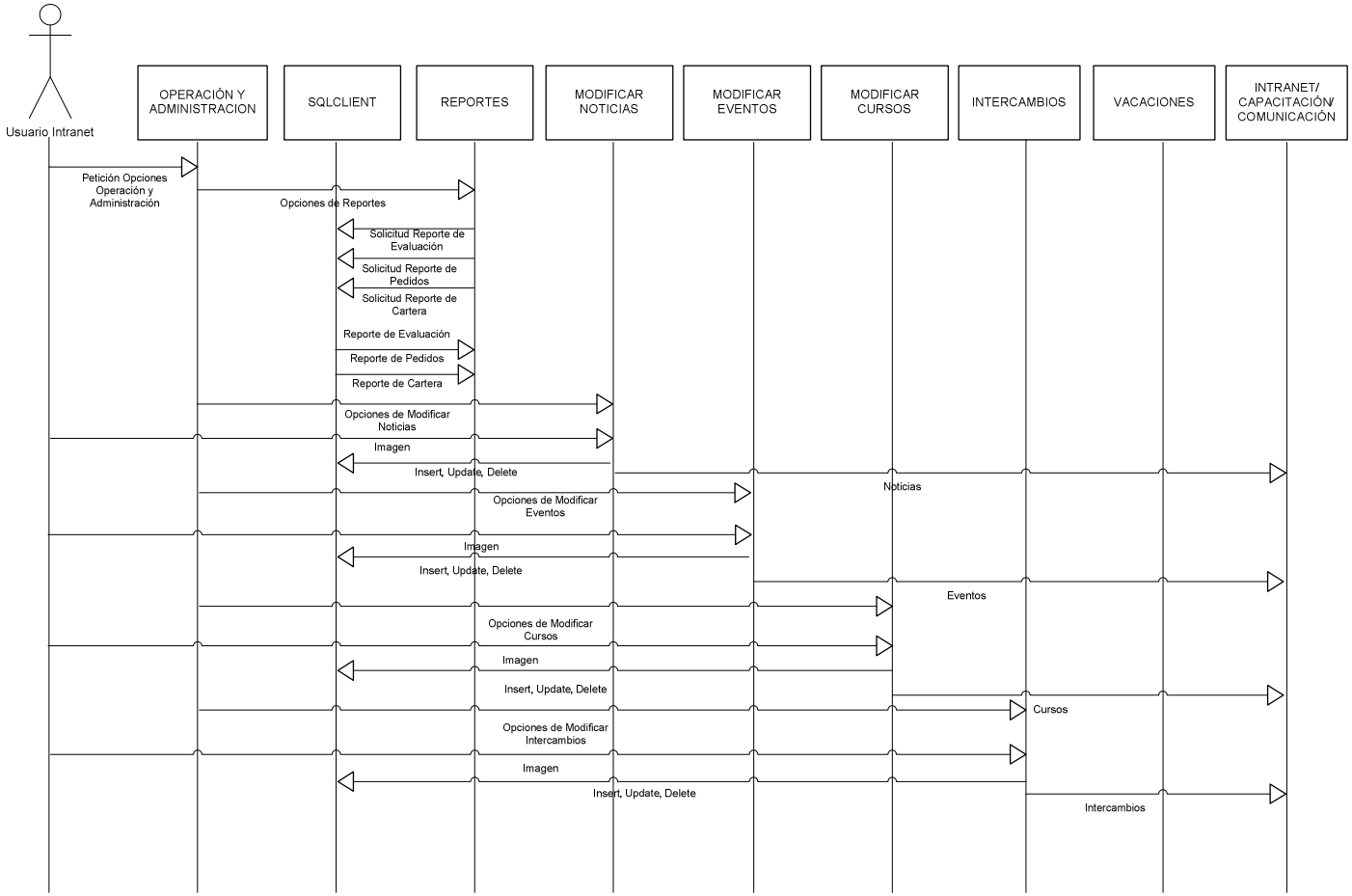

Figura 4-24: Diagrama de Secuencia Caso de Uso: Intranet / Operación y Administración
Fuente: Las Autoras.

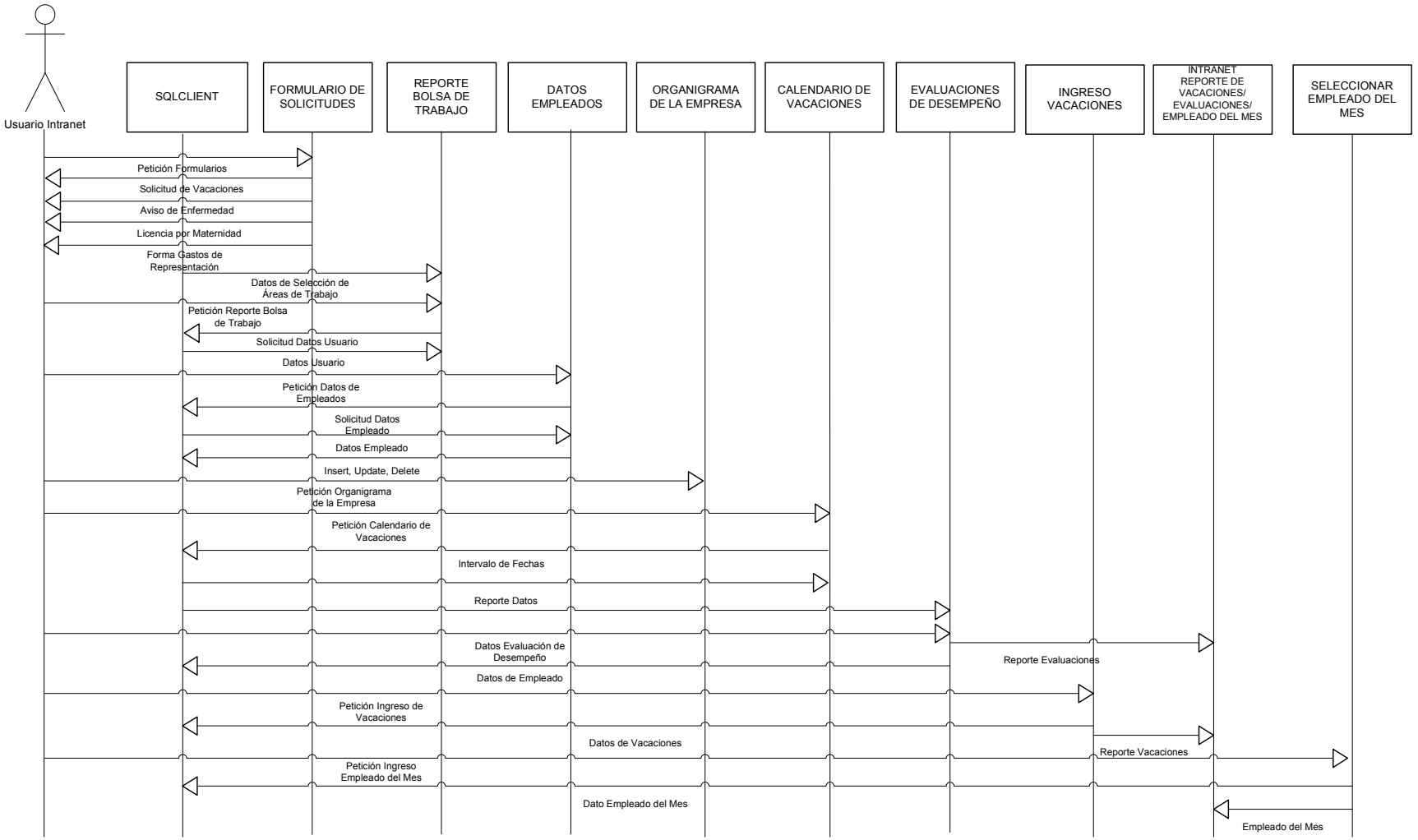

Figura 4-25: Diagrama de Secuencia Caso de Uso: Intranet / RRHH
Fuente: Las Autoras

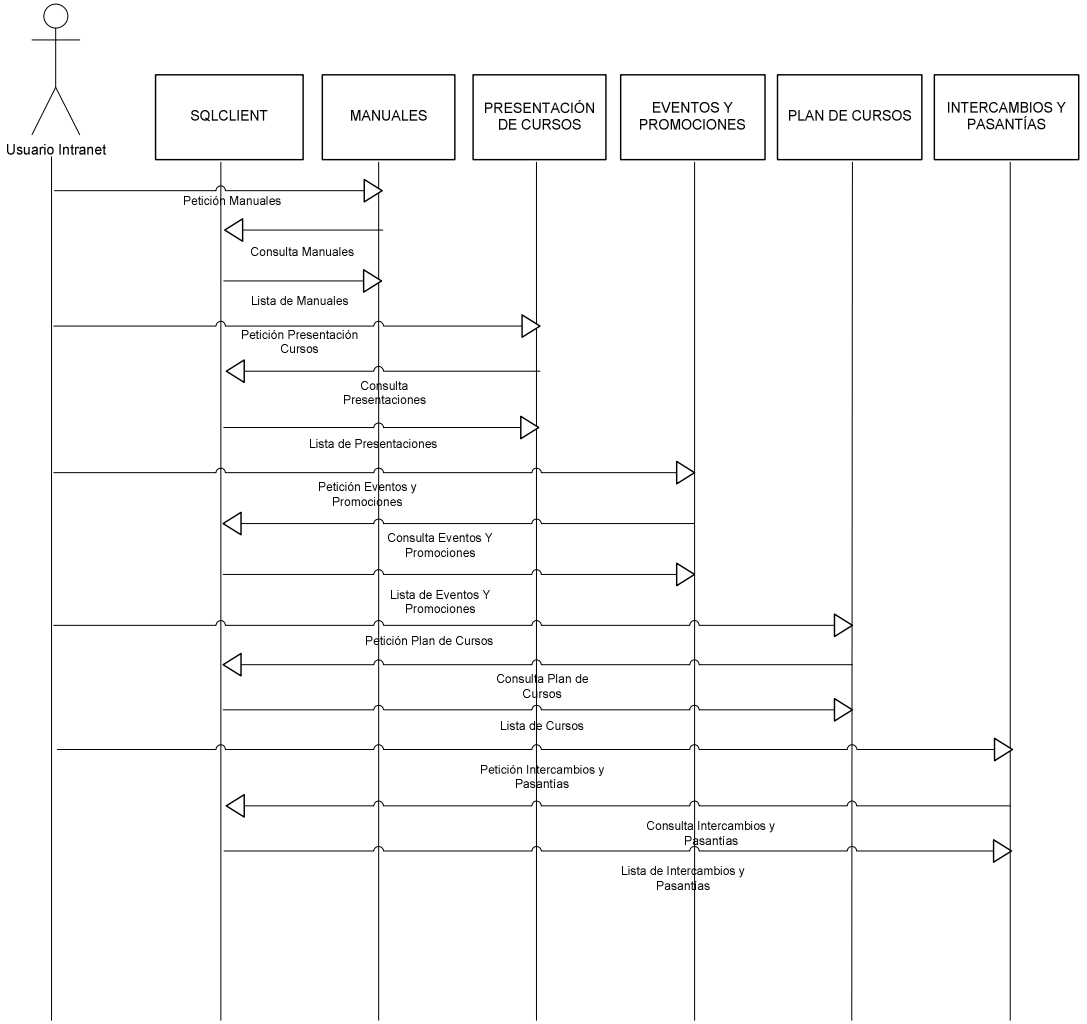

Figura 4-26: Diagrama de Secuencia Caso de Uso: Intranet /Capacitación
Fuente: Las Autoras

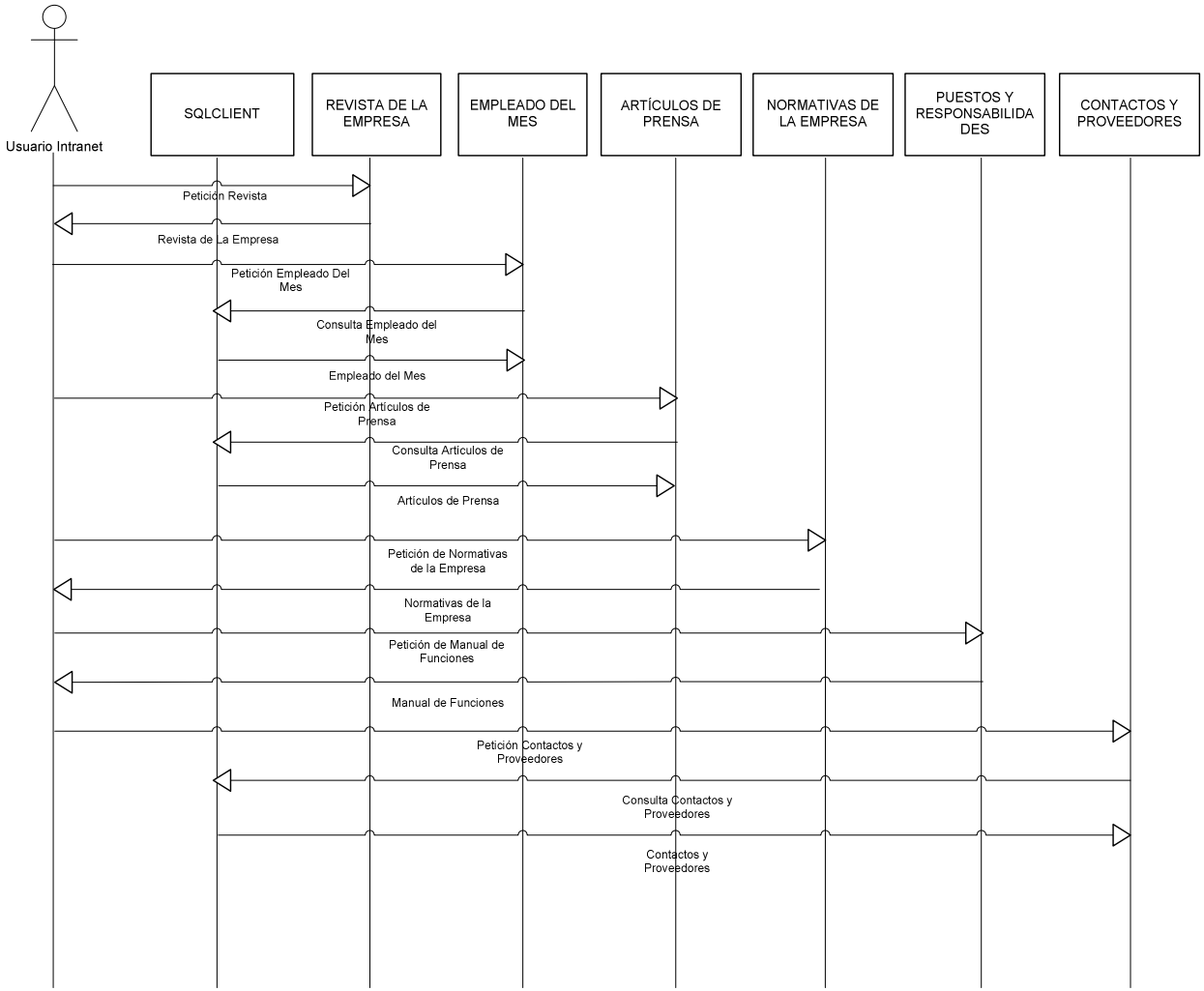

Figura 4-27: Diagrama de Secuencia Caso de Uso: Intranet / Difusión y Comunicación
Fuente: Las Autoras

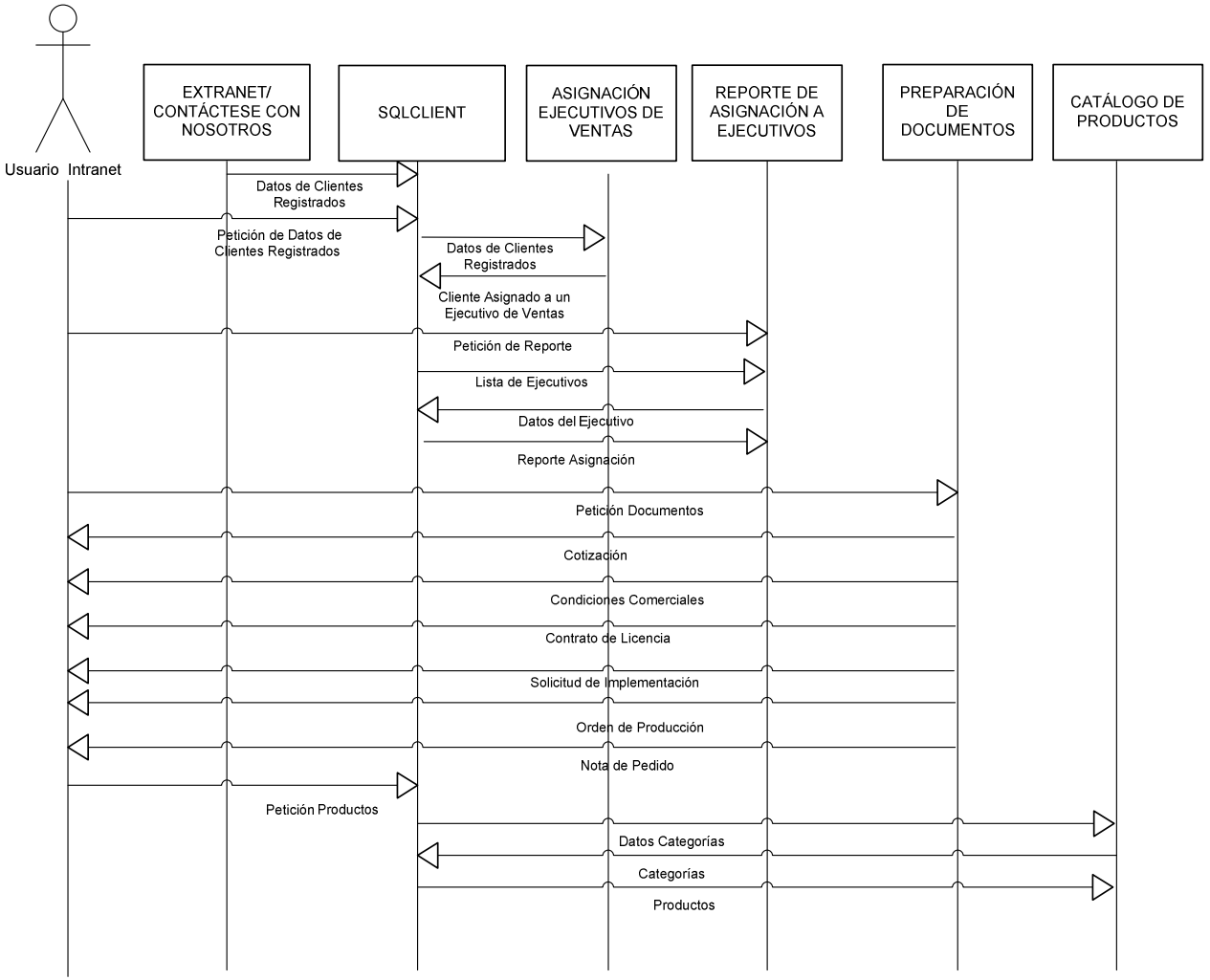

Figura 4-28: Diagrama de Secuencia Caso de Uso: Intranet / Ventas
Fuente: Las Autoras

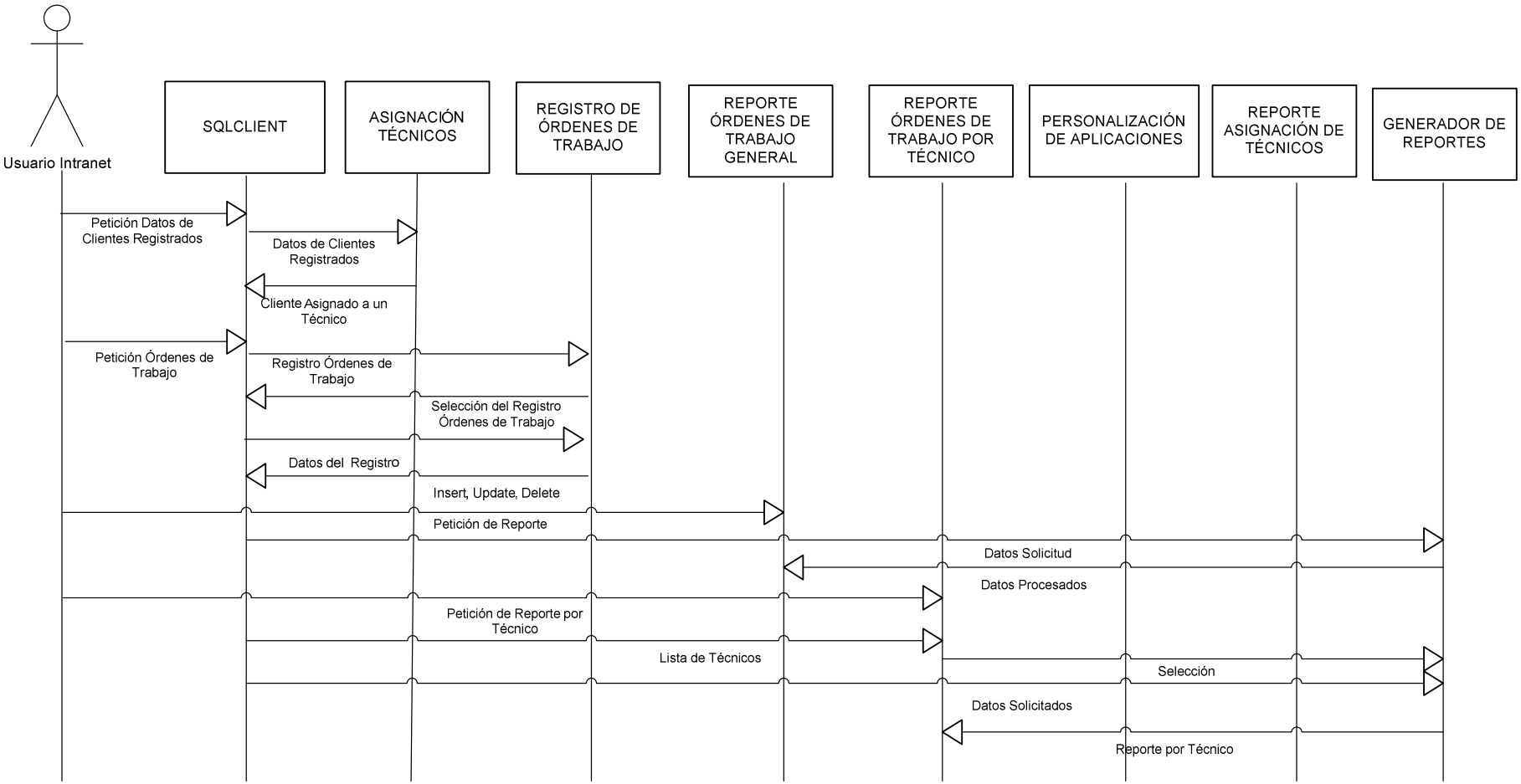

Figura 4-29: Diagrama de Secuencia Caso de Uso: Intranet / Soporte
Fuente: Las Autoras

4.2.1.3 Diagrama de Secuencia: Extranet

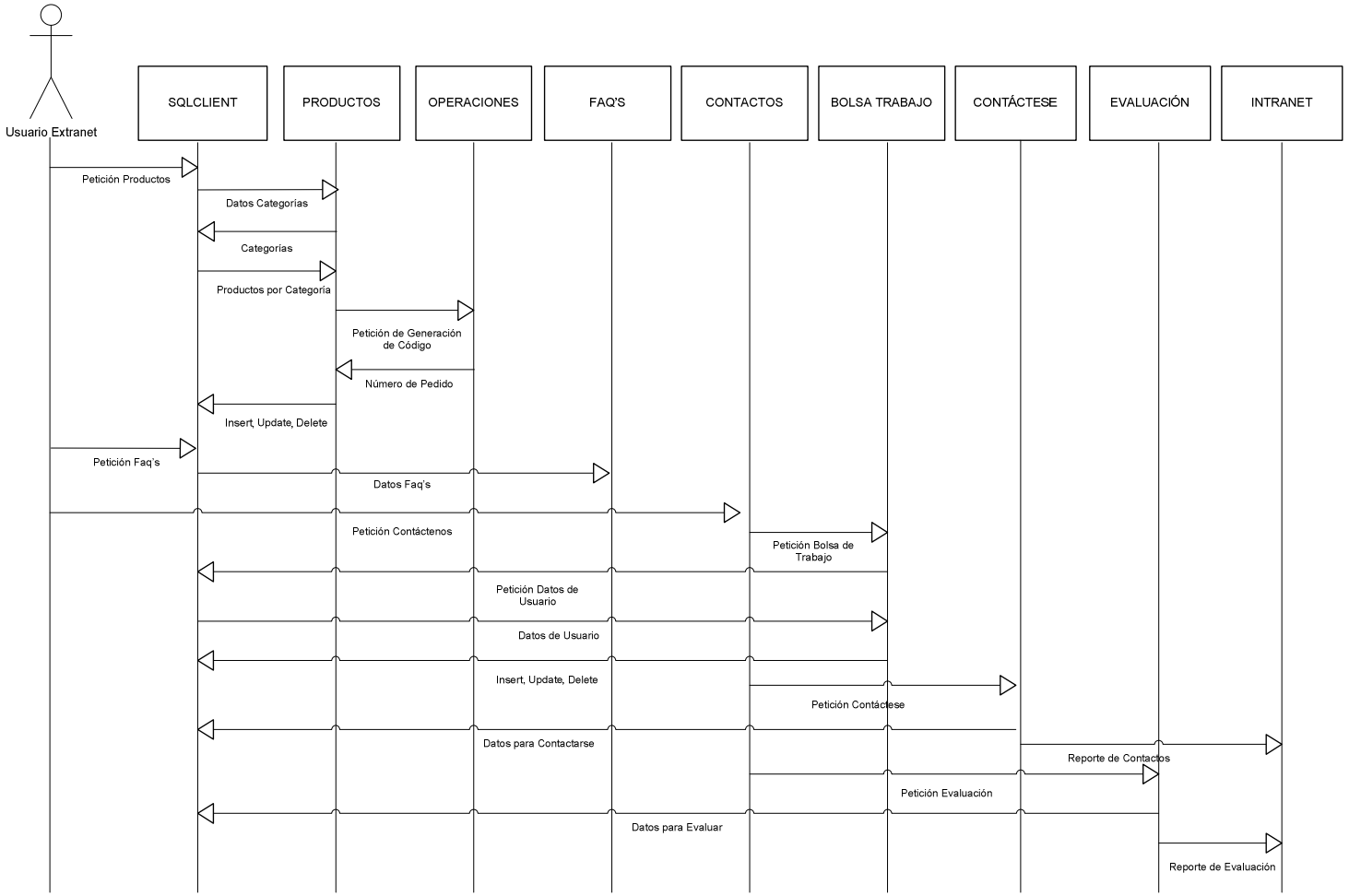

Figura 4-30: Diagrama de Secuencia Caso de Uso: Extranet
Fuente: Las Autoras

4.2.1.4 Diagrama de Secuencia: Administración

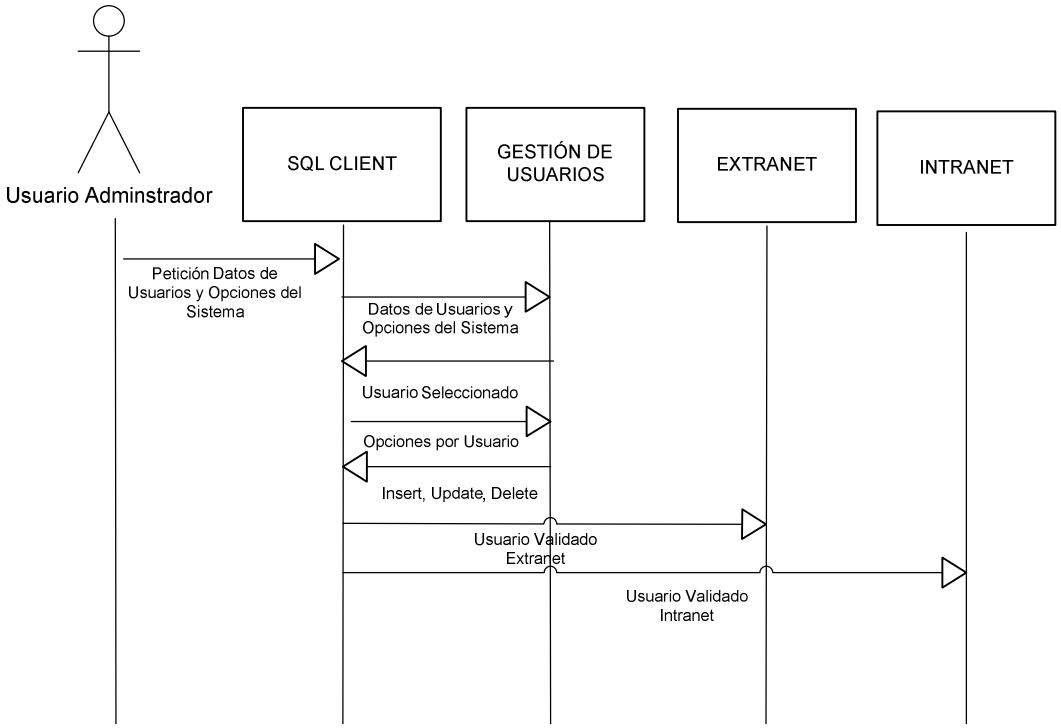

Figura 4-31: Diagrama de Secuencia Caso de Uso: Administración
Fuente: Las Autoras

4.2.2 DISEÑO FÍSICO

El diseño físico de la Intranet / Extranet muestra la estructura y la distribución de los dispositivos que conforman la red, esta dividida en dos secciones: Intranet y Extranet como se muestras en la figura 4-33 “Diseño Físico”.

4.2.2.1 Intranet

Para el presente proyecto se plantea un diseño físico enfocado en el concepto de arquitectura de red segura basado en el diseño de una DMZ. Una DMZ es una red adicionada entre una red protegida y una red externa, con la finalidad de proveer un nivel de seguridad adicional a la información crítica de la empresa.

La DMZ estará limitada por dos servidores firewall con ISA server (Internet Security and Acelerator), configurados sobre las máquinas Poliant ML150 G4 con sistema operativo Windows 2003 Server.

- El primero constituye el firewall de frontera, con funciones de proxy y router
- El segundo como firewall interno con funciones de proxy y servidor VPN.

Dentro de la DMZ estará un servidor con Windows 2000 Server sobre el que se levantará el servidor Web IIS (Internet Information Server) además de SQL 2000 con una réplica parcial de la base de datos interna todo sobre una máquina Proliant ML350 G2.

En la parte interna se dispondrá de dos servidores adicionales ML350 G3 los que se configurarán como:

- El primero como servidor de DNS, DHCP, correo con Exchange, sobre el sistema operativo Windows 2000 Server.
- El segundo como servidor de Base de Datos con SQL 2000 con sus respectivas licencias, sobre el sistema operativo Windows 2000 Server. Aquí también se instalará el Antivirus Symantec Corporated Edition.

El acceso de los usuarios a la intranet es a través del browser con el siguiente URL: https://192.168.100.1/Emcosoft.

4.2.2.2 Extranet

El proveedor del servicio de banda ancha en este caso Satnet, se encargará del apuntamiento de dominio para correo y Web hacia el firewall de frontera.

En la parte externa tenemos dos tipos de usuarios:

- Por un lado tenemos los usuarios con perfil de Extranet que acceden a través de una conexión SSL de la siguiente forma: https://200.200.10.15/Emcosoft.
- Por otro lado los usuarios remotos con perfil de Intranet, que acceden a través de una conexión VPN de la siguiente forma: https://10.10.10.2/Emcosoft.

En la siguiente página se muestra la figura con el diseño físico

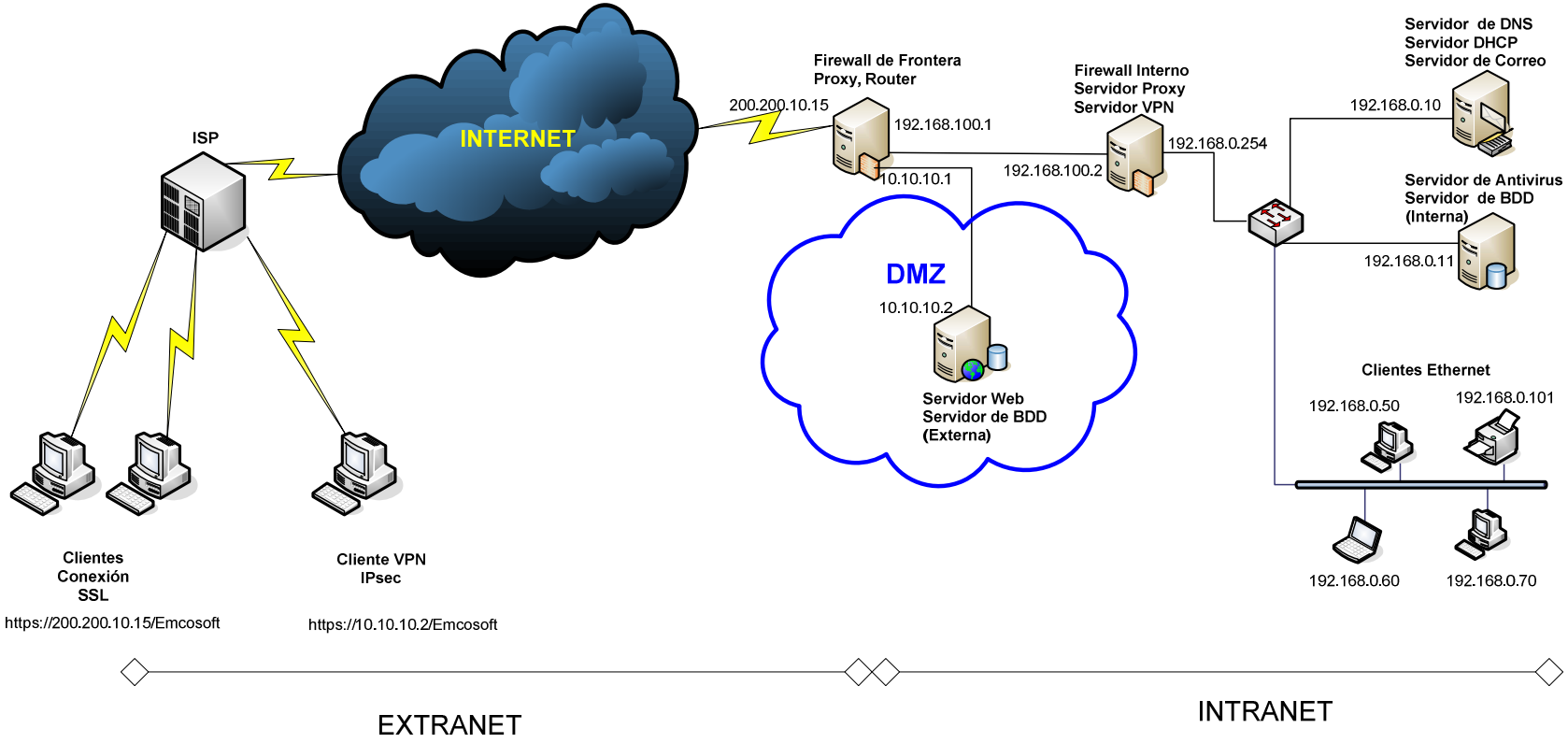

Figura 4-32: Diseño Físico
Fuente: Las Autoras

4.3 IMPLEMENTACIÓN DE LA SOLUCIÓN.

La Intranet/Extranet estará implementada por medio del un sistema Web, que permitirá sistematizar algunas actividades manuales, mejorar la interfaz con el usuario de algunas opciones que se realizan por medio del ERP. Las cuales ahora se pueden efectuar por medio del un sistema Web desarrollado para este propósito. En el diseño del proyecto se determinó la estructura del sistema Web el mismo que inicialmente divide a los usuarios en tres grupos con sendos perfiles:

- Usuario con perfil de Administrador.
- Usuario con perfil de Intranet.
- Usuario con perfil de Extranet.

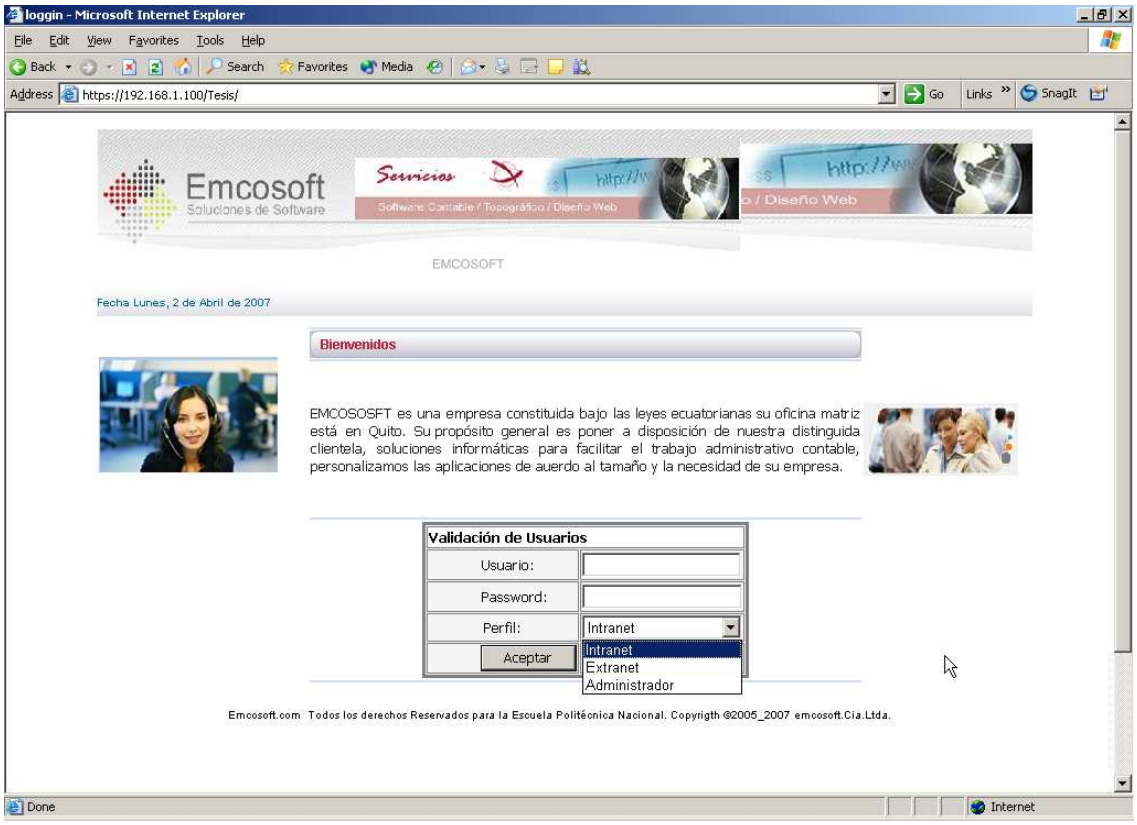

Figura 4-334: Interfaz
Fuente: Las Autoras

Cada uno de estos usuarios tiene opciones de menú desplegadas en la parte lateral izquierda de la página principal. Estas opciones a su vez tienen submenús, que se despliegan en la parte lateral derecha.

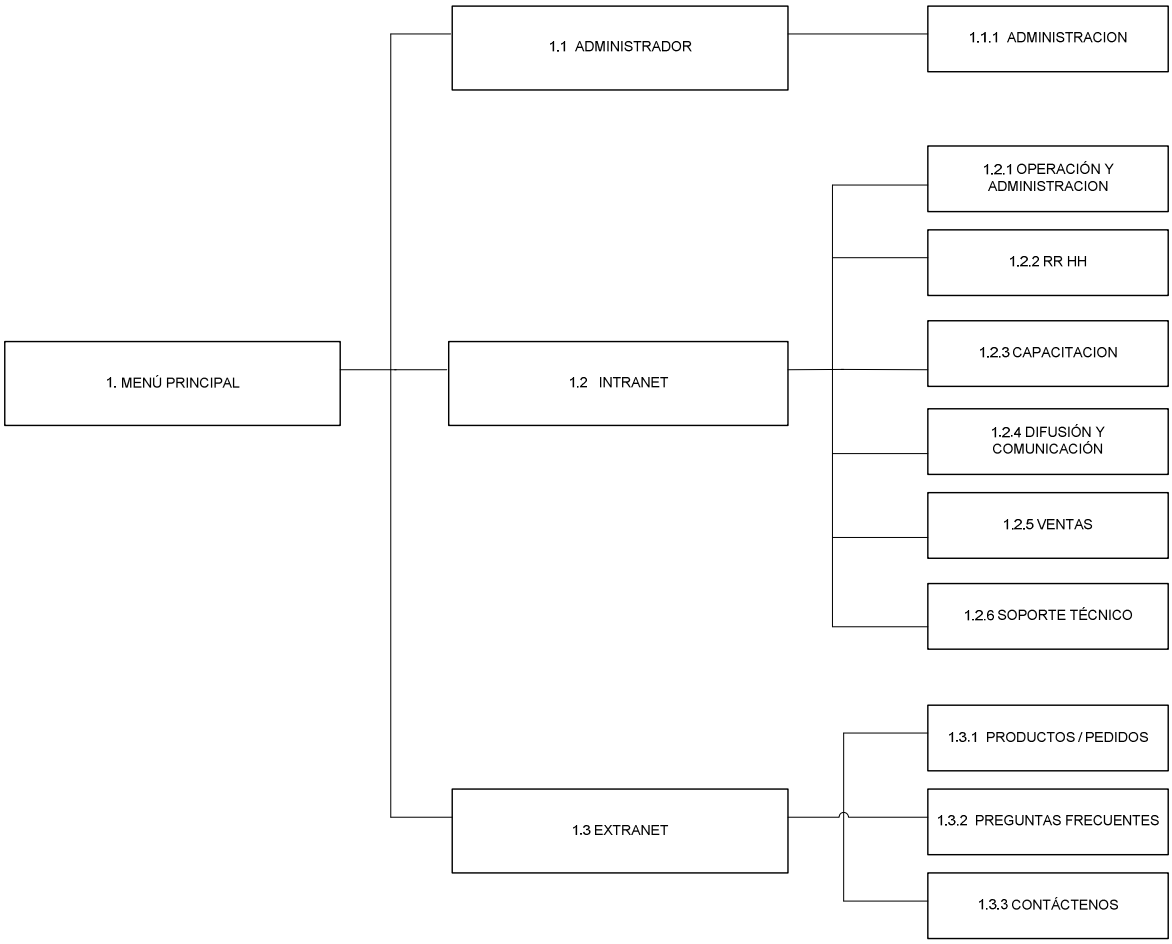

Figura 4-345: Opciones del Sistema
Fuente: Las Autoras

Es en los submenús donde se encuentran distribuidas las diferentes operaciones a las que los usuarios tienen acceso, y que se detallan a continuación.

4.3.1 FUNCIONALIDADES DEL PERFIL DE ADMINISTRADOR

Usuario: el usuario con perfil de administrador del sistema es la persona que tiene la autorización para realizar la Gestión de Usuarios. Específicamente el Jefe de Informática.

Opciones de Menú:

4.3.1.1 Administración

- Crear y Eliminar Usuarios
- Modificar los Permisos de Acceso a Opciones del Sistema.

4.3.1.1.1 Crear y Eliminar Usuarios.

Para realizar estas actividades el administrador requiere información escrita, documentación como: Nombramientos o Contratos de Trabajo para perfiles de Intranet, proporcionados por RRHH ó cartas de Clientes Calificados para acceder al entorno de Extranet, proporcionado por el Departamento de Ventas. El administrador registra esta información en el módulo del sistema Web destinado para este efecto, un formulario al que se accede seleccionando la opción de menú *Administración*, y luego el submenú *Gestión de Usuarios*. En la parte final tenemos el botón *Nuevo* que habilita un formulario en blanco que permite ingresar los datos de un nuevo usuario. Al final se debe presionar el botón *Guardar.*

Como resultado de esta operación, se entrega verbalmente un nombre de usuario, password y perfil con el que tendrá acceso a las diferentes opciones que se le ha autorizado. Adicionalmente, el sistema mantiene el registro de esta información para que el usuario disponga de las opciones asignadas a su perfil cuando acceda al sistema.

Para eliminar usuarios se debe seleccionar del menú desplegable el usuario y a continuación presionar el botón *Eliminar*

4.3.1.1.2 Modificar los Permisos de Acceso a Opciones del Sistema.

Para realizar esta operación, el administrador precisa de una solicitud verbal o escrita del requerimiento, donde se determinen las opciones del sistema a las cuales necesita tener acceso un determinado usuario. Esta solicitud es realizada por un jefe de departamento para si o para un subalterno. El administrador efectúa el cambio en el sistema ingresando a la opción de menú *Administración*, y luego al submenú *Gestión de Usuarios.* Este formulario presenta en la parte superior un menú desplegable del cual se debe escoger el usuario al que se le va a modificar las opciones, y al final se dispone del botón *Modificar,* que habilita las alternativas disponibles según el perfil seleccionado, una vez realizada la selección de las posibilidades, se debe presionar el botón *Guardar* para almacenar los cambios. Como resultado el usuario tiene acceso a las opciones asignadas.

4.3.2 FUNCIONALIDADES DEL PERFIL DE EXTRANET

Usuario: el usuario con perfil de Extranet es un cliente que ha sido calificado para acceder al entorno de Extranet por el jefe del departamento de Ventas mediante una carta de Cliente Calificado.

Opciones de Menú:

4.3.2.1 Catálogo de Productos:

- Descargar Información más Detallada
- Registrar Solicitudes de Pedidos de Compra
- Eliminar Solicitudes de Pedidos de Compra

4.3.2.1.1 Descargar Información más Detallada.

Para efectuar esta operación, el usuario debe hacer una solicitud al sistema. Para lo cual debe ingresar a la opción de *Productos*, escoger una categoría del menú desplegable, bajo la etiqueta *Download Brochure*, aquí encontrará los nombres de los productos en formato de links y dar clic en programa que le interese. Esta

solicitud es procesada por el sistema Web, que como respuesta le presenta una pantalla con la información solicitada, una hoja con especificaciones técnicas en formato pdf.

4.3.2.1.2 Registrar Solicitudes de Pedidos de Compra

Para registrar una solicitud de pedido de compra, el usuario debe hacer una petición al sistema. Para esto debe ingresar a la opción de *Productos*, escoger una categoría del menú desplegable, bajo la etiqueta *Hacer Pedido*, deberá seleccionar los productos que desee comprar, y a continuación hacer clic en la figura del carrito de compras.

Esta solicitud es aceptada por el sistema Web, que inmediatamente muestra en la parte inferior de la pantalla, los datos personales del cliente y una tabla con el detalle de los artículos seleccionados, en esta tabla se muestra el campo *Modificar* bajo el cual está una etiqueta *Edición* en formato de link, que permite al usuario cambiar la cantidad de productos que desea comprar, luego de esto debe seleccionar la etiqueta *Actualizar*.

El sistema procesa la solicitud con toda la información recibida y responde seguidamente al usuario de Extranet, con un mensaje que indica "*Pedido Actualizado Correctamente"*. Adicionalmente, el sistema Web alimenta a un ERP (Enterprise Resource Planning) específicamente al Software Administrativo Contable que se encargará de la revisión de inventarios y facturación. Finalmente el sistema Web genera un reporte de estas solicitudes, al que se tiene acceso en la Intranet, por medio de la siguiente opción: *Operación y Administración*, submenú *Reportes, Reporte de Pedidos de Usuarios*.

4.3.2.1.3 Eliminar Solicitudes de Pedidos de Compra

Esta opción está disponible únicamente si el usuario ha realizado previamente un pedido, siguiendo los pasos descritos anteriormente, hasta el punto en el cual se despliega el detalle de los productos seleccionados, y para esto el usuario debe dar clic en el ícono del carrito de compras marcado con una X.

El sistema procesa la solicitud y responde seguidamente al usuario con un mensaje que indica *“Pedido Eliminado Correctamente”.*

4.3.2.2 Faq’s:

En esta opción se da a conocer información relativa a la empresa, requiere simplemente la selección de la opción Faq`s y el sistema presenta en pantalla directamente las preguntas más frecuentes que se hacen de la empresa.

4.3.2.3 Contáctenos:

Aquí se permite al usuario establecer una comunicación directa con la empresa por medio de las siguientes opciones:

- Interesado en Trabajar con Nosotros
- Contáctese con Nosotros
- Evalúe Nuestros Productos y Servicios

4.3.2.3.1 Interesado en Trabajar con Nosotros

Para desplegar esta pantalla el usuario debe ingresar en la opción de menú *Contáctenos* y seleccionar la opción de submenú *Interesado en Trabajar con Nosotros*, es entonces que se despliega un formulario de inserción de Datos para la Bolsa de Trabajo. Este formulario esta dividido en dos partes, la primera es utilizada cuando el usuario desea actualizar o eliminar el registro de la base de datos, para conseguir esto se debe proceder a la búsqueda ingresando el número de la cédula de identidad del usuario en el campo correspondiente. En este caso, el sistema devuelve toda la información registrada y presenta en la parte inferior dos botones *Eliminar BD ó Actualizar BD.*

En la segunda parte se presenta un formulario vacío que será llenado con la información que el usuario desee ingresar. Al final se encuentra el botón *Enviar Información.*

Como resultado, el sistema Web registra en la base de datos la información que ha sido ingresada, además crea un reporte al que se puede acceder desde la

opción de la *Intranet*, *Recursos Humanos*, submenú *Consulta Hojas de Vida de los Aspirantes de la Bolsa de Trabajo*. Y finalmente el usuario obtiene mensajes en la pantalla que le indican el estado de su operación.

4.3.2.3.2 Contáctese con Nosotros

El usuario debe ingresar en la opción de menú *Contáctenos* y seleccionar la opción de submenú *Contáctese con Nosotros*, es entonces que se despliega un formulario del contacto. Como consecuencia el sistema Web registra en la base de datos la información llenada, además permite la visualización de estos datos en un formulario al que se puede acceder desde la *Intrane*t opción de Ventas, submenú *Asigna Ejecutivo a Cliente*.

Esta operación tiene una funcionalidad adicional que permite que el personal del Call Center de la empresa pueda registrar los requerimientos de posibles clientes que se contactan vía telefónica con la empresa.

4.3.2.3.3 Evalúe Nuestros Productos y Servicios

Para acceder a esta funcionalidad, el usuario debe seleccionar la opción de menú *Contáctenos*, e ingresar al submenú *Evalúe Nuestros Productos y Servicios*, aquí se publica una encuesta que permite al usuario evaluar los productos y servicios que la empresa ofrece por medio de la selección de una calificación, al final de la encuesta se encuentra el botón *Envia*r que finaliza la interacción del usuario de Extranet. El sistema almacena esta información en la base de datos y además permite visualizar los resultados en la Intranet en la opción *Operación y Administración*, y luego en el submenú *Reporte de Evaluación de Nuestros Productos y Servicios*.

4.3.3 FUNCIONALIDADES DEL PERFIL DE INTRANET

Usuario: el usuario con perfil de Intranet es un miembro de la empresa que requiere información ágil para mejorar su desempeño laboral y las opciones a las que tiene acceso son determinadas por el usuario con perfil de administrador, quien a su vez recibió especificaciones con los requerimientos que debe tener.

Opciones de Menú:

4.3.3.1 Operación y Administración:

Donde se publica información relativa a la parte logística de la empresa y se pueden encontrar las siguientes opciones:

- Reportes
- Modificar Noticias
- Modificar Eventos y Promociones
- Modificar Cursos de Capacitación
- Modificar Intercambios y Pasantías
- Reporte de Vacaciones

4.3.3.1.1 Reportes

Esta opción está disponible para el usuario que ha ingresado en el menú *Operación y Administración,* submenú *Reportes*, cuando se ingresa el sistema despliega un submenú que contiene el listado de reportes a los que puede acceder y que son:

- *Reporte de Evaluación de Nuestros Productos y Servicios*
- *Reporte de Pedidos de Usuarios*
- *Reporte de Cartera por Ejecutivos*

Para acceder a cualquiera de estos reportes el usuario debe seleccionar de un menú desplegable un parámetro de generación del reporte, por ejemplo en el caso de Reporte de Evaluación de Nuestros Productos y Servicios, en el combo aparecen las preguntas que se encuentran publicadas en la Extranet, en la opción *Contáctenos*, submenú *Evalúe Nuestros Productos y Servicios*. Para el caso de *Reporte de Pedidos de Usuarios* debe seleccionar el nombre de uno de los clientes. Y consecuentemente en el caso de *Reporte de Cartera por Ejecutivos* el parámetro de selección será el nombre de un ejecutivo o grupo de ellos.

Como resultado el sistema procesa el pedido y despliega en pantalla un cuadro con la información requerida, en algunos casos se incluye un esquema gráfico en forma de pastel.

4.3.3.1.2 Modificar Noticias

Para realizar esta acción el usuario debe ingresar a la opción de menú *Operación y Administración* submenú *Modificar Noticias*, el sistema despliega un formulario que permite eliminar, guardar o modificar los artículos de prensa que se desea publicar, esto por medio de opciones en donde se puede detallar la fuente del reportaje, y agregar imágenes o reportajes escaneados.

4.3.3.1.3 Modificar Eventos y Promociones

Para realizar esta acción el usuario debe ingresar a la opción de menú *Operación y Administración* submenú *Modificar Eventos y Promociones*, el sistema despliega un formulario que permite crear, eliminar, guardar o modificar los eventos y promociones en donde se puede ingresar la información que se quiere anunciar además de la posibilidad de agregar imágenes.

4.3.3.1.4 Modificar Cursos de Capacitación

Para realizar esta acción el usuario debe ingresar a la opción de menú *Operación y Administración* submenú *Modificar Cursos de Capacitación*, el sistema despliega un formulario que permite crear, eliminar, guardar o modificar los cursos de capacitación que están disponibles para los empleados .Por medio de un espacio para detallar la información respectiva, y se puede agregar imágenes.

4.3.3.1.5 Modificar Intercambios y Pasantías

Para realizar esta acción el usuario debe ingresar a la opción de menú *Operación y Administración* submenú *Modificar Intercambios y Pasantías*, el sistema despliega un formulario con una funcionalidad similar a la de las opciones anteriores.

4.3.3.1.6 Reporte de Vacaciones

Para realizar esta acción el usuario debe ingresar a la opción de menú *Operación y Administración* submenú *Reporte de Vacaciones*, el sistema despliega un reporte de todas las personas registradas en la base de datos cuyo status indica "vacaciones", el sistema permite además filtrar el reporte por un rango de fechas establecidas por el usuario.

4.3.3.2 Recursos Humanos:

En esta opción se puede acceder a toda la información correspondiente al personal y facilita el acceso a modelos de solicitudes. Permite las siguientes opciones:

- Formularios de Solicitudes
- Consulta Hojas de vida de los Aspirantes de la Bolsa de Trabajo
- Consulta la Historia Laboral de los Empleados
- Organigrama de la Empresa
- Calendario de Vacaciones y Días de Descanso
- Evaluaciones de Desempeño
- Ingreso Vacaciones de Empleados
- Seleccionar al Empleado del Mes

4.3.3.2.1 Formularios de Solicitudes

Esta opción está disponible para el usuario que ha ingresado en el menú *Recursos Humanos* submenú *Formularios de Solicitudes*, el sistema despliega un listado de solicitudes a las que puede acceder y que son:

- *Solicitud de Vacaciones*
- *Aviso de Enfermedad*
- *Licencia por Maternidad*
- *Forma de Reporte para Gastos de Representación*

Como resultado el usuario podrá visualizar en pantalla el documento respectivo.

4.3.3.2.2 Consulta Hojas de Vida de los Aspirantes de la Bolsa de Trabajo

Esta opción está disponible para el usuario de Intranet que ha ingresado en el menú *Recursos Humanos* submenú C*onsulta Hojas de Vida de los Aspirantes de la Bolsa de Trabajo*. Para su ejecución, el interesado debe seleccionar de un menú desplegable el área de trabajo que le interesa consultar. En la parte inferior, el sistema muestra un cuadro con los datos generales de los aspirantes, para obtener información detallada de alguno de ellos, se debe señalar el guión en formato de link ubicado en la primera columna del cuadro, e inmediatamente se muestra en la forma correspondiente las referencias solicitadas.

4.3.3.2.3 Consulta Historia Laboral de los Empleados

Esta opción está disponible para el usuario que ha ingresado en el menú *Recursos Humanos* submenú *Consulta Historia Laboral de los Emplea*dos.

Esta opción no solo permite consultar un reporte de los datos, además permite crear o eliminar registros de empleados, y modificar información de la base de datos. Para consultar los datos de un empleado o actualizar algún dato, se debe ingresar un parámetro de búsqueda de la base de datos, en este caso corresponde digitar la cédula de identidad. Inmediatamente el sistema despliega en la forma correspondiente los datos personales que se solicitaron. En la parte inferior están los botones que permiten terminar la operación. En caso de necesitar ingresar un nuevo registro, se deben digitar todos los datos en la forma vacía que se presenta al inicio o presionando en botón Nuevo. Al término de la operación el sistema guarda toda la información que se ha modificado.

4.3.3.2.4 Organigrama de la Empresa

Para acceder a esta opción el usuario necesita ingresar en la opción de menú *Recursos Humanos* submenú *Organigrama de la Empresa,* como resultado, se podrá visualizar en pantalla un documento en el que se grafica la organización de la empresa.

4.3.3.2.5 Calendario de Vacaciones y Días de Descanso

Para acceder a esta opción el usuario necesita ingresar el menú *Recursos Humanos* submenú *Calendario de Vacaciones y Días de Descanso*, el sistema despliega en pantalla una forma que contiene un calendario en el cual se debe señalar el rango de fechas que se desea consultar, dando un visto en los cuadrados de inicio y fin. Como resultado en la parte inferior se muestra una tabla que detalla las fechas de feriados y la duración.

4.3.3.2.6 Evaluaciones de Desempeño

Para acceder a esta opción el usuario necesita ingresar en el menú *Recursos Humanos* submenú *Evaluaciones de Desempeño* el sistema despliega un formulario, en el cual primero el usuario debe seleccionar al empleado que será objeto de evaluación, y seguidamente, debe escoger la puntuación de cada pregunta de un rango de 1 a 5 en el que 1 es la peor valoración y 5 corresponde un excelente desempeño. En la selección de la última pregunta se realiza la suma de las valoraciones que será almacenada en el sistema al oprimir el botón “Enviar Datos”.

4.3.3.2.7 Ingreso de Vacaciones de Empleados.

Para disponer de esta opción el usuario necesita ingresar en el menú *Recursos Humanos* submenú *Ingreso de Vacaciones de Empleados*, el sistema despliega en pantalla una forma en la cual se debe ingresar la cédula del empleado del que se desea registrar sus vacaciones. A continuación se despliegan sus datos personales, los cuales no podrán ser modificados, y dos calendarios en los cuales se selecciona el rango de fechas de las vacaciones. Al momento de enviar estos datos el sistema cambia el status del empleado en estas fechas, de “activo” a “vacaciones”.

4.3.3.2.8 Seleccionar al Empleado del Mes

Para realizar esta acción el usuario necesita ingresar en la opción de menú *Recursos Humanos* submenú *Seleccionar Empleado del Mes*, el sistema

despliega un formulario en el cual simplemente el usuario debe seleccionar al empleado que será nominado digitando su número de cédula.

4.3.3.3 Capacitación

Es por medio de esta opción que los usuarios de la Intranet pueden disponer de una parte del conocimiento empresarial por medio de las siguientes operaciones:

- *Manuales de Capacitación*
- *Presentaciones de Cursos de Capacitaciones*
- *Eventos y Promociones*
- *Plan de Cursos de Capacitación para Empleados*
- *Intercambios y Pasantías*

4.3.3.3.1 Manuales de Capacitación

Para acceder a esta opción el usuario necesita ingresar en el menú *Capacitación* submenú *Manuales de Capacitación*. El sistema despliega una lista de los diferentes manuales a los que se pueden acceder dando un clic en las opciones en formato de link. Como resultado el sistema permite visualizar en pantalla un documento que contiene toda la información solicitada.

4.3.3.3.2 Presentaciones de Cursos de Capacitación para Empleados

Para acceder a esta opción el usuario necesita ingresar en el menú *Capacitación* submenú *Presentaciones de Cursos de Capacitación para Empleados*. El sistema despliega una lista de las diferentes presentaciones de los cursos dictados, a los que se pueden acceder dando un clic en las opciones en formato de link. Como resultado se podrá visualizar en pantalla información solicitada.

4.3.3.3.3 Eventos y Promociones

Para realizar esta operación el usuario necesita ingresar en la opción de menú *Capacitación* submenú *Eventos y Promociones*. El sistema despliega una lista de los eventos y promociones programados por la empresa.

4.3.3.3.4 Plan de Cursos de Capacitación para Empleados

Para realizar esta operación el usuario necesita ingresar en la opción de menú *Capacitación* submenú *Plan de Cursos de Capacitación para Empleados.* El sistema despliega un listado con el plan de cursos al que pueden acceder los empleados.

4.3.3.3.5 Intercambios y Pasantías

Para realizar esta operación el usuario necesita ingresar en la opción de menú *Capacitación* submenú *Intercambios y Pasantías.* El sistema despliega un detalle de las opciones que le pueden interesar al personal.

4.3.3.4 Difusión y Comunicación

Este espacio es exclusivo para publicaciones tanto sobre la visión interna de la empresa, como de noticias nacionales e internacionales destacadas.

- Revista de la Empresa
- Empleado del Mes
- Artículos de Prensa
- Normativas de la Empresa (Manual de Procesos)
- Descripción de Puestos y Responsabilidad (Manual de Funciones)
- Contactos y Proveedores

4.3.3.4.1 Revista de la Empresa

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Revista de la Empresa.* El sistema muestra en pantalla un documento con publicaciones relativas a la empresa.

4.3.3.4.2 Empleado del Mes

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Empleado del Mes.* El sistema despliega inmediatamente una foto del empleado del mes con su respectiva felicitación.

4.3.3.4.3 Artículos de Prensa

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Artículos de Prensa*. El sistema presenta directamente publicaciones de prensa que se consideran de interés colectivo.

4.3.3.4.4 Normativas de la Empresa (Manual de Procesos)

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Normativas de la Empresa (Manual de Procesos),* a continuación se visualiza un documento que contiene el Manual de Procesos de la Empresa.

4.3.3.4.5 Descripción de Puestos y Responsabilidades (Manual de Funciones)

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Descripción de Puestos y Responsabilidades (Manual de Funciones)*, inmediatamente se visualiza en pantalla un documento expone ampliamente las actividades de cada uno de los puestos de trabajo y sus respectivas responsabilidades y que corresponde al *Manual de Funciones*.

4.3.3.4.6 Contactos y Proveedores

Para acceder a esta opción el usuario necesita ingresar en el menú *Difusión y Comunicación* submenú *Contactos y Proveedores* seguidamente se despliega una lista de los principales contactos y proveedores de la empresa.

4.3.3.5 Ventas

Este menú presenta varias opciones de submenú que contemplan actividades que facilitan el trabajo del personal del departamento de Ventas por medio de:

- Asigna Ejecutivo a Cliente
- Reporte de Asignación de Ejecutivos
- Preparación de Documentos
- Catálogo de Productos

4.3.3.5.1 Asigna Ejecutivo a Cliente

Para acceder a esta opción el usuario debe ingresar en el menú *Ventas* submenú *Asigna Ejecutivo a Cliente*. Esta operación consta de varios pasos que son: primero el usuario debe seleccionar de entre un rango de fechas todos los contactos que fueron registrados previamente en la Extranet por medio del menú *Contáctenos*, opción *Contáctese con Nosotros*; el sistema responde presentando en pantalla un cuadro con la lista requerida en el que se detalla los datos del cliente; segundo, se debe seleccionar el *guión* en formato de link que aparece en la primera columna del cuadro para que el sistema coloque en una forma que se encuentra a continuación del cuadro, una ampliación de los datos del cliente y el requerimiento que precisa. En tercer lugar, al final de la forma, se encuentra la lista de vendedores, de la cual se debe escoger uno o un grupo al que será asignado el cliente. Además se debe elegir la fecha y la hora en la que se coordinó la cita. El sistema Web almacena esta información en la base de datos y genera un reporte que puede ser accedido desde Ventas, submenú, Reporte de Asignación de Ejecutivos.

4.3.3.5.2 Reporte de Asignación de Ejecutivos

En esta opción el usuario debe ingresar en el menú *Ventas* submenú *Reporte de Asignación Ejecutivo*, y seleccionar de un combo desplegable el nombre de un vendedor o de un grupo de vendedores del que requiere obtener la lista de clientes asignados. El sistema responde presentando en la parte inferior del combo, un cuadro con la información solicitada.

4.3.3.5.3 Preparación de Documentos

Para acceder a esta opción el usuario necesita ingresar en el menú *Ventas* submenú *Preparación de Documento*s. El sistema despliega una lista de los documentos que se requieren para cerrar una venta, a los que se pueden acceder dando un clic en las opciones respectivas. Como respuesta el sistema presenta esta información en pantalla.

4.3.3.5.4 Catálogo de Productos

Para acceder a esta opción el usuario necesita ingresar en el menú *Ventas* submenú *Catálogo de Productos*. El sistema muestra en pantalla una forma en la que se puede seleccionar la categoría del software a la que se quiere acceder. Una vez realizada la elección se puede ver el detalle de cada uno de los paquetes disponibles, donde se incluye una imagen, precio, una descripción y se pueden realizar varias acciones como: descargar información más detallada (brochures), registrar solicitudes de pedidos de compra y eliminar solicitudes de pedidos de compra las cuales tienen la misma funcionalidad descrita inicialmente para el entorno del perfil de Extranet.

4.3.3.6 Soporte

Las opciones que presenta ese submenú están enfocadas en las actividades que realiza el personal del área de Soporte, y las operaciones que se pueden realizar son:

- Asignar Técnico a Cliente
- Registrar Órdenes de Trabajo
- Reporte General de Órdenes de Trabajo
- Reporte de Órdenes de Trabajo por Técnico
- Personalización de Aplicaciones
- Reporte de Asignación de Técnicos

4.3.3.6.1 Asignar Técnico a Cliente

Esta opción esta disponible en el menú *Soporte*, submenú *Asignar Técnico a Cliente*, para esta realizar esta acción el usuario debe escoger de un menú desplegable el cliente al que se le asignará un técnico, inmediatamente en la parte inferior se presenta un cuadro con los datos de la selección. Al final se encuentra otro menú desplegable del cual se debe optar por un técnico que será quien finalmente atienda los requerimientos del cliente. Se debe fijar también la ficha de la cita. El sistema guarda esta información en la base de datos y adicionalmente genera un reporte que se accede desde *Reporte de Asignación de Técnicos* disponible en este mismo menú.

4.3.3.6.2 Registrar Órdenes de Trabajo

Esta opción esta disponible en el menú *Soporte*, submenú *Registrar Órdenes de Trabajo* y su funcionalidad es que permite a los técnicos registrar directamente las actividades realizadas donde los clientes, mediante modificaciones o ingresando órdenes nuevas. Para ello deben llenar los datos que se solicitan en la forma que se presenta en pantalla.

4.3.3.6.3 Reporte General Órdenes de Trabajo

Esta opción esta disponible en el menú *Soporte*, submenú *Reporte General de Órdenes de Trabajo*, cuando el usuario ingresa, el sistema despliega directamente un reporte con los datos que fueron ingresados previamente en la opción anterior.

4.3.3.6.4 Reporte de Órdenes de Trabajo por Técnico

Esta opción esta disponible en el menú *Soporte*, submenú *Reporte de Órdenes de Trabajo por Técnico*, cuando el usuario ingresa debe seleccionar de un combo el nombre del técnico del que desea obtener el reporte e inmediatamente el sistema despliega los datos requeridos filtrados por el nombre del técnico.

4.3.3.6.5 Personalización de Aplicaciones

Esta opción esta disponible en el menú *Soporte*, submenú *Personalización de Aplicaciones*; En el caso de que el usuario requiera ingresar una nueva personalización de algún cliente, debe primero seleccionar de un combo el nombre del cliente y a continuación llenar la forma correspondiente y finalmente guardar. Para modificar o eliminar alguna personalización, se debe seleccionar esta de una tabla que se encuentra al final de la forma, por medio del guión que está en la primera columna.

4.3.3.6.6 Reporte de Asignación de Técnicos

Esta operación esta disponible en la opción *Soporte*, submenú *Reporte de Asignación de Técnicos*, cuando el usuario ingresa debe seleccionar de un combo

el nombre del técnico del que desea obtener el reporte e inmediatamente el sistema despliega los datos requeridos.

4.4 PRUEBAS DE LA SOLUCIÓN

La fase de pruebas consiste en ejecutar el sistema con la intención de encontrar la mayor cantidad de fallas, a fin de solventar los problemas encontrados y garantizar la respuesta del sistema ante cualquier caso que se le presente en la ejecución real. [29]

Las pruebas verifican y validan que un programa, subsistema o aplicación realice las funciones para las cuales fue diseñado. Además determinan si las unidades que están siendo probadas operan sin problemas de funcionamiento ni efectos adversos sobre otros componentes del sistema. El plan de pruebas que se utiliza sostiene el enfoque de abajo hacia arriba lo que implica varios niveles (unidad, subsistema, integración, sistema)[30]

4.4.1 PRUEBA DE UNIDAD

Es la prueba de un programa o módulo individual. Usa un conjunto de casos de prueba que se concentran en la estructura de control del diseño procedimental. Estas pruebas aseguran que la operación interna del programa funciona en conformidad con la especificación.

En la aplicación, el usuario puede confrontar esta prueba por medio de la utilización mensajes de error provenientes de los controles del ASP.net para la validación de los datos ingresados por el usuario como por ejemplo: datos en campos que no pueden estar en blanco, datos de e-mail, valores que se ajustan al tipo de datos que está predefinido en la base de datos. En la siguiente figura se muestra el mensaje de error que provoca la insuficiencia de datos en los campos.

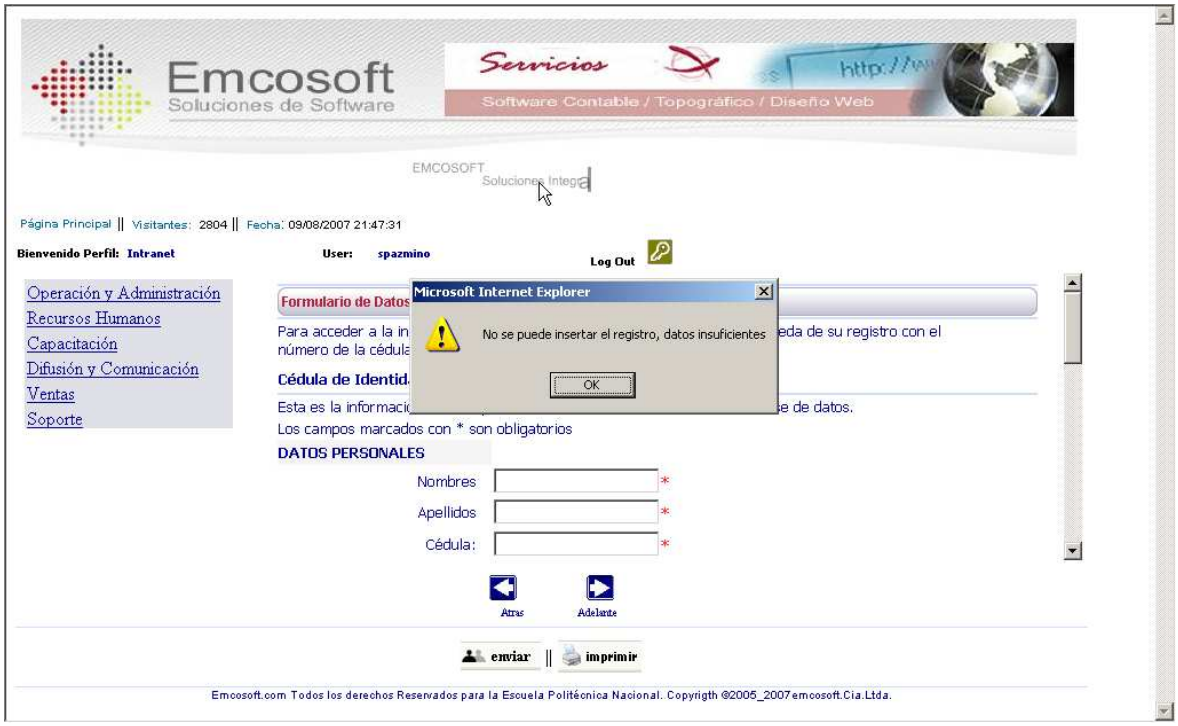

Figura 4-356: Prueba de Unidad
Fuente: Las Autoras

4.4.2 PRUEBA DE INTERFAZ O DE INTEGRACIÓN

Una prueba de hardware o de software que evalúa la conexión de dos o más componentes que pasan información desde un área a otra. El objetivo es tomar módulos probados por unidad y construir una estructura integrada basada en el diseño.

En la aplicación existen varios módulos que están interrelacionados entre si, por ejemplo, por medio de algunos formularios se puede ingresar información, la misma que es utilizada por otros para generar reportes, o se convierten en información de entrada para otras operaciones. Esta prueba se realiza por medio de la comparación entre los datos que se ingresaron, el estado de éstos en la base de datos, y los resultados que se visualizan en las otras funcionalidades relacionadas. Además el usuario visualiza mensajes que le indican que operaciones como insert, update, delete se realizaron respetando las relaciones existentes entre las tablas de la base de datos por medio de llaves primarias y foráneas.

4.4.3 PRUEBAS DEL SISTEMA

Son una serie de pruebas diseñadas para asegurar que los programas modificados, objetos, esquema de base de datos, etc., que constituyan un sistema nuevo o modificado funcionen correctamente de forma colectiva. Durante esta fase se pueden realizar otros tipos de pruebas como:

- Recuperación ante una falla de hardware o de software.
- Seguridad, o que incluya controles de acceso.
- Estrés, someter a la aplicación a grandes cantidades de datos para evaluar su rendimiento en horas pico.
- Volumen, evaluar cantidad máxima de datos que puede procesar.
- Rendimiento, comparar el sistema con otros equivalentes utilizando referencias comparativas bien definidas.

Para esta fase se ha realizado la prueba de estrés, por medio Visual Studio .NET que permite probar aplicaciones basadas en WEB, por medio de Aplication Center Test (ACT), que está integrado en las versiones V.S. Enterprise Developer y Enterprise Architect. Permite obtener una matriz de rendimiento y realizar pruebas de servicios Web XML y de páginas Web.

Se utiliza un Contador de Rendimiento para controlar el rendimiento total de la interacción de ambos. En este caso de la autenticación y de una solicitud de pedido de compra.

Se define el contador para que cuente el número de solicitudes que atiende por segundo. Se arrastra el contador a la página que contiene el servicio. Se instrumenta el contador con un increment y se compila. Se puede ver la consola monitor de rendimiento. Se inicia la sesión de autenticación, se visita la página de productos y llamamos a la opción de hacer pedidos, y damos clic en actualizar repetidamente, esto nos permite máximo 6 solicitudes como se ve el gráfico:

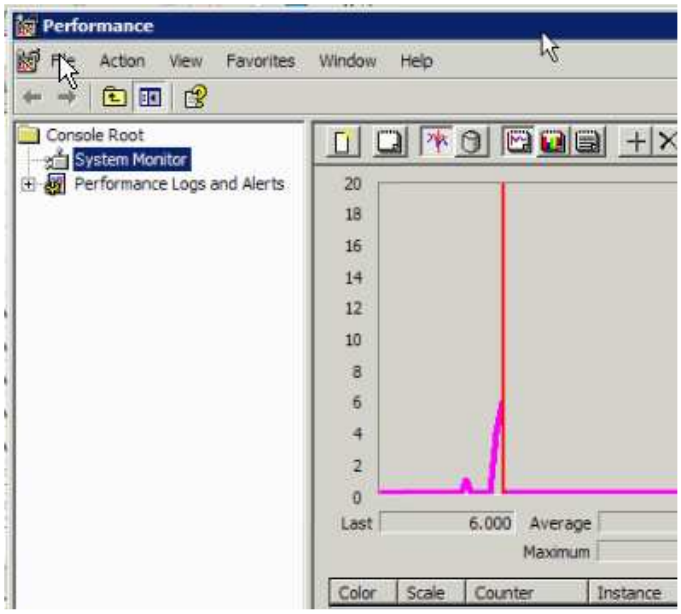

Figura 4-367: Pruebas de Rendimiento Inicial
Fuente: Las Autoras

Para ver realmente el rendimiento que permita ajustar la página, se necesita una herramienta que permita hacer clic mucho más rápido y para esto se recurre a ACT donde se crea una secuencia de comandos llamadas testorderspage, luego se graba utilizando los valores predeterminados y en Start recording se pega la página de pedidos. Ahora se entra y se autentica, y comienza la prueba.

Figura 4-378: Pruebas de Rendimiento ACT
Fuente: Las Autoras

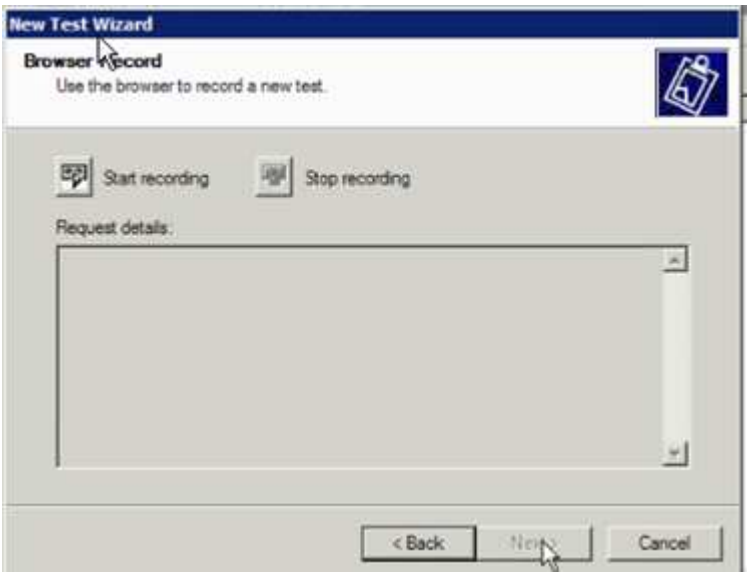

Figura 4-389: Pruebas de Rendimiento ACT 2
Fuente: Las Autoras

Aquí se ve como se incrementa a 150 solicitudes.

Figura 4-39: Pruebas de Rendimiento Incremento de Solicitudes
Fuente: Las Autoras

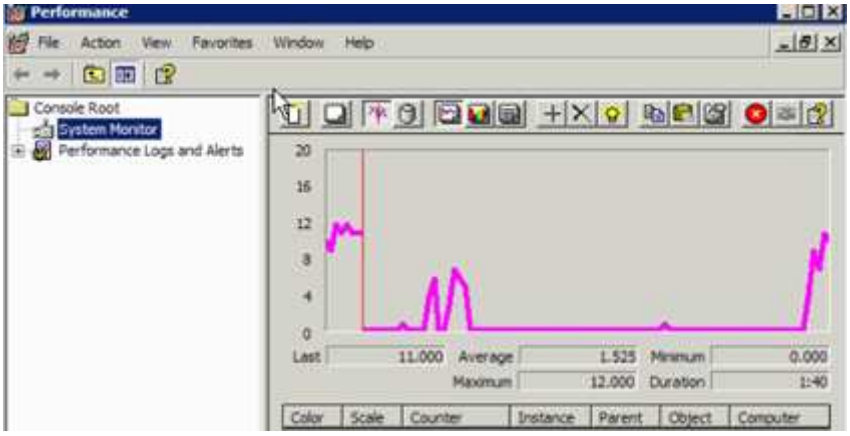

Figura 4-401: Pruebas de Rendimiento Gráfico Inicial
Fuente: Las Autoras

Para optimizar el rendimiento se utiliza el tiempo de duración en cache por medio de la siguiente línea de código:

```
<%@ Register TagPrefix="cc1" Namespace="Msgbox" Assembly="Msgbox" %>
<%@ Page Language="vb" AutoEventWireup="false" Codebehind="WfMOrdTrabajo.aspx.vb"
<%@ OutPutcache Duration="10" VaryByParam="*" %>
```

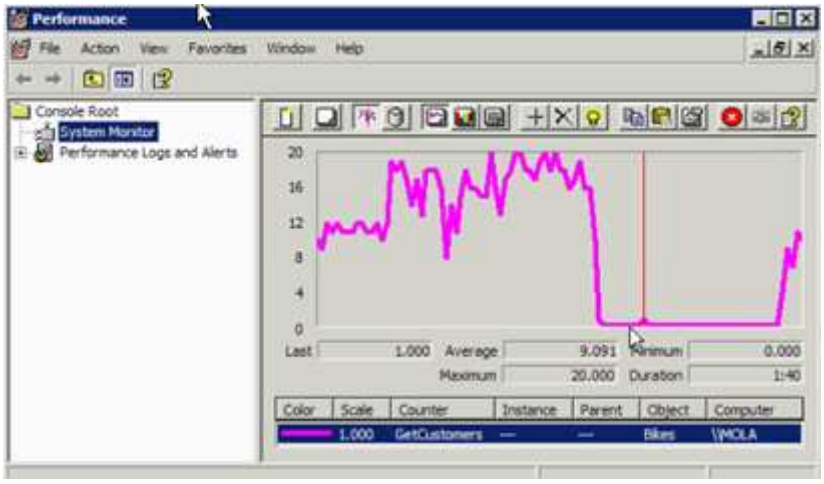

Figura 4-412: Pruebas de Rendimiento Gráfico Final
Fuente: Las Autoras

Ahora el resultado es que se puede controlar muchas más solicitudes por segundo, permitiendo que vaya solo 1 llamada al Web form por que se vuelve a almacenar en cache cada 10 seg. Pasando de 125 solicitudes a un pico de 190.

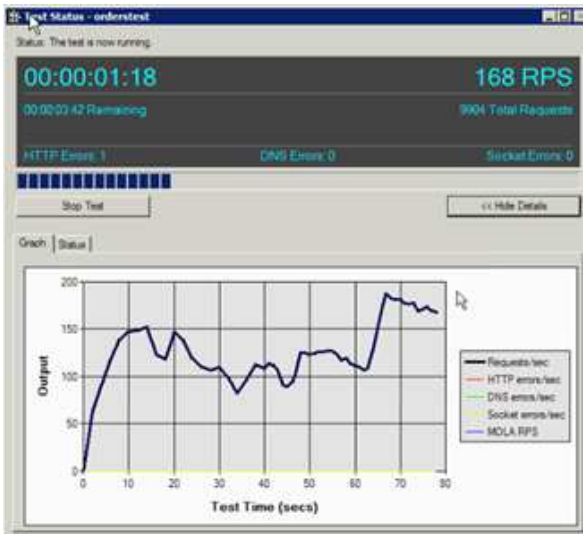

Figura 4-423: Pruebas de Rendimiento. Gráfico Solicitudes
Fuente: Las Autoras

4.4.4 PRUEBA DE ACEPTACIÓN FINAL

Después de que el personal de desarrollo esté satisfecho con sus pruebas iniciales y/o del sistema, el sistema modificado esta listo para la prueba de aceptación, que se lleva a cabo durante la etapa de implementación. Esta prueba tiene dos partes: la prueba de aseguramiento de calidad (QAT), concentrándose en los aspectos técnicos de la aplicación, y la prueba de aceptación del usuario (UAT), concentrándose en el aspecto funcional de la aplicación.

En lo que respecta a (QAT) el sistema cumple con las especificaciones documentadas y la tecnología empleada, pues parte de un amplio análisis de los requerimientos, de la infraestructura tecnológica disponible, y un diseño enfocado en la estructura de la empresa desde el punto de vista de los procesos que se ejecutan en sus diversos departamentos o secciones.

La aplicación fue probada directamente con el personal que utiliza el sistema, obteniéndose al final resultados satisfactorios en lo que corresponde a (UAT) que indica que el sistema cumple con los requerimientos de los usuarios, pues obtienen ágilmente la información que necesitan por medio de un interfaz que muestra las opciones a las que pueden acceder, y guían a los usuarios en caso de errores u omisiones al ingresar información al sistema.

CAPÍTULO 5

ADMINISTRACIÓN Y SEGURIDAD DE LA INTRANET/ EXTRANET

La administración de redes es una completa disciplina que abarca la administración de personas, procesos y procedimientos, productos y herramientas tecnológicas, fabricantes y proveedores de servicios. Este proceso asegura que la red opere eficazmente en todo momento y así evitar efectos desfavorables en el funcionamiento de la empresa.

Es el responsable de la confiabilidad, coherencia y escalabilidad de las infraestructuras de red que cumplen o sobrepasan los niveles de servicio y optimiza los activos de la empresa.

Una red confiable y coherente que proporciona servicios adecuados a los usuarios, aminora el impacto de los cambios efectuados en la red, controla los problemas eficientemente y reduce el riesgo de errores

5.1 POLÍTICAS DE ADMINISTRACIÓN DE LA INTRANET/ EXTRANET

Las políticas son documentos de alto nivel que representan la filosofía corporativa de una organización y el pensamiento estratégico de la alta gerencia y de los dueños de los procesos del negocio. Las políticas deben ser claras y concisas para que sean efectivas. La administración debe crear un ambiente de control positivo, asumiendo la responsabilidad de formular, desarrollar, documentar, promulgar y controlar las políticas que abarcan las metas y las directrices generales. La gerencia debe emprender las acciones necesarias para asegurar que los empleados afectados por una política específica reciban una explicación completa de la política y entiendan cual es su propósito.

Los principios básicos de la administración de la red son la administración de los errores, el rendimiento, y la seguridad.

5.1.1 ADMINISTRACIÓN DE LOS ERRORES

El análisis de la información acerca de la red para predecir y administrar los errores dentro de la infraestructura es la tarea de la función de administración de errores. Esta función se divide en tres categorías: administración de errores predictiva, proactiva y reactiva.

- La administración de errores predictiva consiste en el uso analítico de los datos recopilados a partir de la supervisión y la medida. Los datos se utilizan para predecir posibles interrupciones en el sistema y formular una estrategia de mantenimiento preventivo. Los procesos asociados con este tipo de administración de errores comparan y contrastan el costo y los riesgos de los sistemas existentes con las posibles alternativas y su costo asociado. Las alternativas posibles podrían incluir nuevas tecnologías y nuevas versiones de las tecnologías existentes.
- La administración de errores proactiva consiste en responder a las alarmas generadas cuando se alcanzan los umbrales de rendimiento. Se establecen unos umbrales para las operaciones de la red que normalmente indican una posible degradación en el servicio, que podría resultar en su interrupción. El propósito de la administración de errores proactiva es utilizar la información de supervisión como base para tomar acciones correctivas antes de que ocurran interrupciones en el funcionamiento del sistema.
- La administración de errores reactiva consiste en los procesos y los procedimientos que se utilizan cuando hay una interrupción no programada en el funcionamiento del sistema. Incluso cuando se efectúa una rigurosa administración de errores proactiva en el sistema, las interrupciones pueden seguir siendo una amenaza. El propósito de este tipo de administración de errores es el de disponer de procedimientos para movilizar recursos, restablecer rápidamente el servicio y aminorar el efecto de una interrupción.

Los métodos para desarrollar la administración de errores incluyen la supervisión, el examen de los registros de errores, la presentación y el control de las alertas, el seguimiento y la identificación de los errores, la ejecución de pruebas de diagnóstico y la corrección de los errores. Sus funciones principales son:

- Detección de errores
- Aislamiento y diagnóstico de errores
- Inicio de acciones correctivas
- Informe inmediato de errores
- Informe periódico de errores
- Creación y mantenimiento de una base de datos de fichas de errores
- Reasignación de los problemas
- Administración de la resolución
- Administración de proveedores

5.1.2 RENDIMIENTO

Para un correcto análisis del rendimiento se debe realizar una eficiente supervisión, la cual se utiliza para determinar tanto el estado actual de la red como la posible necesidad de modificarla o expandirla.

Para lograr este fin se emplean los procedimientos como por ejemplo mediciones de tiempos de respuesta a consultas frecuentes, accesos recurrentes. Todo esto durante los tiempos pico

Esto permitirá hacer modificaciones necesarias, controladas y programadas en el sistema, para mantener un óptimo rendimiento del mismo.

Este procedimiento debe ser periódico y debidamente registrado.

5.1.3 SEGURIDAD

Se trata de una cuestión muy amplia que engloba a cada parte de la administración de la red y a todas sus disciplinas principales. Incluye los

procesos, procedimientos, personas y hardware necesarios para proteger la red ante intrusiones y otras fisuras en la seguridad, ya sean internas o externas. Su propósito es proteger la red. Se amplia con más detalle en el capítulo 5.3.

5.2 CONFIGURACIÓN DE LOS SERVICIOS INTRANET / EXTRANET

Todos los detalles de la configuración se encuentran documentados en el Anexo 1 “Manual de Instalación”

5.2.1 INSTALACIÓN DEL SISTEMA OPERATIVO

Para instalar el sistema Operativo Windows 2003 Server, primero se verifica los requerimientos mínimos de hardware, mientras carga los drivers se va revisando compatibilidad de hardware, luego con la controladora de discos, busca versiones previas de Windows 2003. Pregunta la partición que se desea escoger, formatea permite escoger entre FAT 32 y NTFS, luego instala drivers y controladores y configuración regional, teclado y licencia, nombre de la empresa, usuario, nombre del equipo, controladora de red, si se desea grupo de trabajo o dominio.

5.2.2 CONFIGURACIÓN DEL DIRECTORIO ACTIVO DE DOMINIO

En esta configuración se definirá el nombre del dominio y del respectivo administrador del dominio, sobre el directorio activo van a registrarse todos los equipos que hayan sido registrados por un usuario con perfil de administrador, permite: crear grupos y usuarios, crear y aplicar políticas tanto de grupos como usuarios. Esta es la plataforma básica para que el resto de servicios se vayan integrando al mismo. Ver Anexo 2 “Configuraciones”.

5.2.3 CONFIGURACIÓN DE DNS

Permite hacer la resolución de nombres de equipos a direcciones IP, permite hacer búsquedas de dominios tanto internos como externos a través de los reenviadores (forwards). Ver Anexo 2 “Configuraciones”.

5.2.4 CONFIGURACIÓN DE DHCP

Este servicio permite asignaciones dinámicas de direcciones IP's a diferentes equipos que lo soliciten esto se lo hace a través de rangos de direcciones IP's que son configuradas en el servidor de DHCP, también guarda un registro del nombre de la máquina que solicitó el mismo y la dirección IP que le fue asignada. Ver Anexo 2 "Configuraciones".

5.2.5 CONFIGURACIÓN DE IIS (INTERNET INFORMARION SERVICES)

El servidor Web permite la administración de sitios Web y manejar la seguridad de éstos. Ver Anexo 2 "Configuraciones".

5.2.6 CONFIGURACIÓN DE MICROSOFT EXCHANGE

El servidor de correo se integra de forma transparente con el Active Directory de tal forma que permite administrar los usuarios directamente desde la misma consola del Active Directory por lo tanto permite el manejo ágil de los buzones de Exchange. También tiene un administrador propio que se centra en las funciones del servidor de correo como administración de protocolos, tamaño de los buzones o manejo de cuotas, administración de colas. (Microsoft Exchange Manager). Ver Anexo 2 "Configuraciones".

5.2.7 CONFIGURACIÓN DEL ISA (INTERNET SECURITY & ACCELETATOR SERVER)

El servidor de firewall que permite el bloqueo cualquier tipo de intrusión por medio de administración de puertos, hacia la parte interna de la red.

Permite publicar cierto tipo de servicios que son necesarios, (servidor de correo, Web, ftp) y ponerles a disposición de acceso público pero bajo reglas o políticas de seguridad.

Permite crear VPN's, crear filtros de contenidos, bloqueos a diferentes servicios.

Permite varios escenarios de seguridad generar modelos de seguridad por medio de DMZ, como por ejemplo (manejo de un servidor primario y un secundario).

Permite opciones de supervisión para mantener registros, para controlar estatus de la red y todo el tráfico que atraviesa el ISA. Ver Anexo 2 “Configuraciones”

5.3 POLÍTICAS DE SEGURIDADES DE LA INTRANET / EXTRANET

Objetivo.- El objetivo de estas políticas consiste en explicar que es lo que se considera un uso apropiado de los recursos informáticos, así como también las responsabilidades que supone el uso de estos recursos y las consecuencias de su abuso.

Se considera recursos informáticos de la organización: servidores, estaciones de trabajo, terminales, periféricos, infraestructura y equipos de comunicación, redes, sistemas informáticos, tecnologías que permiten el acceso, comunicación y distribución de información, originada por la organización o en cualquier otro lugar. Además de toda la información contenida en estos equipos.

También se hace referencia a las responsabilidades y derechos de usuarios y administradores, se expresa lo que se va a proteger y de lo que se esta tratando de proteger. Adicionalmente se mencionan las sanciones, las cuales deben ser revisadas, autorizadas, aplicadas y actualizadas.

Alcance: Este procedimiento aplica a todo el personal de Emcosoft, así como también a cualquier otra entidad externa que utilice los recursos informáticos como clientes, socios estratégicos, consultores, proveedores, personal temporal y otros.

El intentar violar los sistemas de seguridad y de control de personal se consideran actos graves de contravención a las políticas y normas de la organización así como atentatorias a la seguridad y confidencialidad de la información de la organización y sujeta a las leyes penales del Ecuador.

Responsable: El Jefe del Departamento de Informática, es el responsable de difundir, cumplir y hacer cumplir las Políticas de Seguridades y, además de recomendar normas y alertas en el manejo de programas, correo electrónico, información, Internet, archivos.

5.3.1 POLÍTICAS DE CUENTAS DE USUARIO Y PASSWORD

- Las claves de usuario de nivel administrador deben cambiarse con una frecuencia mensual.

- Las claves de usuario de Intranet deben cambiarse con una frecuencia trimestral.

- Las claves de usuario de Extranet se mantienen hasta que el usuario tramite una solicitud de cambio de password.

5.3.1.1 Normas Generales para la Creación de Contraseñas

Las contraseñas se utilizan para varios propósitos, como por ejemplo: cuentas de usuario, cuentas de acceso a e-mail, claves de protectores de pantalla, etc. En todos los casos es importante que la clave pueda resistir no solo el criptoanálisis sino también la ingeniería social, para esto todas las claves deben ser creadas siguiendo las siguientes normas:

- Utilizar caracteres en mayúsculas y minúsculas (a-z, A-Z)
- Incluir números, letras y caracteres especiales.
- Tener más de 8 caracteres

Evitar en lo posible utilizar como claves nombres de novias, esposas, hijos, mascotas, amigos, nombres mitológicos o astronómicos, términos informáticos, comandos, marcas, componentes, nombres relacionados con la empresa, fechas personales importantes o fechas en general, y patrones de letras o números tales como: “qwerty” “1234567” “abcdefge”.

5.3.1.2 Normas para la Protección de Claves

- No utilizar la misma contraseña para las cuentas del Sistema Web y para otras cuentas (ejemplo cuenta del ISA).

- Todas las claves deben ser confidenciales, no se debe compartir la cuenta con nadie bajo ninguna circunstancia.

- No se debe exponer las claves en ningún medio de comunicación como por ejemplo: decir las claves por teléfono, escribir las claves en un e-mail, escribir las claves en papel.

- No se debe almacenar las contraseñas en un archivo en ningún sistema informático (incluyendo PDA's o dispositivos similares).

- No se debe revelar las claves anteriores que dejo de usar.

5.3.1.3 Uso de Claves para Usuarios de Acceso Remoto

El acceso remoto de los usuarios a los servicios de red se lo hace utilizando autenticación de claves publicas y privadas, incluidas en los protocolos de comunicación.

5.3.2 POLÍTICAS DE SEGURIDAD PARA ESTACIONES DE TRABAJO

- EL Jefe de Informática, al entregar un equipo de informática o una cuenta a un usuario debe procurar la firma de un documento donde declara conocer las Políticas de Seguridades, la asignación y estado de los equipos, como aceptación de sus responsabilidades con relación al uso de los recursos asignados.

- Los equipos sólo deben usarse para actividades de trabajo y no para otros fines ajenos a los objetivos de la organización, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.

- No se permite fumar, comer o beber mientras se está usando un PC. Ni fijar adhesivos o publicidad sobre los equipos.

- Deben protegerse los equipos de riesgos del medio ambiente (por ejemplo, polvo, incendio y agua).

- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- No se pueden mover los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la organización se requiere una autorización escrita.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

- Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla.

- Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir a los usuarios las posibilidades de leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC’s adicionales al utilizado para la conexión a la red local (LAN).

- Los usuarios no deben copiar a un medio removible (como un diskettes, memorias flash, cd’s, etc), el software o los datos residentes en las computadoras de la organización, sin la aprobación previa de la gerencia.

- No pueden extraerse datos fuera de la sede de la organización sin la aprobación previa de la gerencia.

- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos.

- Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de de la organización.

- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- El Jefe de Informática debe asignar un código para cada equipo y sus componentes para su identificación y control de inventario; además debe garantizar que esté siempre legible. Los usuarios no deben destruir el código.
- El Jefe de Informática debe mantener actualizados los inventarios de los equipos.

- El Jefe de Informática debe instalar y activar un antivirus en todos los equipos, el cual debe mantenerlo actualizado.

- El Jefe de Informática debe garantizar que los servidores, los equipos de comunicación y el rack de cableado estructurado están protegidos contra daños y robo. Debe restringir el acceso a personas no autorizadas a la ubicación de los mismos.

5.3.3 POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES

5.3.3.1 Uso de los Sistemas de Comunicación

- Los sistemas de comunicación de la organización generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y

recursos, y además no interfiera con las productividades del empleado ni con las actividades de la organización.

- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la organización y en tal sentido deben usarse las horas no laborables.

- Los usuarios no deben usar los sistemas informáticos para insultar o molestar a ningún usuario. El lenguaje en las comunicaciones debe ser respetuoso y en los parámetros de la cordialidad.

5.3.3.2 Confidencialidad y Privacidad

- El Jefe de Informática debe garantizar que no exista información confidencial en las estaciones de trabajo antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la organización.

- Los empleados y funcionarios de la organización no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La organización se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

- Es política de la organización no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

- Los usuarios que manejan datos confidenciales de la organización los deben borrar de sus equipos cuando ya no sean de utilidad. Los usuarios

- La información de la organización clasificada como confidencial o de uso restringido, debe guardarse y transmitirse utilizando herramientas que hayan sido probadas y autorizadas.

- Cada usuario es responsable de identificar el tipo de información que está transmitiendo o guardando, con un texto o leyenda al pie del documento.

- Los usuarios que sospechen cualquier actividad ilegal o fraudulenta deben notificar inmediatamente al Jefe Informática.

5.3.3.3 Reenvío de Mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de de la organización, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la organización sin la debida aprobación.

5.3.3.4 Borrado de Mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

5.3.4 POLÍTICAS DE SEGURIDAD PARA REDES

5.3.4.1 Modificaciones

Todos los cambios en los servidores y equipos de red de de la organización, incluyendo la instalación de el nuevo software, el cambio de direcciones IP's, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

5.3.4.2 Cuentas de los Usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

- La solicitud de una nueva cuenta o el cambio de privilegios deben ser hecha por escrito y debe ser debidamente aprobada.

- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Jefe de Informática determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Jefe de Informática debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- Cuando un empleado es despedido o renuncia a la organización, debe desactivarse su cuenta antes de que deje el cargo.

5.3.4.3 Contraseñas y el Control de Acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
  La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión.

- El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña.

- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de de la organización, pudiendo ser causal de despido.

- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

- Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación (routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

5.3.5 POLÍTICAS DE BACKUP

5.3.5.1 Responsabilidades de la Organización y de los Usuarios

- Periódicamente, los usuarios deben sacar respaldos de sus archivos guardados en las estaciones de trabajo y servidores, en otros medios magnéticos y/o sistemas diferentes, los mismos que deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones, para que, en caso de cualquier eventualidad, el usuario pueda rever sus datos.

- Los usuarios de las estaciones de trabajo son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Jefe de Informática es el responsable de hacer copias de respaldo periódicas. Los gerentes de las distintas divisiones y departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- Los usuarios tienen la responsabilidad de leer las noticias anunciadas en el login de su cuenta (noticias que informan sobre paradas eventuales del sistema, manutención de hardware y software) y así prever rescates.

5.3.5.2 Backups y Restauración

Un backup general que incluye el área de usuario, es efectuado una vez por mes. En caso de remoción accidental de un archivo, es posible restaurarlo a partir del backup general efectuado. Pero nada garantiza que el archivo pueda ser restaurado y tampoco que la fecha de remoción coincida con la fecha más próxima del backup general.

5.3.5.3 Seguridad e Integridad de los Datos

- En el caso de que ocurran fallas de disco o sistema, los discos serán restaurados a partir del backup más reciente. De esta forma el usuario deberá estar al tanto de que archivos actualizados o creados, entre la fecha de falla y del backup más reciente, pueden ser perdidos.

- La organización garantiza que los archivos de los usuarios están protegidos al acceso de otros usuarios, siempre y cuando el usuario no altere el permiso de acceso a sus archivos.

- Se obtiene un backup semanal de las bases de datos operativas de tal forma que se garantice la operación de las aplicaciones existentes.

5.3.6 POLÍTICAS DE COMPRA, CONTROL Y ADMINISTRACIÓN DE ANTIVIRUS

5.3.6.1 Compra de Antivirus

El antivirus deberá cumplir con las siguientes características:

a) Deben actualizar los patrones o firmas, por lo menos una vez por semana.
b) La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos

y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.

c) Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.

d) Se deben poder adaptar a las necesidades de diferentes usuarios.

e) Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.

f) Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.

g) Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.

h) Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.

i) No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.

j) El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible.

k) Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.

l) Deben de tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

5.3.6.2 Seguridad de Infección de Virus Informáticos

Controles

a) Control de acceso físico a los equipos.
b) Control de entradas a los programas de la computadora a través de claves de acceso (passwords).
c) Registro, verificación y control de los diskettes, cd's, memorias flash que se conecten a la computadora.
d) Se recomienda algún programa de tipo menú que restrinja los programas que se pueden ejecutar a sólo los autorizados a cada usuario.

Bloqueos

a) Uso del candado o llave de encendido, si la computadora lo tiene.
b) Deshabilitar el acceso desde unidades externas (diskettes, cd's puertos USB).
c) Habilitación de la facilidad de palabra clave (password).
d) Activar la protección anti-virus en BIOS.

5.3.6.3 Actualización Antivirus

a) Instalar el antivirus y asegurar cada 15 días su actualización
b) Utilizar o activar las diversas opciones de protección.
c) Al actualizar el antivirus, verificar el PC completamente. En caso de detectar un virus, proceder a verificar todos loss soportes (diskettes, CD's, ZIP's, etc.)
d) Comprar las versiones actualizadas de las vacunas.
e) Leer la documentación y manuales de los antivirus.

5.3.6.4 Servicios en Línea (navegación – correo electrónico)

a) Para bajar páginas de Internet, archivos ejecutables, etc., definir siempre en nuestra PC una carpeta o directorio para recibir el material. De ese modo sabemos que todo lo que bajemos de Internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.

b) Nunca abrir un adjunto de un e-mail sin antes chequearlo con el antivirus. Si el adjunto es de un desconocido que no avisó previamente del envío del material, directamente borrarlo sin abrir.

c) Verificar contra virus todo programa que se transfiera.

d) Verificar contra virus todo archivo autodescomprimible (aunque sea de datos).

5.3.6.5 Cd's y Memorias Flash

Estos son puntos muy importantes, prácticamente todos los virus se introducen a una computadora por medio de cd's y memorias flash.

a) Verificar contra virus todos los, cd's y memorias flash que se introduzcan en la computadora, aunque sólo sean de datos.
b) No ejecutar programas de origen dudoso.
c) No meter, cd's o memorias flash extraños.
d) Nunca arranque desde cd's en la operación normal de su computadora.
e) Nunca dejar puestos cd's al apagar la computadora.
f) Proteja contra escritura sus discos del sistema, así como sus discos de programas de aplicación.
g) Que los usuarios sólo manejen cd's de datos y nunca de programas.
h) Instalar nuevos paquetes en una máquina que sirva para estudio de comportamiento y que esté un tiempo en observación.
i) Mantener copias respaldo, tanto de los programas, como de los datos.

j) Hacer por separado los respaldos de datos y de programas.
k) Revisar todo cd y memoria flash que provenga del exterior, es decir que no haya estado bajo control, o que haya sido ingresado en la disquetera de otra PC.

5.3.6.6 Otros

a) Capacitar a los usuarios en protección contra virus.
b) Mantenerse informado, o sea leer sobre el tema

5.3.7 POLÍTICAS DE SEGURIDAD LÓGICA

5.3.7.1 De la administración y monitoreo de los servidores.

a) La administración de los servidores debe realizarse únicamente por el personal aprobado por el Área de Sistemas, a fin de mantener consistencia con las Políticas de Seguridad.

b) Deben existir únicamente dos cuentas de usuario de administrador del sistema operativo en los equipos de cómputo o servidores donde residirán los sistemas.

c) El Jefe de Informática debe implantar un sistema de autorización y control de acceso a los archivos compartidos para disminuir la posibilidad de que los usuarios no autorizados puedan leer, escribir, modificar, crear, o borrar datos importantes.

d) En caso de intento o infiltración o contravención a la seguridad o sistemas informáticos de la organización, el Jefe de Informática deberá capturar, grabar y guardar la información o el hecho sospechoso.

e) Es necesario la utilización de sistemas de seguridad Firewall, para detección de intrusos; y el personal encargado de la administración del Firewall deberá ser aprobado por el Área de Sistemas. Se deberá

manejar bitácoras que registre intentos de acceso autorizados y no autorizados.

f) El Jefe de Informática debe revisar periódicamente los logs y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones. A los mismos que los debe conservar por un periodo de por lo menos tres meses.

g) El Jefe de Informática debe garantizar que los servidores estén conectados a UPS, y que estos respondan efectivamente en caso de necesitarlos.

5.3.7.2 De la Asignación de Claves de Monitoreo

a) La administración de la contraseña del o los equipos de cómputo o servidores es responsabilidad del Jefe de Informática .

b) La contraseña de administración y configuración del Firewall, deberá ser de conocimiento del Jefe de Informática.

c) Las Unidades no debe escribir ni colocar la contraseña de la cuenta de administración y configuración del sistema de seguridad en lugares donde pueda ser descubierta por terceros.

5.3.7.3 De las Políticas de Seguridad que se Aplicarán en el Firewall

a) Las políticas de seguridad del o los Firewalls serán instrumentadas y puestas en operación por el Jefe de Informática.

5.3.7.4 Sobre las Licencias de Software y "Copyrights"

a) El Jefe de Informática debe garantizar que todo software que se adquiera para la organización debe estar debidamente licenciado.

b) Los usuarios deben asumir que todo el software de la organización está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

c) Toda otra información que también posea derechos de autor y esté en formato electrónico y que haya sido obtenida de otro equipo, se debe usar con la autorización pertinente.

d) Todo software que se use ya sea para fines administrativos o investigativos debe estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios a utilizarlo. Para la utilización del software "libre" (Open source, freeware, Trial, etc.) debe estar aprobado por el Departamento de Informática.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- La reutilización de la infraestructura tecnológica disponible de la empresa, abarató los costos de la implementación del proyecto, debido a que no se incurrió en gastos elevados en la adquisición de toda la plataforma de hardware y software necesaria, ya que se reestructuró las instalaciones existentes y se adquirió solo una parte de la infraestructura faltante en función de los requerimientos del nuevo esquema de red propuesto.

- El correcto análisis de los requerimientos de cada departamento generó como resultado un sistema informático que cumple con las expectativas de los usuarios, además de asegurar que la información que se administra es oportuna, consistente y correctamente dirigida.

- Una de las áreas que más se benefició de la implementación del Sistema Web fue el departamento de Recursos Humanos, ya que la automatización de sus procesos facilitó la recuperación eficiente de la información y optimizó el tiempo en la gestión de trámites propios del área.

- El análisis de los índices financieros de rentabilidad VAN (USD $6,190.58 cuyo valor es positivo), TIR (30.43%, superior a la tasa de descuento) y PRI (2 años 4.3 meses) constituyeron los principales parámetros para determinar la viabilidad del proyecto, en cada caso los valores calculados se traducen en beneficios para la empresa.

- La agrupación de los usuarios en perfiles (Administrador, Intranet y Extranet) sirvió para obtener una mejor organización de la información y

permitió definir las funcionalidades específicas para cada usuario del sistema

- La fase de pruebas garantizó que la funcionalidad del sistema esté acorde con los requerimientos de los usuarios, y adicionalmente con el uso de las herramientas del ACT (Application Center Test) disponibles en Visual Studio .NET, se pudo medir el desempeño eficiente del sistema.

- La redistribución de la carga transaccional en diferentes servidores, optimizó la operatividad de los ya existentes y la adición de otros con mejores características, contribuyó de manera determinante al momento de realizar el diseño físico de la red, pues facilitó la implementación de una zona desmilitarizada (DMZ) que garantiza la seguridad de los datos y la disponibilidad de los servicios.

- El uso de la metodología UML permitió obtener la documentación completa de todas las fases (captura de requisitos, análisis y diseño) que intervienen en el desarrollo del proyecto, además facilitó la abstracción de los procesos de la empresa y en conjunto con los modelos obtenidos, se logró plasmar los requisitos de los usuarios en una aplicación informática orientada al Internet.

- La utilización de la tecnología .NET agilitó el desarrollo del proyecto debido a que: proporcionó la factibilidad de programar distintos componentes de la aplicación empleando varios lenguajes que se integran en un mismo entorno, complementariamente se pudo disponer de otros componentes ya desarrollados y probados, finalmente se utilizó los asistentes que suministran una buena guía y facilitan el trabajo.

6.2 RECOMENDACIONES

- Se recomienda formalizar un plan de capacitación, concientización y difusión de los usuarios de la empresa Emcosoft, respecto a las políticas de

seguridad, porque la seguridad sólo puede ser efectiva si los empleados conocen su nivel de responsabilidad en la administración de la información, las consecuencias que se producen por un mal manejo de éstas, negligencia en el uso de los recursos informáticos y/o desconocimiento de estas políticas de seguridad.

- Se sugiere que este proyecto sea considerado como base para que la empresa pueda realizar comercio electrónico e integrarse a los negocios a través de Internet (E-Business), que no solo le permitirá comprar y vender directamente sus productos, sino además hacer contactos con posibles nuevos proveedores, clientes y socios estratégicos.

- Se recomienda utilizar este sistema “Intranet / Extranet para una Empresa Comercializadora de Software” como referencia para ampliar la gama de funcionalidades del actual proyecto hacia otros segmentos de la empresa, con la finalidad de llegar a la completa integración de todas las áreas de la organización.

- Debido a que la infraestructura de red y hardware limitarían la capacidad del sistema, no se ha considerado como un requerimiento de la empresa el uso de aplicaciones multimedia (audio y video). Pero con la tendencia a mejorar el ancho de banda, se recomienda aprovechar de mejor manera los recursos de multimedia, para incrementar la interactividad entre los usuarios de la organización tanto en Intranet como en Extranet,

- Se recomienda a la gerencia de la empresa, inicialmente definir un Plan de Recuperación ante Desastres (DRP) debido a la sensibilidad de la información que se transmite por la infraestructura del Internet (DMZ de la empresa), y a mediano plazo definir e implementar un Plan de Continuidad del Negocio (BCP).

GLOSARIO

ACK: (Confirmación) notificación enviada desde un dispositivo de red a otro para confirmar que ocurrió cierto evento (ejemplo la recepción de un mensaje).

Active X: Lenguaje desarrollado por Microsoft para la elaboración de aplicaciones para red capaces de funcionar sobre cualquier plataforma a través, normalmente de www. Permite dar dinamismo a las páginas Web.

ADO+: Es una interface que permite a los programadores tener acceso a bases de datos relacionales y no relacionales. El sistema fue desarrollado por Microsoft para la plataforma .NET.

API: Es un interfaz de programación de aplicaciones (Application Programming Interface), un conjunto de funciones o métodos usados para acceder a cierta funcionalidad.

ASP+: Nueva tecnología de Microsoft que corresponde a la actualización más seria de ASP. Contiene especificaciones y funcionalidades de ASP, junto al acceso de tecnologías como ADO.NET y COM+, así como el manejo de XML.

B2B: Business to Business. Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre empresas. (Por ejemplo una empresa con sus proveedores y no con sus usuarios finales).

Clase: Es la descripción de un conjunto de objetos que comparten los mismos atributos operacionales, métodos, relaciones y semántica.

COM+: Component Object Model. COM+ es el modelo de objetos basados en componentes de Microsoft .NET, una tecnología para construir aplicaciones a partir de componentes binarias de software.

Contenedor: Es un objeto que existe para contener otros objetos y que provee operaciones para acceder sobre su contenido.

CORBA: (Common Objetc Request Broker Architecture), esta arquitectura es un conjunto de objetos y librerías que permiten la creación de aplicaciones que contienen objetos que realizan y reciben peticiones en un entorno distribuido.

DCOM+: (Distributed Component Object Model), es un protocolo que permite a los componentes de software, comunicarse directamente sobre una red de una manera confiable, segura y eficiente. Constituye parte de la tecnología Microsoft .NET.

DES: Encriptador por bloque de 64 bits de longitud. Usa claves de 56 bits. DES es lo suficientemente seguro como para dejar fuera a hackers casuales, sin embargo puede ser quebrado con hardware especial.

DMZ: (Delimitarized Zone), constituye la primera barrera contra la intrusión, creando un foso entre Internet y la red de servicios.

E-Business: Negocio electrónico, entendido como la mejora de las relaciones entre empresas gracias a la conectividad.

E-Commerce: Comercio electrónico, referido a aplicaciones que permiten transacciones e interacciones entre la compañía y el consumidor sobre Internet. También llamadas aplicaciones Business-To-Consumer.

EJB: (Enterprise Java Beans), es la arquitectura de componentes de la parte de servidor para la plataforma J2EE. EJB posibilita el desarrollo rápido y simplificado de aplicaciones Java distribuidas, transaccionales y seguras.

ERP: (Enterprise Resource Planning), es un término industrial para abarcar un conjunto amplio de actividades soportado por una aplicación multimódulos que ayuda a un manufacturero o a las partes más importantes de la administración empresarial.

Escenario: Es la secuencia específica de acciones que ilustran un comportamiento. Un escenario puede ser usado para ilustrar una interacción.

Extranet: Es una Intranet que permite el acceso controlado a usuarios externos mediante la autenticación.

HTTP: (Hipper Text Transfer Protocol), protocolo de transferencia de hipertexto, protocolo de Internet basado en TCP/IP y utilizado para recoger objetos de hipertexto desde sistemas centrales remotos.

HTTPS: URL creada por Netscape Communications Corporation para designar documentos que llegan desde un servidor WWW seguro. Esta seguridad es dada por el protocolo SSL (Secure Sockets Layer), basado en la tecnología de encriptación y autentificación desarrollada por la RSA Data Security Inc.

IIOP: (Internet InterORB Protocol), es un protocolo de comunicación para componentes CORBA. Define el modo que se comunican sobre un medio de objetos CORBA, clientes y servidores.

Intranet: Es una red de computadores conectadas por medio de un protocolo de comunicación TCP/IP, dentro de una empresa u organización, que enlaza a empleados y miembros, facilitando el acceso a la información y convirtiendo el uso de recursos y aplicaciones en un proceso más amigable, funcional y productivo.

IP: (Internet Protocol), es un protocolo básico de Internet. Permite la transmisión (no fiable) de paquetes individuales desde un sistema central a otro. No garantiza si el paquete se entregará o no, cuanto tardará o si los diversos paquetes enviados se entregarán en el orden que se ha enviado.

IPSec: (Internet Protocol Security), es un protocolo que sirve para establecer una sesión segura entre dos hosts que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red, definiendo nuevos formatos de paquete: la cabecera de autentificación (AH), que permite asegurar la integridad de los datos y el ESP (Encapsulating Security Payload), que permite asegurar la privacidad e

integridad de los datos. AH protege la integridad y autenticidad de los datos, incluyendo los campos invariantes de la cabecera IP. Esta cabecera no proporciona confidencialidad, mientras que ESP protege tanto la confidencialidad como la integridad y la autenticidad de los datos. Cuando se usa para comprobar la integridad de los datos no incluye los variantes de la cabecera IP.

JDBC: (Java DataBase Connectivity), es una interface de programación de aplicaciones (API) que permite acceder desde el lenguaje de programación Java, a virtualmente cualquier fuente de datos tabulados.

JSP: (Java Server Pages), permite a los diseñadores y desarrolladores de sitios Web crear rápidamente y mantener de manera sencilla las páginas Web dinámicas, ricas en información sobe las que se basan los sistemas de negocio.

JVM: (Java Virtual Machine), parte del entorno runtime de Java que es responsable de interpretar los bytecodes de Java.

J2EE: (Java 2 Enterprise Edition), soporta un modelo de aplicación distribuida de multinivel basado en componentes escritos en Java.

Kerberos: Permite a los equipos de un dominio de W2000 o de distintos dominios de W2000 entre los que exista una relación de confianza autentificarse los unos a los otros. Se trata del método de autentificación más potente y seguro de los tres.

LDAP: (Lightweight Directory Access Protocol), es un protocolo se servicio de directorio que corre sobre TCP/IP.

L2TP*:* *(Layer 2 Tunneling Protocol)* es un protocolo que permite separar el servidor de conexión de nivel 2 OSI (el que “escucha” en el final de la línea telefónica en un módem por ejemplo) del servidor de PPP. De esta manera el cliente accede a un servidor de conexión (ej. banco de módems) y éste -usando L2TP- se comunica con la red (host) con el que el cliente quiere tener acceso. Esto consigue `juntar' dos segmentos de red (uno de ellos es point-to-point) virtualmente.

Microsoft .NET: Es un conjunto de servicios comunes que pueden ser utilizados desde varios lenguajes.

Objeto: Es una entidad delimitada precisamente y con entidad, que encapsula estado y comportamiento. Es estado es representado por sus atributos y relaciones, el comportamiento es representado por sus operaciones y métodos.

ODBC: (Open DataBase Connectivity), objeto que permite acceder a bases de datos en un entorno protegido. Esta pasarela ofrece la posibilidad de visualizar y modificar el contenido de varias bases de datos existentes.

OMT: (Object Modeling Technique), es una técnica para el modelamiento orientado a objetos.

PKI: La solución que ofrece los mecanismos y elementos necesarios de gestión de información criptográfica para el establecimiento de comunicaciones seguras es lo que se llama PKI (Public Key Infrastructure) o Infraestructura de Clave Pública.

PPP: (*Point-to-Point Protocols*), un conjunto de protocolos estándar que permiten la interacción de software de acceso remoto de diversos proveedores. Una conexión habilitada para PPP puede conectar con redes remotas a través de cualquier servidor PPP normalizado. PPP es la base de los protocolos PPTP y L2TP, que se utilizan en las conexiones protegidas de red privada virtual (VPN). PPP es el estándar principal para la mayor parte de los procesos de equipos de acceso remoto.

PPTP: *(Point-to-Point Tunneling Protocol)* protocolo de encapsulado de PPP sobre IP. Es una especificación desarrollada por un consorcio de fabricantes, entre los que estaban gente como Microsoft, 3Com o U.S. Robotics. El protocolo se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE (Generic Routing Encapsulation). Es una especificación genérica, que permite la adición de diversos mecanismos de autentificación y algoritmos de encriptación. Nótese que

estas técnicas de seguridad no están dentro del protocolo, sino que se añaden a posteriori.

RPC: (Remote Procedure Calls), llamadas remotas a procedimientos o invocación a método mediante el sistema de envío de paquetes de red a un sistema remoto.

Servicios Web: Un servicio Web es una aplicación programable a la que se tiene acceso de forma lógica utilizando los productos estándar de Internet o dicho de otro modo la implementación de los estándares basados en Web para la comunicación transparente entre equipos y aplicaciones.

Servlets: proporcionan a los desarrolladores Web un mecanismo simple y consistente para extender la funcionalidad de un servidor Web y para acceder a los sistemas de negocio existentes.

SOAP: (Simple Object Abstrac Protocol), es básicamente un mecanismo RPC actual, adecuado a los tiempos de Internet. Basado en el estándar XML, se usa para transportar las llamadas y respuestas a través de la Web, sobre el protocolo HTTP, lo cual permite utilizarlo en redes heterogéneas sin importar los lenguajes, sistemas ni plataformas.

SSL: (Secure Socket Layer), protocolo que permite establecer comunicación encriptada entre un navegador Web y un servidor, para mayor seguridad.

TCP/IP: Protocolo de control de transmisión basado en IP, se trata de un protocolo de Internet que proporciona la entrega fiable de datos de un sistema a otro.

UDDI: (Universal Description, Discovery and Integration), protocolo de reciente creación que tiene por objetivo simplificar la descripción y la publicación de servicios, por parte de unas empresas y su descubrimiento e integración por parte de aquellas interesadas en su uso.

URL: localizador de recursos uniforme, estándar para escribir una referencia a texto en una serie de datos en la www.

VPN: (Virtual Private Network), es una configuración lógica de una serie de componentes hardware y software que permite la utilización de redes públicas para establecer canales de comunicaciones privados a los que solo pueden acceder usuarios autorizados.

WSDL: (Web Service Description Language), lenguaje de descripción de servicios web, lenguaje de marcas basado en el estándar XML usado para describir servicios web por parte de las empresas, de tal forma que los clientes puedan acceder a ellos y utilizarlos.

XML: (eXtensible Markup Language), permite definir etiquetas (marcas) que se necesitan para identificar los datos y el texto en un documento XML.

3DES: una variante de DES es Triple DES o 3DES que se basa en el uso del Algoritmo DES (normalmente con la secuencia encrypt-decrypt con claves diferentes no relacionadas).

BIBLIOGRAFÍA

AMUNDESEN Michael, LITWIN Paul: “Creación de Sitios Web con ASP.NET”, Prentice Hall. Madrid, 2002.

CCNA Ver. 3.1 Cisco Networks.

CISA 2006, (Manual de Preparación al Examen) Asociación de Auditoría y Control de Sistemas de Información.

GARRET David: “Harnessing the Power: Intranet Defined”. Intranets Unleashed The Intranet Journal.

JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software” Addison Wesley, Madrid, 2000.

MAXWELL Steve, BREMMER Lynn, ISAI Anthony: “Red Hat Linux: Herramientas para la administración de Redes”.

REILLY Douglas “Diseño para Aplicaciones Microsoft con ASP.NET” Mc Graw Hill. Madrid, 2002.

RUMBAUGH James, BLAHA M., PREMERLANI W. “Object Oriented Modeling and Design” Englewood Cliffs NJ, Prentice Hall 1991.

SAPAG Y SAPAG, “Preparación y Evaluación de Proyectos”, Mc Graw Hill, Santafé de Bogotá, 2000.

REFERENCIAS BIBLIOGRÁFICAS

[1] Cfr. Intranettotal.com. FAQ sobre Intranets (Mayo 2007)

[http://www.intranettotal.com/referencia/faq.htm]

[2] Cfr. Intranettotal.com. FAQ sobre Intranets (Mayo 2007)

[http://www.intranettotal.com/referencia/faq.htm]

[3] Cfr. “Como Funciona una Intranet” Monografías.COM, (Mayo 2007) http://www.monografias.com/trabajos12/intranets.shtml#VISION

[4] Ref. ZULUAGA Juan Fernando. “Las Intranets: resultado del viraje hacia los negocios electrónicos” (noviembre del 2005). “http:// www.intranettotal.com/index.html, 9 de noviembre del 2005.

[5] Cfr.”Ingeniería Del Software Un Enfoque Práctico”. Capítulo 20 Conceptos Madrid 2000 primera ed. Principios Orientados a Objetos Pags. 344. JACOBSON Ivar. Ed. Tercera. Estados Unidos. 1980

[6] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 2. Pags. Ed Addison Wesley. Madrid, 2000 primera ed.

[7] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 2. Ed Addison Wesley. Madrid, 2000 primera ed.

[8] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 7 ‘Captura de Requisitos Como Casos de Uso’. Pags. 125-163. Ed Addison Wesley. Madrid 2000 primera ed.

[9] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 7 ‘Análisis’. Pags. 165-204. Ed Addison Wesley. Madrid 2000 ed. primera

[10] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 9 ‘Diseño’. Ed Addison Wesley. Madrid 2000 ed. Primera

[11] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 8 ‘Diseño’. Pags. 205-253. Ed Addison Wesley. Madrid 2000 ed. primera

[12] Cfr. JACOBSON Ivar, BOOCH Grady, RUMBAUGH James. “El proceso Unificado de Desarrollo de Software”. Capítulo 9 ‘Diseño’. Pags. 205-253. Ed Addison Wesley. Madrid 2000 ed. primera

[13] Cfr. MAC KAY Patrick “de ASP.NET a SQL, Encriptación Simétrica” http://msmvps.com/blogs/pmackay/default.aspx, Noviembre 2004 http://www.microsoft.com/spanish/msdn/comunidad/mtj.net/voices

[14] Cfr. LUCENA LÓPEZ Manuel J. “Criptografía y Seguridad en Computadores”, Tercera Edición (Versión 2.14). Febrero de 2004

[15] Cf. ALVAREZ MARAÑON Gonzalo, Secure Socket Layer (SSL)”,http://www.iec.csic.es/criptonomicon/ssl.html, “ Marzo 2007

[16] Cfr. MAC KAY Patrick , “de ASP.NET a SQL, Encriptación Asimétrica” http://www.microsoft.com/spanish/msdn/comunidad/mtj.net/voices

[17] Harkins D., Carrel D., RFC 2409, The Internet Key Exchange (IKE), November 1998

[18] Cfr. http://www.microsoft.com/latam/windowsserver2003/docs/overview_win_server2003.pdf

[19] Cfr. DVD de Linux Magazine. “Fedora Core 3”, 22 de noviembre del 2004. Pág. 96-97.

[20] Cfr. http://www.ucpr.edu.co/Auditores/basesdatos/index.htm.

[21] Cfr. http://windowsxp.ethek.com/WindowsXP/contenido.asp?IDContenido=712, marzo del 2007.

[22] Cfr. Características de IIS. http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch08s02.html, marzo 2007.

[23] Cfr. “Servidor Exhange 2003” (Marzo 2007) Microsoft Corporation. http://www.microsoft.com/spain/servidores/exchange/evaluacion/10_razones.asp

[24]Cfr. www.microsoft.com/spain/servidores

[25] Cfr. Symantec Enterprise Securiry CD “Portafolio de Productos y Servicios ” V.3

[26] Cfr. información tomada de la publicación de Symantec CD productos 2007

[27] Cfr. http://www.cisco.com....

[28] Cfr. SAPAG Y SAPAG, “Preparación y Evaluación de Proyectos”, McGraw Hill, Santafé de Bogotá, 2000

[29] Cfr. http://www.lab.dit.upm.es/~lprg/material/apuntes/pruebas/testing.htm#s1, marzo 2007

[30] Cfr.ISACA (Information Systems Audit and Control Association)“Manual de Preparación al Examen CISA 2006” Illinois USA