Universidad Nacional Autónoma de México

Facultad de Ingeniería

Sistema integral de banca por Internet

T E S I S
Que para obtener el título de
Ingeniero en computación
P r e s e n t a:
Sebastián Mantilla Beniers

Director: Juan José Carreón Granados

México D.F. Marzo 2004

Tabla de contenido

Agradecimiento 10

Dedicatoria 12

Tablas 14

Diagramas 14

Pantallas 14

Código 15

Capítulo 1 Antecedentes e Introducción 16

Antecedentes 16

Introducción 18

Capítulo 2 Objetivos 22

Objetivo general 22

Objetivos particulares 22
Sistema de administración de contenido 22
Sistema aplicativo o transaccional 23
Seguridad 24
Consideraciones 24

Capítulo 3 Diseño de la solución 26
El sistema en su conjunto 26
Plan de trabajo 26
Cronograma 27
Configuración de los componentes del sistema base 36
Configuración del servidor de páginas 36
Configuración de PHP 41
Configuración de Zend 50
El sistema de administración de contenido 51
Selección 52
eZ Publish 52
Sistema de administración de contenido (SAC/CMS) 52
¿A quién está dirigido? 53
Separación de contenido y código. 53
Internacionalización. 53
Independencia de plataforma y navegador. 54
Velocidad y cache. 54
Sin límites. 54
Preferencias del usuario y sesiones. 54
Especificaciones técnicas de eZ Publish. 54

Software que se necesita para ejecutarlo. ... 55
Equipo necesario ... 55
Diseño gráfico ... 59
eZBancos ... 69
eZTasas ... 69
eZ Publish Desktop Edition ... 70
El sistema aplicativo o transaccional ... 75
eZTransaccion ... 77
eZUserBB ... 78
La seguridad ... 78
Sistema Operativo ... 84
LIDS ... 84
PortSentry ... 85
HostSentry ... 85
Log Check ... 85
Aplicaciones ... 85
Datos ... 86

Capítulo 4 Construcción de la solución ... 88

Implementación del IVA ... 88
Adecuación y ampliación ... 88
Traducción ... 88

Introducción a la construcción de módulos en eZ Publish. ... 93
eZ Publish como marco de construcción (framework) ... 93

Sistema de manejo de contenido ... 93
ezBancos ... 95
Descripción ... 95
Clase ... 95
La base de datos ... 98
Pantallas ... 99
Código ... 100
Plantilla ... 102
Archivo de localización ... 104
ezTasas ... 104
Descripción ... 104
Clase ... 104
La base de datos ... 108
Pantallas ... 110
Código ... 113

Sistema aplicativo o transaccional ... 115
ezTransaccion ... 115
Descripción ... 116
Código ... 117
Plantilla ... 119
ezUserBB ... 121
Descripción ... 121
Pantallas ... 122
Código ... 124

Seguridad ... 125
Sistema Operativo ... 126

LIDS 126
Descripción 126
Configuración 127
PortSentry 135
Descripción 135
Configuración 136
HostSentry 140
Descripción 140
Configuración 144
Tripwire 145
Descripción 145
Configuración 146
Logcheck 161
Descripción 161
Configuración 161
ssh 164
Descripción 164
Configuración 164
GRUB 166
Descripción 166
Configuración 166
Aplicaciones 167
Libsafe 167
Descripción 167
Configuración 168
Datos 169
Apache 171
Bitácoras 171

Capítulo 5 Operación 176

Procedimientos de Operación 176
Alta del servidor o los servicios 176
Baja del servidor 182

Procedimiento Monitoreo 182
BigSister 182
Configuración ejemplo 183
Pantallas de muestra del resultado del monitoreo 184
Correos electrónicos: muestra de los resultados de monitoreo. 186

Capítulo 6 Resultados y conclusiones 190

Resultados 190

Resultado general 190

Resultados particulares 190
Sistema de administración de contenido 190
Sistema aplicativo o transaccional 192
Seguridad 194

Conclusiones 195
El sistema en su conjunto 195

El sistema de administración de contenido 196
El sistema aplicativo o transaccional 198
La seguridad 198

A futuro 198
Administrador de transacciones 198
Portal 198
Personalización 199

Glosario 200

A 200

B 201

C 202

D 203

E 204

F 204

G 205

H 205

I 206

J 207

K 207

L 207

M 207

N 208

O 209

P 209

Q 210

R 210

S 210

T 211

U 211

V 211

W 212

X 212

Y 213

Z 213

Glosario de traducciones 214

Bibliografía 216

Notas 220

Agradecimiento

A todos los mexicanos que pagamos impuestos, sin los cuales no existiría esta gran Universidad.
A quienes crearon a la UNAM como una universidad pública y gratuita.
A todos los universitarios que hemos luchado por mantener a la Universidad pública y gratuita.
A la UNAM que me dio mis estudios.
A mis profesores y compañeros.
A mis compañeros de IAC.
Al equipo de BB.
A mi familia y amigos.

Dedicatoria

A mi padre quien me hubiera encantado que viera este trabajo y a su nieta.
A mi madre quien en todo momento me ha apoyado y ayudado con un inmenso amor.
A Nativer porque su ejemplo en la academia me ha motivado a seguirlo intentando hasta lograrlo.
A mi Piojita con quien he hecho un gran equipo y una hermosa familia.
A Camille Juliette por ser tan extraordinaria en todo sentido.

Tablas

Diagramas

Diagrama 1 Arquitectura. 19
Diagrama 2 Conectividad. 19
Diagrama 3 Estructura de módulos de eZ Publish. 56
Diagrama 4 Flujo de la atención a una petición. 65
Diagrama 5 Caso de uso eZ Bancos. 69
Diagrama 6 Caso de uso eZTasas. 70
Diagrama 7 Caso de uso genérico de una transacción. 76
Diagrama 8 Un caso de uso genérico de una transacción que incluye los módulos encargados de su atención. 77
Diagrama 9 Diagrama conceptual del diseño de seguridad. 83
Diagrama 10 Integración de la seguridad. 84
Diagrama 11 Funcionamiento general de una transacción. 116
Diagrama 12 Procesamiento de una transacción. 117
Diagrama 13 La seguridad en la solución. 126
Diagrama 14 Kernel + LIDS. 127
Diagrama 15 Funcionamiento de Tripwire. 146
Diagrama 16 Integración de mod_ssl en Apache. 171
Diagrama 17 Granja de servidores que atiende hoy en día Bajionet. 195

Pantallas

Pantalla 1 Módulo ezArticle, administración, alta artículo. 58
Pantalla 2 Módulo ezArticle, usuario, despliegue artículo. 59
Pantalla 3 eZ Publish Desktop Edition, administración, listado de artículos en bajionet. 71
Pantalla 4 eZ Publish Desktop Edition, administración, propiedades de un artículo. 72
Pantalla 5 eZ Publish Desktop Edition, administración, modificación del contenido de un artículo. 73
Pantalla 6 eZ Publish Desktop Edition, administración, modificación de una imagen. 74
Pantalla 7 eZ Publish Desktop Edition, administración, listado de imágenes de una categoría. 74
Pantalla 8 Herramienta de traducción: QtLinguist. 91
Pantalla 9 Página de traducciones de eZ Publish. 92
Pantalla 10 Módulos activos en una configuración normal. 94
Pantalla 11 Módulos activos en la configuración de BB. 94
Pantalla 12 Módulo eZBancos, administración, administración de la relación de bancos. 100
Pantalla 13 Módulo ezTasas, administración, alta tasas. 111
Pantalla 14 Módulo ezTasas, administración, vigencia de las tasas. 112
Pantalla 15 Módulo ezTasas, usuario, comparativo de tasas. 113
Pantalla 16 Módulos ezUserBB, usuario, pantalla para establecer sesión. 122
Pantalla 17 Módulos ezUserBB, usuario, que aparece cuando se intenta acceder a las transacciones sin haber establecido previamente una sesión. 123
Pantalla 18 Módulos ezUserBB, usuario, cuando los datos de usuario o clave no son válidos. 124
Pantalla 19 Página principal de un servidor de despliegue de BigSister. 185
Pantalla 20 Página de detalle sobre el estado de un servicio. 185
Pantalla 21 Página principal con la configuración corregida. 186
Pantalla 22 Correo con aviso de BigSister notificando que la carga disminuyó y por ello el servidor salió del estado crítico en el que se encontraba. 187
Pantalla 23 Correo con aviso de BigSister notificando que el servicio de correo dejo de contestar y por ello el servidor se encuentra en estado crítico (status red). 188
Pantalla 24 Página principal. 196
Pantalla 25 Páginas de información. 197
Pantalla 26 Páginas del administrador. 197

Código

Código 1 Archivo ks.cfg utilizado en la instalación de servidores. 33
Código 2 Configuración del DNS, para el dominio bb.com.mx. 35
Código 3 Configuración del servidor de páginas, sección módulos. 36
Código 4 Configuración del servidor de páginas, sección virtualhosts. 40
Código 5 Configuración de php. 49
Código 6 Configuración de Zend. 50
Código 7 El archivo frame.php tal como se adecuó para el proyecto. 64
Código 8 Ejemplo de un archivo .ini. 89
Código 9 Ejemplo de un archivo .ini traducido. 90
Código 10 Ejemplo de un archivo .ts (fragmento). 90
Código 11 La clase eZBancos. 98
Código 12 El controlador del módulo eZBancos. 101
Código 13 La operación catálogo del módulo eZBancos. 102
Código 14 La plantilla para la operación catálogo del módulo eZBancos. 103
Código 15 El archivo de internacionalización para la operación catálogo del módulo eZBancos. 104
Código 16 La clase eZTasas. 108
Código 17 La operación consultatasas del módulo eZTasas. 115
Código 18 Programa datasupplier.php para el módulo ezTransaccion (fragmento). 118
Código 19 Método PostToHost de la clase ezTransaccion, del módulo ezTransaccion. 119
Código 20 Plantilla para una transacción. 119
Código 21 Del menú de las transacciones (fragmento). 121
Código 22 De la plantilla del menú. 121
Código 23 Fragmento del código de validación de usuarios con el servidor bancario. 125
Código 24 Manejo de las variables de sesión. 125
Código 25 Script para establecer el comportamiento de LIDS. 134
Código 26 Configuración de portsentry. 140
Código 27 Configuración de hostsentry. 145
Código 28 Archivo de políticas de Tripwire. 161
Código 29 Configuración de logcheck, hacking. 162
Código 30 Configuración de logcheck, ignore. 163
Código 31 Configuración de logcheck, violations. 164
Código 32 Configuración de logcheck, violations ignore. 164
Código 33 Configuración de sshd. 166
Código 34 Archivo grub.conf encargado del control del sistema de carga del sistema operativo. 166
Código 35 Configuración de libsafe. 168
Código 36 Código antes de compilar (datasupplier eZTasas). 169
Código 37 Código compilado (datasupplier eZTasas). 169
Código 38 Configuración y activación de los distintos elementos de seguridad. 171
Código 39 Ejemplo de un reporte preparado por logcheck (fragemento). 173
Código 40 Archivo de configuración de BigSister utilizado para realizar un monitoreo local-local. 183

Capítulo 1 Antecedentes e Introducción

Antecedentes

Un banco en Internet es la versión electrónica, pública y segura de un banco tradicional. A través de Internet un banco puede ofrecer a sus clientes, actuales y potenciales, los servicios que ofrece en sus sucursales.

Los servicios de un banco en Internet son muy variados: tan simples como la consulta de saldos, o tan complejos como apertura de cuentas, transferencias de fondos e inversiones. Naturalmente, una de las preocupaciones principales de un banco en Internet es la seguridad de las transacciones que realiza; los servicios del banco deben brindarse en un marco seguro de comunicaciones, de información y de las transacciones, para la tranquilidad tanto del cliente como del mismo banco.

Dadas las tendencias actuales de globalización y competitividad es fundamental para las organizaciones financieras buscar un espacio en el aguerrido mundo electrónico a través de las telecomunicaciones. Contar desde ya con una presencia de calidad en el ámbito de lo que será el movimiento de información de los próximos años, tanto personal como empresarialmente hablando, ha dejado de ser una posibilidad o un lujo, para convertirse en una imperante necesidad.

Es por ello que Banco del Bajío (BB) - que es uno de los pocos sobrevivientes de una nueva generación de bancos de alcance nacional que, a pesar de tener representación en prácticamente todos los estados del país, es más un banco regional que nacional - decidió ofrecer a sus clientes servicios de banca por Internet.

Banco del Bajío utiliza como plataforma bancaria Ovation, un sistema desarrollado por Prologic, una compañía canadiense. Gracias a varios años de desarrollo del banco, Ovation se encuentra ya totalmente adaptado a la legislación y a las necesidades nacionales. Ovation ofrece un módulo para que los bancos ofrezcan banca por Internet a sus clientes, sin embargo, por la funcionalidad ofrecida en comparación con las necesidades de Banco del Bajío se optó por construir una solución propia.

A lo largo de este trabajo revisaremos las soluciones que se implementaron para construir la banca por Internet para Banco del Bajío.

El resultado de este proyecto dio origen a Bajionet, la banca por Internet de Banco del Bajío.

Ilustración 1 Logotipo de la banca por Internet de Banco del Bajío.

Esta tesis es el resultado del ejercicio de la práctica profesional que se corresponde con la carrera de Ingeniería en Computación que imparte la Facultad de Ingeniería de la Universidad Nacional Autónoma de México y fue desarrollada en el marco de un contrato de prestación de servicios profesionales entre Banco del Bajío e Internet de Alta Calidad, la empresa donde laboro.

Introducción

En este trabajo se va a desarrollar un Sistema Integral de banca por Internet; puesto que se tratan los aspectos de:

- administración de contenido
- aplicación transaccional
- seguridad

que en su conjunto brindan todo lo necesario para ofrecer los servicios de banca por Internet a los clientes de un banco; por ello se le denomina integral.

Al conjunto de herramientas que conforman la solución se le ha denominado IVA - Internet Virtual Appliance for Internet Banking. El IVA es un producto que permite proporcionar a los clientes de un Banco un medio de acceso moderno, seguro, ágil y confiable a los servicios financieros que se brindan en una sucursal tradicional, pero desde la comodidad de su casa u oficina, sin importar dónde se encuentre el cliente, y sin estar sujeto a un horario específico de atención al público.

Esta tesis es una visión global a un sistema integral de banca por Internet, por esta razón en ninguno de los tres aspectos fundamentales del proyecto se hace una revisión con gran detalle, sin embargo, sí se tratan con el suficiente para resaltar sus características, ventajas y capacidades.

De los alcances de este trabajo quedan excluidos temas importantes como son: el aseguramiento de la calidad de los sistemas, entendidos como equipo, software base y aplicaciones y el aseguramiento de calidad de los programas, las pruebas de carga y la optimización correspondiente al análisis de los resultados obtenidos, los sitios adicionales al de contenido y transaccional que componen la solución, la seguridad de los dispositivos externos, Cisco PIX, cajas SonicWall, tarjetas aceleradoras de SSL, la administración del proyecto y del código. Y aunque se mencionan, hay actividades o temas que no se desarrollan con la profundidad que hubiera sido deseable, entre ellos está la creación del disco compacto de instalación y la revisión de las bitácoras.

En este trabajo se asume que el lector está familiarizado con sistemas operativos tipo Unix, el lenguaje de programación PHP, bases de datos SQL, programación orientada a objetos y HTML, de tal suerte que en muchos casos no se hace una explicación detallada o profunda de algún aspecto que se está tratando, por considerarse que el lector tiene las bases para comprender el trabajo sin dicha explicación.

Con la idea de introducir al lector en el sistema que nos concierne, en el siguiente (diagrama 1) diagrama de arquitectura, se muestra el conjunto de herramientas y dispositivos que conforman la solución. Este diagrama es útil para entender la relación entre las herramientas, los programas, la aplicación transaccional y la aplicación de manejo de contenido.

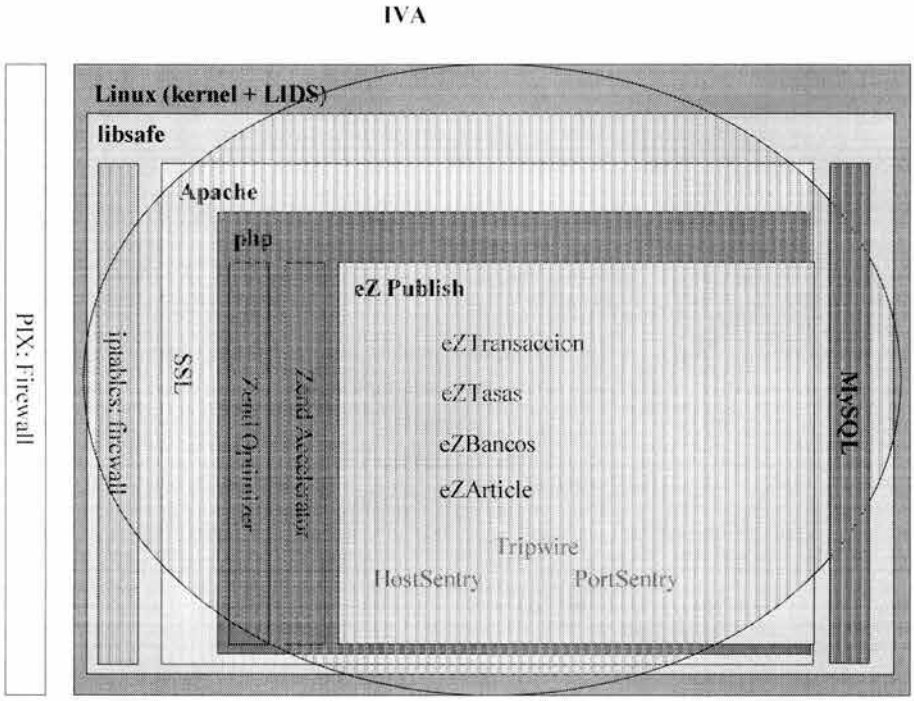


Diagrama 1 Arquitectura.

Desde la perspectiva de conectividad, los servicios de banca por Internet llegan hasta los clientes a través de las siguientes (diagrama 2) conexiones.

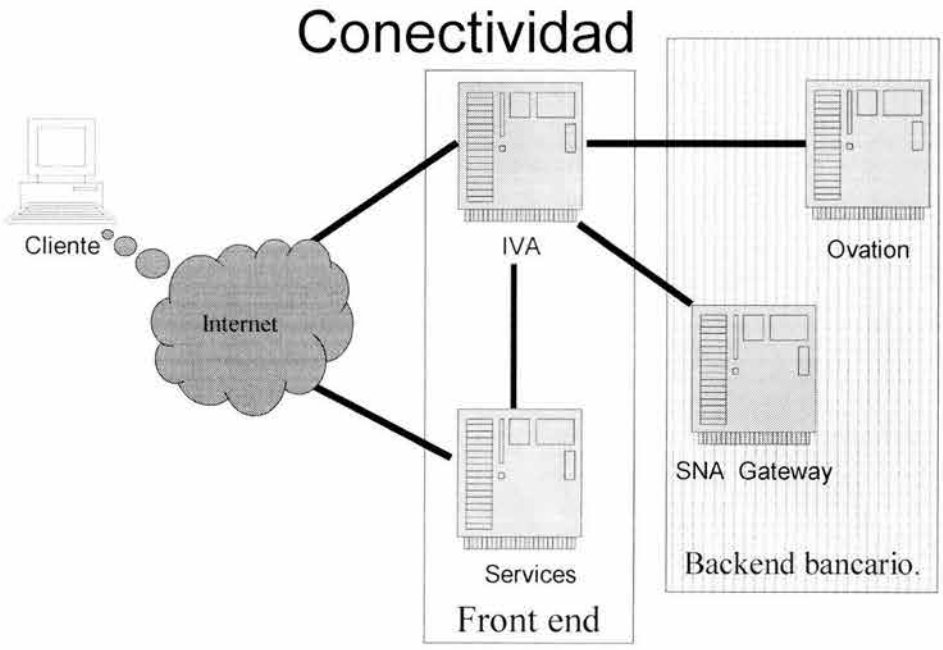


Diagrama 2 Conectividad.

La organización de este trabajo es la siguiente: el capítulo dos establece los objetivos, tanto generales como particulares. En el capítulo tres se lleva a cabo el diseño de la solución, abordando todos los aspectos que fueron considerados tanto en la selección de herramientas como en la programación y los elementos de seguridad. El capítulo cuatro detalla la construcción, incluyendo aspectos como el plan de trabajo, el sistema base y el detalle de los demás componentes. El capítulo cinco habla sobre los aspectos de operación de la solución, tanto tareas cotidianas, como el monitoreo. El último capítulo hace un resumen de los resultados y expone las conclusiones.

Capítulo 2 Objetivos

Objetivo general

Construir un sistema integral de banca por Internet que ofrezca una disponibilidad de servicios de 7 x 24 x 365, que pueda crecer y satisfacer una demanda creciente, sin comprometer ninguno de sus parámetros y que permita a los clientes encontrar toda la información relevante sobre los productos y servicios del banco así como efectuar desde Internet toda clase de operaciones bancarias en tiempo real, con el mayor grado de seguridad y confiabilidad, con lo que se aumente la capacidad de atención y la calidad de los servicios.

Objetivos particulares

Sistema de administración de contenido

A continuación se presenta un listado de los requerimientos que se han planteado para el sistema de administración de contenido:

- Permitir el acceso directo de los clientes
  - a un buzón de sugerencias,
  - a la descripción del 100% los productos y servicios del banco,
  - a los detalles del 100% de sucursales y cajeros automáticos,
  - a las preguntas más frecuentes de nuestros clientes y a la liga a las respuestas y
  - a la información sobre seguridad pertinente para los servicios de banca por Internet en el momento en que el portal esté al aire.
- Permitir el cambio del tipo de letra, imagen de fondo y formato de fechas sin tener que modificar todos y cada uno de los documentos que formen parte del sitio.
- Contar con la capacidad de incluir imágenes en la información que se incorpore al portal.
- Impartir capacitación del sistema de administración de contenido y operación.
- Impartir capacitación sobre el desarrollo de temas y plantillas.
- Contar con la capacidad de ofrecer a los clientes un comparativo de las tasas de interés que ofrece el banco contra las que ofrecen otros bancos.
- Contar con la capacidad de delegar la administración del contenido al área de mercadotecnia.
- Reflejar una imagen moderna y de servicios financieros de alto nivel con noticias financieras y de negocios, así como un recuadro con principales indicadores financieros.
- Desarrollar un encabezado y un pie de página que serán comunes a todas las páginas del sitio.
- Establecer el control de acceso a los distintos módulos del sistema de acuerdo a usuarios, claves y privilegios asignados.
- Construir el sistema asegurando que será de fácil manejo.
- Desarrollar el sistema para que todos los cambios al contenido se reflejen inmediatamente.
- Desarrollar el sistema para que administre todo el contenido del portal, es decir para que tenga carácter integral.
- Generar automáticamente un mapa del sitio con el contenido que ha sido publicado.
- Construir un motor de búsqueda integrado al sistema.

- Ofrecer la facilidad de mostrar una presentación de la información previa a su publicación.
- Permitir que desde la página principal se acceda directamente a Bajionet, la parte del sitio donde se puede realizar operaciones bancarias.
- Lograr rapidez, utilizando como métrica de referencia las evaluaciones que proporcionan sitios especializados en la medición del desempeño de sitios en Internet.
- Dar un carácter uniforme al manejo y a la presentación del sistema.

Sistema aplicativo o transaccional

A continuación se presenta un listado de los requerimientos que se han planteado para el sistema aplicativo.

Permitir el acceso directo de los clientes a las siguientes transacciones:

- Cambio de clave de acceso.
- Clave mancomunada (Empresas).
- Consulta de movimientos.
- Consulta de saldos en cuentas de vista, créditos e inversiones (que se despliegue automáticamente al entrar).
- Consultas de estado de cuenta.
- Generación de órdenes de pago interbancario (SPEUA, IDEA, EDI) con cargo a una cuenta de vista.
- Inversiones (Plazos, bajío premier).
- Inversión a plazo fijo con cargo a una cuenta de vista.
- Operaciones con cheques.
- Operaciones con tarjetas de débito.
- Pago de impuestos con cargo a una cuenta de vista.
- Pago de servicios (luz, teléfono, colegiaturas, agua, etc. con cargo a una cuenta de vista).
- Pagos a terceros con cargo a una cuenta de vista, ejemplo: pago a proveedores.
- Proceso y dispersión de nómina electrónica con cargo a una cuenta de vista.
- Reporte de robo o extravío de cheques y tarjetas de débito.
- Reposiciones de tarjeta, reexpedición de NNIIPP.
- Tesorería Empresarial (concentración y dispersión de fondos).
- Transferencias de fondos (propias, terceros, ligas a cuentas de terceros, SPEUA, Pago Interbancario, verificación de cuentas).
- Tasas y tipo de cambio

en el momento en que el portal esté al aire.

- Construir el sistema asegurando que será de fácil manejo.
- Construir el sistema con la modularidad suficiente para asegurar que será a través de él que los clientes realizarán todas las operaciones que puedan realizar utilizando Internet (integral).
- Construir el sistema utilizando técnicas de programación de orientación a objetos.
- Construir el sistema garantizando que no presentará fallas[i]; es decir, lograr robustez.
- Construir el sistema para que los tiempos de respuesta a las peticiones de los clientes sea el menor posible (rápido).

Seguridad

La seguridad debe abarcar todos los aspectos de la solución, es decir debe incluir protección desde el sistema operativo hasta la aplicación en si, pasando por las herramientas intermedias que intervienen.

Es por ello que el objetivo es que nunca el sistema sea comprometido, ni a nivel de sistema operativo o herramientas ni a nivel de aplicación. Estamos hablando de que nunca sufra una intrusión.

El objetivo con respecto a la seguridad del contenido es muy simple: nunca deberá ser modificado por alguien que no cuente con la autorización respectiva para hacerlo.

Por lo que respecta a las transacciones bancarias el parámetro es que nunca se debe permitir realizar una transacción a alguien que no se haya autenticado como el legítimo cliente.

En cuanto a la información de los clientes y su información financiera esta nunca debe ser vista por alguien distinto del cliente mismo.

Consideraciones

En la solución se debe considerar lo siguiente:

- No todos los clientes tienen acceso a todos los servicios.
- No todas las operaciones financieras utilizan la misma secuencia. Algunas operaciones se realizan en un paso, otras en dos pasos y algunas requieren de tres.

Tómese en cuenta la plataforma tecnológica del Banco:

- Sistema operativo: Linux
- Base de datos: PostgreSQL
- Servidor de páginas: Apache
- Lenguaje de desarrollo: PHP

Capítulo 3 Diseño de la solución

El sistema en su conjunto

El sistema en su conjunto son los servidores y los servicios - de páginas, de transacciones y de nombres - que deben operar para ofrecer servicios de banca por Internet y las aplicaciones de administración de contenido y transaccional que van a residir en dichos servidores.

Para construir la solución buscaremos tener:

- sistema operativo
- herramientas
- servicios
- aplicaciones

trabajando armónicamente en un ambiente seguro.

Con tal finalidad, utilizaremos nuestra experiencia en el manejo de la tecnología Internet, diseño gráfico y entornos de operación y configuración UNIX.

Plan de trabajo

El grupo de trabajo para el proyecto con Banco del Bajío se integró por dos equipos, uno del banco, otro de la empresa, conformados de la siguiente manera:

- El equipo del Banco
    - Un coordinador de proyecto por parte del Banco
        - Carlos Rocha
    - Un encargado del contenido y diseño gráfico
        - Alan Maciel
    - Un encargado del backend del banco
        - Ana Carolina Blanco
- El equipo de Internet de Alta Calidad
    - Un coordinador del proyecto por parte de Internet de Alta Calidad
        - Juan Carlos Lozada
    - Un desarrollador por parte de Internet de Alta Calidad
        - Sebastián Mantilla Beniers

Los productos de los servicios se identifican como los entregables para este proyecto, los cuales hemos estructurado en las siguientes fases:

Fase 1: Desarrollo del IVA.
Fase 2: Instalación de la infraestructura.
Fase 3: Transferencia tecnológica.
Fase 4: Soporte técnico post-liberación.

Actividad	Número Horas / hombre
Preparación de un documento de requerimientos	40
Manual de identidad gráfica electrónica	40
Estimación de infraestructura necesaria	10
Manual de la arquitectura de información	40
Implementación del IVA: Presentación, negocios, datos y gateway transaccional	100
Proceso de pruebas automatizadas	40
Pruebas de seguridad	20
Transferencia tecnológica	80

Cronograma[ii]

De acuerdo al análisis preliminar realizado se han identificado una serie de actividades para este proyecto. Las presentamos a continuación.

- Integración transaccional
- Especificación funcional
- Construcción
- Presentación
- Validación
- Manejador de la transacción
- Gateway al backend
- Bitácoras y auditoría
- Pruebas unitarias
- Estimación de infraestructura
- Instalación de la infraestructura
- Instalación de software base
- Instalación y configuración del IVA
- Instalación y configuración de herramientas de monitoreo y seguridad
- Pruebas de volumen
- Pruebas de seguridad
- Optimización y puesta a punto

- Transferencia Tecnológica
- Desarrollo de Procedimientos de Operación
- Desarrollo de Procedimientos Monitoreo
- Desarrollo de Procedimientos Auditoría
- Desarrollo de Procedimientos Actualización y Cambio de Contenido del Sitio
- Capacitación a Operadores o Webmasters

- Soporte técnico post-liberación

El primer paso es por tanto el sistema operativo, y por los requerimientos que se establecieron en las consideraciones de los objetivos, el primer paso fue seleccionar una distribución[iii] de Linux sobre la cual se construiría la solución.

Se selecciona una distribución en lugar de construir el sistema desde las fuentes de cada elemento porque así se obtiene una solución en menor tiempo, sin perder la capacidad de personalizar o adaptar a necesidades específicas todo aquello que lo requiera, gracias a que, en general las distribuciones tienen una herramienta de administración de paquetes[iv] que permite, a partir de los fuentes de cada paquete, volver a construir los binarios específicos de una plataforma haciendo cualquier modificación necesaria, sin perder control ni capacidades. Además, al utilizar una distribución se tiene acceso a una comunidad de usuarios muy numerosa que puede ayudar en la solución de problemas, se puede contratar soporte técnico en caso de ser necesario. Una distribución tiene documentación, hay medios o imágenes de los medios y se pueden utilizar estas para hacer instalaciones automatizadas y personalizadas.

Por la experiencia que se tenía con ella, la distribución seleccionada fue RedHat Linux. Sobre ella se hicieron las modificaciones necesarias para construir el sistema.

Tenemos que RedHat Linux ofrece todos los servicios y las herramientas que se necesitan para la solución para el Banco a saber:

- Servidor de páginas (apache) con soporte para PHP y SSL.
- PHP.
- DNS.
- Manejador de bases de datos (PostgreSQL y MySQL).
- PortSentry.
- HostSentry.
- LogSentry.
- Zend Encoder[v].
- Zend Optimizer.
- Zend Accelerator.

Una vez seleccionada la distribución, el siguiente paso fue hacer una selección de los paquetes que se instalarían, los servicios que estarían activos en un sistema instalado, la configuración de los servicios activos, la configuración de las herramientas que la requirieran, los parámetros básicos de red, la clave inicial del administrador y las particiones del disco duro. Con esta información se definió un archivo de kickstart[vi].

```
lang en_US
langsupport en_US
keyboard us
mouse generic3ps/2
timezone --utc America/Mexico_City
rootpw --iscrypted $1$óÞiwÆÙÐÝ$Q1P8DlNkZiljq.D87Sbq8.
reboot
text
bootloader --location=mbr
install
cdrom
clearpart --all --initlabel
part / --fstype ext3 --size 750
part /usr --fstype ext3 --size 3500
part /home --fstype ext3 --size 750
part /var --fstype ext3 --size 750 --grow
part  swap --size 1000 --grow --maxsize 2000
network --bootproto static   --ip 192.1.2.143   --netmásk 255.255.0.0   --gateway 192.1.1.1   --
nameserver 192.1.1.142
```

```
auth  --useshadow  --enablemd5
firewall --enabled
#Do not configure the X Window System
skipx
%packages
rdist
console-tools
eject
gpm
hdparm
hotplug
kbdconfig
libstdc++-devel
mouseconfig
pciutils
quota
reiserfs-utils
setserial
anacron
apache
apache-devel
ash
aspell
at
authconfig
autoconf
automake
basesystem
bash
bc
bdflush
bind
bind-devel
bind-utils
binutils
bison
byacc
bzip2
bzip2-devel
bzip2-libs
cdecl
chkconfig
cpio
cpp
cracklib
cracklib-dicts
crontabs
ctags
curl
curl-devel
cvs
cyrus-sasl
cyrus-sasl-devel
cyrus-sasl-md5
cyrus-sasl-plain
db1
db1-devel
db2
db3
db3-devel
db3-utils
dev
dhcpcd
diffstat
diffutils
dosfstools
e2fsprogs
ed
expat
expat-devel
```

```
file
filesystem
fileutils
findutils
flex
freetype
gawk
gcc
gcc-c++
gd
gd-devel
gdb
gdbm
gdbm-devel
gettext
glib
glibc
glibc-common
glibc-devel
gmp
gmp-devel
gnupg
grep
groff
gzip
apmd
dev86
grub
lilo
ltrace
mkbootdisk
syslinux
indent
indexhtml
info
initscripts
ipchains
iproute
iptables
iputils
kernel
kernel-headers
krb5-libs
ksymoops
kudzu
kudzu-devel
lclint
less
libjpeg
libjpeg-devel
libpng
libpng-devel
libstdc++
libtermcap
libtermcap-devel
libtiff
libtiff-devel
libtool
libtool-libs
libxml2
lockdev
lockdev-devel
logrotate
logwatch
lokkit
losetup
lsof
lv
m4
mailcap
```

```
mailx
make
MAKEDEV
man
man-pages
mc
mingetty
mkinitrd
mktemp
mm
mm-devel
mod_ssl
modutils
mount
mrtg
mt-st
mysql
mysql-server
ncftp
ncompress
ncurses
ncurses-devel
net-tools
netconfig
netpbm
netpbm-devel
newt
newt-devel
njamd
nmap
nscd
ntsysv
openjade
openldap
openldap-devel
openssh
openssh-clients
openssh-server
openssl
openssl-devel
pam
pam-devel
parted
passwd
patch
pax
pciutils-devel
pcre
pcre-devel
perl
perl-SGMLSpm
php
php-mysql
pidentd
pine
pinfo
pmake
popt
procinfo
procmail
procps
psmisc
pspell
pwdb
python
python-devel
raidtools
rcs
rdate
readline
```

```
readline-devel
redhat-logos
redhat-release
rootfiles
rpm
rpm-build
rpm-devel
rsync
screen
sed
sendmail
sendmail-cf
setup
setuptool
sgml-common
sgml-tools
sh-utils
shadow-utils
slang
slang-devel
slocate
stat
strace
sudo
swig
symlinks
sysklogd
sysstat
SysVinit
tar
tcl
tcp_wrappers
tcpdump
tcsh
termcap
texinfo
textutils
time
timeconfig
tmpwatch
traceroute
tree
units
utempter
util-linux
vim-common
vim-minimal
vixie-cron
webalizer
wget
which
whois
words
xdelta
xinetd
zlib
zlib-devel
%post
/sbin/chkconfig --level 345 httpd on
/sbin/chkconfig --level 345 anacron on
/sbin/chkconfig --level 345 atd on
/sbin/chkconfig --level 345 crond on
/sbin/chkconfig --level 345 keytable on
/sbin/chkconfig --level 345 kudzu on
/sbin/chkconfig --level 345 linuxconf on
/sbin/chkconfig --level 345 mysqld on
/sbin/chkconfig --level 345 network on
/sbin/chkconfig --level 345 random on
/sbin/chkconfig --level 345 rconfig on
/sbin/chkconfig --level 345 sendmail on
```

```
/sbin/chkconfig --level 345 sshd on
/sbin/chkconfig --level 345 syslog on
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 apmd off
/sbin/chkconfig --level 345 autofs off
/sbin/chkconfig --level 345 gpm off
/sbin/chkconfig --level 345 ipchains off
/sbin/chkconfig --level 345 iptables off
/sbin/chkconfig --level 345 isdn off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 netfs off
/sbin/chkconfig --level 345 nfslock off
/sbin/chkconfig --level 345 portmap off
/sbin/chkconfig --level 345 rawdevices off
/sbin/chkconfig --level 345 xfs off
```

Código 1 Archivo ks.cfg utilizado en la instalación de servidores[vii].

Revisando este archivo (código 1) tenemos que las líneas 1-3 establecen el idioma, el idioma para la ayuda y la distribución del teclado, la 5 establece el uso horario, la 6 pone una clave por omisión para el administrador del sistema (se encuentra cifrada), las líneas 12 a 17 establecen la distribución de las particiones del disco duro, la 18 define la configuración inicial de red, la 19 especifica que se active el firewall, la 22 deshabilita el modo gráfico de forma que el servidor trabajará en modo texto, las línea 23 a 285 son la relación de los paquetes a instalar y finalmente las líneas 288 a 314 son la configuración pertinente para cada uno de los servicios.

Con el archivo de kickstart, con los paquetes originales y los paquetes modificados se construyó un disco compacto que sirvió para hacer las instalaciones. El resultado se sometió a las pruebas necesarias para asegurar que el resultado de utilizar este disco compacto en una instalación era lo que se estaba buscando. Esto aseguraría repetibilidad en el proceso de instalación, minimizando errores, asegurando la calidad de cada instalación y minimizando el tiempo que tomaba cada instalación. A este conjunto de configuraciones y paquetes le llamaremos sistema base.

El software base corresponde al entorno del sistema operativo en el cual se instalará el producto IVA. En este sentido, estamos integrando la distribución de GNU/Linux conocida como RedHat Linux.

En términos generales, los cambios realizados en la versión utilizada de RedHat Linux se orientaron a los siguientes aspectos:

- Simplificación del proceso de instalación.
- Actualización de componentes del *core system*.
- Inclusión de algunos controladores nuevos y actualización de muchos otros.
- Soporte a RPM 4.0.
- Todos los paquetes del RedHat Linux han sido completamente mejorados para dar un mayor rendimiento. Algunos lo han sido para los Pentium Pro y los procesadores superiores, aunque siguen siendo compatibles con los procesadores 386, 486 y Pentium.
- RedHat Linux incluye el soporte para los dispositivos USB (sobre todo los ratones y los teclados, aunque también incluye otros módulos adaptables a otros aparatos).
- Con el IDE Disk Drive Tuning la mejora del desempeño de las unidades de disco duro se logra más fácilmente.
- La distribución presenta cambios importantes en el esquema de cifrado OpenSSH y en el soporte de VPN.

- Además, integra de forma anticipada los componentes de software que conformarán la próxima generación de tecnología Linux.

Como ya dijimos, a fin de satisfacer las necesidades del proyecto, se construyó una distribución especial del sistema operativo que incluye de forma adicional los siguientes componentes:

Kernel versión 2.4: Corresponde a la más estable y reciente versión del Kernel de Linux.

libsafe: Es una capa de software de "middleware" que se encarga de interceptar las llamadas realizadas a las funciones del sistema operativo que son vulnerables a ataques de "buffer overflow". Este producto ha demostrado su habilidad para detectar y evitar los ataques de este tipo más comunes en Linux, pero sobre todo su capacidad para minimizar ataques desconocidos en esta categoría. Adicionalmente, este producto no impacta el rendimiento global del sistema operativo. Las vulnerabilidades generadas por la explotación de una condición de "buffer overflow" como consecuencia de un ataque, se han constituido como uno de los métodos de ataque a la seguridad preferidos en los últimos años.

Netfilter: El sistema de filtrado de paquetes que utiliza el Kernel 2.4 corresponde a la herramienta Netfilter, que es la primera en Linux que integra un esquema inteligente de Firewall, lo cual representa un salto tecnológico importante para este tipo de dispositivos. Entre las muchas mejoras que ofrece esta herramienta, la más relevante radica en la capacidad de detectar y bloquear "escaneos" que previamente no eran identificables en los firewalls del servidor Linux. Adicionalmente la arquitectura del producto permite la administración más fácil y poderosa de los NAT (Network Address Translation), Proxies y Redireccionamientos. Esta última funcionalidad permite la configuración sencilla de servidores en conglomerado para el balanceo de carga. Adicionalmente, NetFilter permite bloquear más ataques del tipos DoS (Denial of Service). Este producto es una re-implementación del código firewall de Linux, pero permanece totalmente compatible con la versión anterior.

Al terminar una instalación tenemos un sistema operativo y servicios, falta configurar una parte de la seguridad y la aplicación. Para la configuración de la seguridad y la instalación de la aplicación se construyeron archivos de ejecución por lotes que veremos más adelante, en las secciones correspondientes.

Con esto hemos resuelto nuestras primeras necesidades, contar con un sistema operativo, las herramientas y los servicios.

El detalle de la aplicación y de la seguridad lo presentamos a continuación, dentro de las secciones correspondientes.

Vale la pena considerar, dentro de esta visión global del sistema, que dentro del proyecto que se desarrolló para Banco del Bajío, pero sin formar parte integral de esta tesis, se realizó la configuración del DNS, del firewall de red Cisco PIX, del servidor de correo electrónico y de servidores de respaldo para dichas funciones.

Se menciona aquí el DNS o servidor de nombres debido a que su funcionamiento es indispensable para que la solución sea visible a los clientes de BB por Internet. Además, gracias al DNS se ha hecho balanceo de carga – utilizando una técnica conocida como *round robin*- entre distintos servidores para la parte del sitio que sólo es información.

Este DNS fue configurado para los siguientes dominios:

- bb.com.mx
- bancobajio.com.mx
- bancodelbajio.com.mx
- bajionet.com.mx
- bajionet.com

Utilizaremos la configuración (código 2) del dominio bb.com.mx para analizar el balanceo del que estamos hablando.

```
$ttl 38400
$ORIGIN bb.com.mx.
@       IN      SOA     ns.bb.com.mx. seguridad.bb.com.mx. (
995338579
10800
3600
432000
38400 )
@                               IN  NS      ns.bb.com.mx.
@                               IN  NS      mail.bb.com.mx.
bb.com.mx.                        IN  MX      10 mail.bb.com.mx.
ns.bb.com.mx.                     IN  A       200.76.36.67
bb.com.mx.                        IN  A       200.76.36.68
mail.bb.com.mx.                   IN  A       200.76.36.68
www.bb.com.mx.                    IN  A       200.76.36.69
www.bb.com.mx.                    IN  A       200.76.36.70
ayuda.bb.com.mx.                  IN  A       200.76.36.69
ayuda.bb.com.mx.                  IN  A       200.76.36.70
secure.bb.com.mx.                 IN  A       200.76.36.71
demodivisas.bb.com.mx.            IN  A       200.76.36.69
demodivisas.bb.com.mx.            IN  A       200.76.36.70
servicios.bb.com.mx.              IN  A       200.76.36.72
dns.bb.com.mx.                    IN  CNAME   ns
dns2.bb.com.mx.                   IN  CNAME   mail
pop.bb.com.mx.                    IN  CNAME   mail
pop3.bb.com.mx.                   IN  CNAME   mail
smtp.bb.com.mx.                   IN  CNAME   mail
```

Código 2 Configuración del DNS, para el dominio bb.com.mx.

Como podemos ver en las líneas 15 y 16 se encuentra repetido al nombre de la máquina www, con dos direcciones IP distintas, 200.76.36.69 y 200.76.36.70. Esto da lugar a que en el momento que se solicita la resolución de nombre a IP para www.bb.com.mx, una vez se de cómo respuesta 200.76.36.69 y la siguiente 200.76.36.70 y así alternadamente. Gracias a esta facilidad del DNS es posible poner 2 o más servidores y repartir la cantidad de peticiones que cada uno de ellos atiende. Esta solución es rápida, económica y sencilla, sin embargo no siempre funciona.

En el caso de que lo que se esté haciendo sea balanceo entre servidores aplicativos se presentan fallas, puesto que la información sobre la sesión de un usuario, por ejemplo, normalmente residirá en el servidor donde empezó su sesión y en una gran mayoría de los caso no estará disponible si cambia de servidor. Siempre es posible adaptar la aplicación para que sea

compatible con este tipo de balanceo, sin embargo, hacerlo puede requerir de un gran esfuerzo y/o de recursos adicionales especiales. Hay más mecanismos, dispositivos y herramientas para realizar balanceo, pero no se analizarán en este trabajo.

Configuración de los componentes del sistema base

Entre los componentes del sistema base es importante revisar el servidor de páginas, el lenguaje de scripting PHP, las herramientas de Zend que se integraron a PHP y el servidor de nombres. Revisaremos a continuación la configuración de dichas herramientas, con la excepción del servidor de nombres que ya hemos analizado con anterioridad.

Configuración del servidor de páginas

La configuración del servidor de páginas la analizaremos en dos fragmentos importantes, el primero de ellos (código 3) corresponde a, lo que respecta a los módulos que se van a cargar y activar junto con el servidor y el segundo, aquello que corresponde a la configuración de los sitios activos en el servidor de páginas.

```
LoadModule access_module modules/mod_access.so
# LoadModule auth_module modules/mod_auth.so
# LoadModule auth_anon_module modules/mod_auth_anon.so
# LoadModule auth_dbm_module modules/mod_auth_dbm.so
# LoadModule auth_digest_module modules/mod_auth_digest.so
# LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
# LoadModule mime_magic_module modules/mod_mime_magic.so
# LoadModule cern_meta_module modules/mod_cern_meta.so
# LoadModule expires_module modules/mod_expires.so
# LoadModule headers_module modules/mod_headers.so
# LoadModule usertrack_module modules/mod_usertrack.so
# LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
# LoadModule dav_module modules/mod_dav.so
# LoadModule status_module modules/mod_status.so
# LoadModule autoindex_module modules/mod_autoindex.so
# LoadModule asis_module modules/mod_asis.so
# LoadModule info_module modules/mod_info.so
# LoadModule cgi_module modules/mod_cgi.so
# LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule negotiation_module modules/mod_negotiation.so
# LoadModule dir_module modules/mod_dir.so
# LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
# LoadModule speling_module modules/mod_speling.so
# LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
# LoadModule proxy_module modules/mod_proxy.so
# LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
# LoadModule proxy_http_module modules/mod_proxy_http.so
# LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

Código 3 Configuración del servidor de páginas, sección módulos.

En la configuración del servidor de páginas, apache, una línea que comienza con # es un comentario y no será tomada en cuenta en el establecimiento de la configuración del servidor. Es

por ello que, si revisamos la lista anterior, veremos que hay una gran cantidad de módulos pero sólo algunos de ellos los estamos cargando junto con el servidor. A continuación revisaremos por qué cargamos algunos de estos módulos.

Para poder tener bitácoras de las peticiones, errores y respuestas del servidor necesitamos mod_log_config. Dado que deseamos restringir el acceso a algunos archivos de nuestro servidor, necesitamos contar con mod_access. Con el fin de enviar correctamente la información sobre la codificación de la información a los navegadores, cargamos mod_mime. El módulo de mod_rewrite lo necesitamos para la configuración de eZ Publish que estamos utilizando. También necesitamos mod_env y mod_setenvif. El módulo mod_alias lo utilizamos para redireccionar las peticiones no seguras que se hacen al sitio secure.bb.com.mx a www.bb.com.mx. Mod_actions y mod_negotiation se utilizan para establecer parámetros de comunicación, tales como idioma, compresión, etc., con los navegadores modernos. La capacidad de tener varios sitios en un mismo servidor nos la ofrece mod_vhosts, del cual analizaremos detalladamente la configuración (código 4) a continuación.

```
NameVirtualHost *

<VirtualHost *>
  ServerName ayuda.bb.com.mx:80
  ServerAdmin webmáster@bb.com.mx
  DocumentRoot /var/www/html/ayuda
  CustomLog /var/log/httpd/ayuda-extended_log "%h %l %u %t \"%r\" %s %b \"%{Referer}i\" \"%{User-
agent}i\""
  ErrorLog /var/log/httpd/ayuda-error_log
  <Directory /var/www/html/ayuda>
        Options FollowSymLinks Indexes ExecCGI
        AllowOverride None
  </Directory>
</VirtualHost>

<VirtualHost *>
  ServerName demodivisas.bb.com.mx:80
  ServerAdmin webmáster@bb.com.mx
  DocumentRoot /var/www/html/demodivisas
  CustomLog /var/log/httpd/demodivisas-extended_log "%h %l %u %t \"%r\" %s %b \"%{Referer}i\"
\"%{User-agent}i\""
  ErrorLog /var/log/httpd/demodivisas-error_log
  <Directory /var/www/html/demodivisas>
        Options FollowSymLinks Indexes ExecCGI
        AllowOverride None
  </Directory>
</VirtualHost>

<VirtualHost *>
  ServerName admin.bb.com.mx:80
  ServerAdmin webmáster@bb.com.mx
  DocumentRoot /var/www/html/bajio
  CustomLog /var/log/httpd/admin-extended_log "%h %l %u %t \"%r\" %s %b \"%{Referer}i\" \"%{User-
agent}i\""
  ErrorLog /var/log/httpd/admin-error_log
  <Directory /var/www/html/bajio>
        Options FollowSymLinks Indexes ExecCGI
        AllowOverride None
        RewriteEngine On
        RewriteRule ^cron.php /var/www/html/bajio/cron.php [L]
        RewriteRule !\.(gif|css|jpg) /var/www/html/bajio/index_admin.php
  </Directory>
</VirtualHost>


<VirtualHost *>
```

```
        ServerName www.bb.com.mx:80
        ServerAdmin webmáster@bb.com.mx
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bb.com.mx/article/articleview/86/1/7
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/www-rewrite.log
        RewriteRule                                          .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                          ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        CustomLog  /var/log/httpd/www-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/www-error_log
        <Directory /var/www/html/bajio>
                Options FollowSymLinks Indexes ExecCGI
                AllowOverride None
        </Directory>
</VirtualHost>

<VirtualHost *>
        ServerName www.bajionet.com.mx:80
        ServerAdmin webmáster@bajionet.com.mx
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bajionet.com.mx/article/articleview/86/1/7
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/www-rewrite.log
        RewriteRule                                          .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                          ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        CustomLog  /var/log/httpd/www-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/www-error_log
        <Directory /var/www/html/bajio>
                Options FollowSymLinks Indexes ExecCGI
                AllowOverride None
        </Directory>
</VirtualHost>

<VirtualHost *>
        ServerName www.bancobajio.com.mx:80
        ServerAdmin webmáster@bancobajio.com.mx
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bancobajio.com.mx/article/articleview/86/1/7
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/www-rewrite.log
        RewriteRule                                          .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                          ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        CustomLog  /var/log/httpd/www-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/www-error_log
        <Directory /var/www/html/bajio>
                Options FollowSymLinks Indexes ExecCGI
```

```
                AllowOverride None
        </Directory>
</VirtualHost>

<VirtualHost *>
        ServerName www.bancodelbajio.com.mx:80
        ServerAdmin webmáster@bancodelbajio.com.mx
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bancodelbajio.com.mx/article/articleview/86/1/7
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/www-rewrite.log
        RewriteRule                                              .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                          ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        CustomLog  /var/log/httpd/www-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/www-error_log
        <Directory /var/www/html/bajio>
                Options FollowSymLinks Indexes ExecCGI
                AllowOverride None
        </Directory>
</VirtualHost>

<VirtualHost *>
        ServerName www.bajionet.com:80
        ServerAdmin webmáster@bajionet.com
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bajionet.com/article/articleview/86/1/7
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/www-rewrite.log
        RewriteRule                                              .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                          ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        CustomLog  /var/log/httpd/www-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/www-error_log
        <Directory /var/www/html/bajio>
                Options FollowSymLinks Indexes ExecCGI
                AllowOverride None
        </Directory>
</VirtualHost>

<VirtualHost *>
  ServerName secure.bb.com.mx:80
  ServerAdmin webmáster@bb.com.mx
  DocumentRoot /var/www/html/bajio
  CustomLog  /var/log/httpd/secure80-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
  ErrorLog /var/log/httpd/secure80-error_log
  <Directory /var/www/html/bajio>
        Options FollowSymLinks Indexes ExecCGI
        AllowOverride None
        <IfModule mod_alias.c>
             RedirectMatch (.*)$ http://www.bb.com.mx/
        </IfModule>
  </Directory>
</VirtualHost>
```

```
<VirtualHost 192.168.100.249:443>
        ServerName secure.bb.com.mx:443
        ServerAdmin webmáster@bb.com.mx
        DocumentRoot /var/www/html/bajio
        ErrorDocument 403 http://www.bb.com.mx/article/articleview/86/1/7
        SSLEngine on
        SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
        SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
        RewriteEngine On
        RewriteLogLevel 9
        RewriteLog /var/log/httpd/secure-rewrite.log
        RewriteRule ^/impuestos/(.*)$  /var/www/html/bajio/impuestos/$1 [L]
        RewriteRule                                          .*/ezmediacatalogue/catalogue/(.*)$
/var/www/html/bajio/ezmediacatalogue/catalogue/$1 [T="application/oct-stream",S=4]
        RewriteRule ^/xmlrpc.*$  /var/www/html/bajio/index_xmlrpc.php [S=3]
        RewriteRule   ^/stats/store/(.*).gif$      /var/www/html/bajio/ezstats/user/storestats.php
[S=2]
        RewriteRule                                        ^/filemanager/filedownload/([^/]+)/(.*)$
/var/www/html/bajio/ezfilemanager/files/$1 [T=application/oct-stream,S=1]
        RewriteRule !\.(gif|css|jpg|png)$ /var/www/html/bajio/index.php
        SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
        CustomLog  /var/log/httpd/ssl_request_log  "%t  %h  %{SSL_PROTOCOL}x  %{SSL_CIPHER}x  \"%r\"
%b"
        CustomLog  /var/log/httpd/secure-ssl_request_log  "%t  %h  %{SSL_PROTOCOL}x  %{SSL_CIPHER}x
%{SSL_CIPHER_EXPORT}x %{SSL_CIPHER_ALGKEYSIZE}x %{SSL_CIPHER_USEKEYSIZE}x \"%r\" %b"
        CustomLog  /var/log/httpd/secure-extended_log  "%h  %l  %u  %t  \"%r\"  %s  %b  \"%{Referer}i\"
\"%{User-agent}i\""
        ErrorLog /var/log/httpd/secure-error_log
        <Files ~ "\.(cgi|shtml)$">
            SSLOptions +StdEnvVars
        </Files>
        <Directory "/var/www/cgi-bin">
            SSLOptions +StdEnvVars
        </Directory>
        <Directory /var/www/html/bajio>
                # SSLRequire %{SSL_CIPHER_USEKEYSIZE} >= 128
                Options FollowSymLinks Indexes ExecCGI
                AllowOverride None
        </Directory>
</VirtualHost>
```

Código 4 Configuración del servidor de páginas, sección virtualhosts.

Si analizamos esta configuración tenemos que las líneas:

- 3 a 13 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a ayuda.bb.com.mx. Se puede decir que ésta es una configuración normal de un servidor de páginas, ya que no involucra módulos especiales ni bitácoras especiales.
- 14 a 15 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a demodivisas.bb.com.mx. Se puede decir que ésta es también una configuración normal de un servidor de páginas, ya que no involucra módulos especiales ni bitácoras especiales.
- 27 a 40 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a admin.bb.com.mx. Ésta es una configuración especial puesto que incluye las líneas 36 a 38 que configuran al módulo mod_rewrite de apache para que todas las peticiones que se hagan a admin.bb.com.mx sean atendidas por el programa index_admin.php.
- 42 a 61 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a www.bb.com.mx. Ésta es una configuración especial, puesto que incluye las líneas 36 a 38 que configuran al módulo mod_rewrite de apache para que las peticiones que se hagan a www.bb.com.mx sean atendidas de diferentes maneras, dependiendo de si cumplen o no con algunos de los filtros que se han establecido

utilizando expresiones regulares. En el caso en que la petición no coincida con alguno de los patrones, se atenderá por omisión por el programa index.php. A manera de ejemplo, analicemos uno de estos filtros: consideremos pues la línea 51, de sus 4 elementos separados por espacio tenemos que el primero RewriteRule define que lo siguiente es una instrucción de configuración para el módulo mod_rewrite, el segundo, ^/xmlrpc.*$, dice que todas las peticiones que cumplan con el patrón de que el inicio del URI de la petición contenga los caracteres xmlrpc deben ser atendidos por el tercer elemento, /var/www/html/bajio/index_xmlrpc.php, que es un script de php especial para la interacción con eZ Publish Desktop Edition, y el cuarto elemento [S=3] dice que si esta regla se cumple, el motor de los filtros se debe saltar las siguientes tres definiciones. Además, las líneas 47 a 49 establecen una bitácora especial para el módulo mod_rewrite.

- 63 a 145 definen una configuración equivalente a la analizada pero para otros dominios. Hay que señalar aquí que todos apuntan al mismo directorio por lo tanto todos muestran la misma información.
- 147 a 160 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a secure.bb.com.mx. cuando éstas no se hagan por el canal seguro, es decir cuando no se utilice SSL en la comunicación. El comportamiento será redireccionar la petición que había llegado a http://secure.bb.com.mx/ a http://www.bb.com.mx/; y eso está definido en las línea 156 a 158 que dependen de que el módulo mod_alias se encuentre incorporado al servidor de páginas apache.
- 162 a 197 definen la configuración para el servidor de páginas que va a atender las peticiones que se hagan a secure.bb.com.mx. cuando éstas sí se hagan por el canal seguro, es decir cuando si se utilice SSL en la comunicación. Ésta es probablemente la configuración más compleja de todas las que se han analizado. En la línea 167 le decimos al servidor que debe utilizar SSL para las peticiones y respuestas que se hagan. Las líneas 168 y 169 definen qué certificado se va a utilizar y qué llave privada corresponde a dicho certificado. Las líneas 180 a 182 son bitácoras especiales para la actividad que se lleve al cabo por el canal cifrado.

Configuración de PHP

Analicemos a continuación la configuración de PHP y Zend en el contexto que ha sido definido por los requerimientos. La configuración está dada por archivo /etc/php.ini, cuyo contenido presentamos a continuación:

```
[PHP]

;;;;;;;;;;;
; WARNING ;
;;;;;;;;;;;
; This is the default settings file for new PHP installations.
; By default, PHP installs itself with a configuration suitable for
; development purposes, and *NOT* for production purposes.
; For several security-oriented considerations that should be taken
; before going online with your site, please consult php.ini-recommended
; and http://php.net/manual/en/security.php.


;;;;;;;;;;;;;;;;;;;
; About this file ;
;;;;;;;;;;;;;;;;;;;
```

```
; This file controls many aspects of PHP's behavior.  In order for PHP to
; read it, it must be named 'php.ini'.  PHP looks for it in the current
; working directory, in the path designated by the environment variable
; PHPRC, and in the path that was defined in compile time (in that order).
; Under Windows, the compile-time path is the Windows directory.  The
; path in which the php.ini file is looked for can be overridden using
; the -c argument in command line mode.
;
; The syntax of the file is extremely simple.  Whitespace and Lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.
;
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
;
; The value can be a string, a number, a PHP constant (e.g. E_ALL or M_PI), one
; of the INI constants (On, Off, True, False, Yes, No and None) or an expression
; (e.g. E_ALL & ~E_NOTICE), or a quoted string ("foo").
;
; Expressions in the INI file are limited to bitwise operators and parentheses:
; |        bitwise OR
; &        bitwise AND
; ~        bitwise NOT
; !        boolean NOT
;
; Boolean flags can be turned on using the values 1, On, True or Yes.
; They can be turned off using the values 0, Off, False or No.
;
; An empty string can be denoted by simply not writing anything after the equal
; sign, or by using the None keyword:
;
;  foo =         ; sets foo to an empty string
;  foo = none    ; sets foo to an empty string
;  foo = "none"  ; sets foo to the string 'none'
;
; If you use constants in your value, and these constants belong to a
; dynamically loaded extension (either a PHP extension or a Zend extension),
; you may only use these constants *after* the line that loads the extension.
;
; All the values in the php.ini-dist file correspond to the builtin
; defaults (that is, if no php.ini is used, or if you delete these lines,
; the builtin defaults will be identical).


;;;;;;;;;;;;;;;;;;;;
; Language Options ;
;;;;;;;;;;;;;;;;;;;;

; Enable the PHP scripting language engine under Apache.
engine = On

; Allow the <? tag.  Otherwise, only <?php and <script> tags are recognized.
short_open_tag = On

; Allow ASP-style <% %> tags.
asp_tags = Off

; The number of significant digits displayed in floating point numbers.
precision    =  14

; Enforce year 2000 compliance (will cause problems with non-compliant browsers)
y2k_compliance = Off

; Output buffering allows you to send header lines (including cookies) even
; after you send body content, at the price of slowing PHP's output layer a
; bit.  You can enable output buffering during runtime by calling the output
; buffering functions.  You can also enable output buffering for all files by
; setting this directive to On.  If you wish to limit the size of the buffer
```

```
; to a certain size - you can use a maximum number of bytes instead of 'On', as
; a value for this directive (e.g., output_buffering=4096).
output_buffering = Off

; You can redirect all of the output of your scripts to a function.  For
; example, if you set output_handler to "ob_gzhandler", output will be
; transparently compressed for browsers that support gzip or deflate encoding.
; Setting an output handler automatically turns on output buffering.
output_handler =

; The unserialize callback function will called (with the undefind class'
; name as parameter), if the unserializer finds an undefined class
; which should be instanciated.
; A warning appears if the specified function is not defined, or if the
; function doesn't include/implement the missing class.
; So only set this entry, if you really want to implement such a
; callback-function.
unserialize_callback_func=

; Transparent output compression using the zlib library
; Valid values for this option are 'off', 'on', or a specific buffer size
; to be used for compression (default is 4KB)
;
; Note: output_handler must be empty if this is set 'On' !!!!
;
zlib.output_compression = On

; Implicit flush tells PHP to tell the output layer to flush itself
; automatically after every output block.  This is equivalent to calling the
; PHP function flush() after each and every call to print() or echo() and each
; and every HTML block.  Turning this option on has serious performance
; implications and is generally recommended for debugging purposes only.
implicit_flush = Off

; Whether to enable the ability to force arguments to be passed by reference
; at function call time.  This method is deprecated and is likely to be
; unsupported in future versions of PHP/Zend.  The encouraged method of
; specifying which arguments should be passed by reference is in the function
; declaration.  You're encouraged to try and turn this option Off and make
; sure your scripts work properly with it in order to ensure they will work
; with future versions of the language (you will receive a warning each time
; you use this feature, and the argument will be passed by value instead of by
; reference).
allow_call_time_pass_reference = On

; Safe Mode
;
safe_mode = Off

; By default, Safe Mode does a UID compare check when
; opening files. If you want to relax this to a GID compare,
; then turn on safe_mode_gid.
safe_mode_gid = Off

; When safe_mode is on, UID/GID checks are bypassed when
; including files from this directory and its subdirectories.
; (directory must also be in include_path or full path must
; be used when including)
safe_mode_include_dir =

; When safe_mode is on, only executables located in the safe_mode_exec_dir
; will be allowed to be executed via the exec family of functions.
safe_mode_exec_dir =

; open_basedir, if set, limits all file operations to the defined directory
; and below.  This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
;

;open_basedir =
```

```
; Setting certain environment variables may be a potential security breach.
; This directive contains a comma-delimited list of prefixes.  In Safe Mode,
; the user may only alter environment variables whose names begin with the
; prefixes supplied here.  By default, users will only be able to set
; environment variables that begin with PHP_ (e.g. PHP_FOO=BAR).
;
; Note:  If this directive is empty, PHP will let the user modify ANY
; environment variable!
safe_mode_allowed_env_vars = PHP_

; This directive contains a comma-delimited list of environment variables that
; the end user won't be able to change using putenv().  These variables will be
; protected even if safe_mode_allowed_env_vars is set to allow to change them.
safe_mode_protected_env_vars = LD_LIBRARY_PATH

; This directive allows you to disable certain functions for security reasons.
; It receives a comma-delimited list of function names.  This directive is
; *NOT* affected by whether Safe Mode is turned On or Off.
disable_functions =

; Colors for Syntax Highlighting mode.  Anything that's acceptable in
; <font color="??????"> would work.
highlight.string  = #CC0000
highlight.comment = #FF9900
highlight.keyword = #006600
highlight.bg      = #FFFFFF
highlight.default = #0000CC
highlight.html    = #000000


;
; Misc
;
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
expose_php = On


;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

max_execution_time = 30     ; Maximum execution time of each script, in seconds
memory_limit = 32M      ; Maximum amount of memory a script may consume (8MB)


;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; error_reporting is a bit-field.  Or each number up to get desired error
; reporting level
; E_ALL             - All errors and warnings
; E_ERROR           - fatal run-time errors
; E_WARNING         - run-time warnings (non-fatal errors)
; E_PARSE           - compile-time parse errors
; E_NOTICE          - run-time notices (these are warnings which often result
;                     from a bug in your code, but it's possible that it was
;                     intentional (e.g., using an uninitialized variable and
;                     relying on the fact it's automatically initialized to an
;                     empty string)
; E_CORE_ERROR      - fatal errors that occur during PHP's initial startup
; E_CORE_WARNING    - warnings (non-fatal errors) that occur during PHP's
;                     initial startup
; E_COMPILE_ERROR   - fatal compile-time errors
; E_COMPILE_WARNING - compile-time warnings (non-fatal errors)
; E_USER_ERROR      - user-generated error message
; E_USER_WARNING    - user-generated warning message
```

```
; E_USER_NOTICE     - user-generated notice message
;
; Examples:
;
;   - Show all errors, except for notices
;
;error_reporting = E_ALL & ~E_NOTICE
;
;   - Show only errors
;
;error_reporting = E_COMPILE_ERROR|E_ERROR|E_CORE_ERROR
;
;   - Show all errors except for notices
;
error_reporting  =  E_ALL & ~E_NOTICE

; Print out errors (as a part of the output).  For production web sites,
; you're strongly encouraged to turn this feature off, and use error logging
; instead (see below).  Keeping display_errors enabled on a production web site
; may reveal security information to end users, such as file paths on your Web
; server, your database schema or other information.
display_errors = On

; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed.  It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off

; Log errors into a log file (server-specific log, stderr, or error_log (below))
; As stated above, you're strongly advised to use error logging in place of
; error displaying on production web sites.
log_errors = On

; Store the last error/warning message in $php_errormsg (boolean).
track_errors = Off

; Disable the inclusion of HTML tags in error messages.
;html_errors = Off

; String to output before an error message.
;error_prepend_string = "<font color=ff0000>"

; String to output after an error message.
;error_append_string = "</font>"

; Log errors to specified file.
;error_log = filename

; Log errors to syslog (Event Log on NT, not valid in Windows 95).
;error_log = syslog

; Warn if the + operator is used with strings.
warn_plus_overloading = Off


;;;;;;;;;;;;;;;;;
; Data Handling ;
;;;;;;;;;;;;;;;;;
;
; Note - track_vars is ALWAYS enabled as of PHP 4.0.3

; The separator used in PHP generated URLs to separate arguments.
; Default is "&".
;arg_separator.output = "&amp;"

; List of separator(s) used by PHP to parse input URLs into variables.
; Default is "&".
; NOTE: Every character in this directive is considered as separator!
;arg_separator.input = ";&"
```

```
; This directive describes the order in which PHP registers GET, POST, Cookie,
; Environment and Built-in variables (G, P, C, E & S respectively, often
; referred to as EGPCS or GPC).  Registration is done from left to right, newer
; values override older values.
variables_order = "EGPCS"

; Whether or not to register the EGPCS variables as global variables.  You may
; want to turn this off if you don't want to clutter your scripts' global scope
; with user data.  This makes most sense when coupled with track_vars - in which
; case you can access all of the GPC variables through the $HTTP_*_VARS[],
; variables.
;
; You should do your best to write your scripts so that they do not require
; register_globals to be on;  Using form variables as globals can easily lead
; to possible security problems, if the code is not very well thought of.
register_globals = On

; This directive tells PHP whether to declare the argv&argc variables (that
; would contain the GET information).  If you don't use these variables, you
; should turn it off for increased performance.
register_argc_argv = On

; Maximum size of POST data that PHP will accept.
post_max_size = 64M

; This directive is deprecated.  Use variables_order instead.
gpc_order = "GPC"

; Magic quotes
;

; Magic quotes for incoming GET/POST/Cookie data.
magic_quotes_gpc = On

; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
magic_quotes_runtime = Off

; Use Sybase-style magic quotes (escape ' with '' instead of \').
magic_quotes_sybase = Off

; Automatically add files before or after any PHP document.
auto_prepend_file =
auto_append_file =

; As of 4.0b4, PHP always outputs a character encoding by default in
; the Content-type: header.  To disable sending of the charset, simply
; set it to be empty.
;
; PHP's built-in default is text/html
default_mimetype = "text/html"
;default_charset = "iso-8859-1"

; Always populate the $HTTP_RAW_POST_DATA variable.
;always_populate_raw_post_data = On

;;;;;;;;;;;;;;;;;;;;;;;;;
; Paths and Directories ;
;;;;;;;;;;;;;;;;;;;;;;;;;

; UNIX: "/path1:/path2"
;include_path = ".:/php/includes"
;
; Windows: "\path1;\path2"
;include_path = ".;c:\php\includes"

; The root of the PHP pages, used only if nonempty.
; if PHP was not compiled with FORCE_REDIRECT, you SHOULD set doc_root
; if you are running php as a CGI under any web server (other than IIS)
; see documentation for security issues.  The alternate is to use the
; cgi.force_redirect configuration below
```

```
doc_root =

; The directory under which PHP opens the script using /~usernamem used only
; if nonempty.
user_dir =

; Directory in which the loadable extensions (modules) reside.
extension_dir = /usr/lib/php4

; Whether or not to enable the dl() function.  The dl() function does NOT work
; properly in multithreaded servers, such as IIS or Zeus, and is automatically
; disabled on them.
enable_dl = On

; cgi.force_redirect is necessary to provide security running PHP as a CGI under
; most web servers.  Left undefined, PHP turns this on by default.  You can
; turn it off here AT YOUR OWN RISK
; **You CAN safely turn this off for IIS, in fact, you MUST.**
; cgi.force_redirect = 1

; if cgi.force_redirect is turned on, and you are not running under Apache or Netscape
; (iPlanet) web servers, you MAY need to set an environment variable name that PHP
; will look for to know it is OK to continue execution.  Setting this variable MAY
; cause security issues, KNOW WHAT YOU ARE DOING FIRST.
; cgi.redirect_status_env = ;

;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
upload_max_filesize = 64M

.
.
.


;;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;;
;
; If you wish to have an extension loaded automatically, use the following
; syntax:
;
;   extension=modulename.extension
;
; For example, on Windows:
;
;   extension=msql.dll
;
; ... or under UNIX:
;
;   extension=msql.so
;
; Note that it should be the name of the module only; no directory information
; needs to go here.  Specify the location of the extension with the
; extension_dir directive above.


;Windows Extensions
;Note that MySQL and ODBC support is now built in, so no dll is needed for it.
;
```

```
;extension=php_bz2.dll
;extension=php_ctype.dll
.
.
.
;extension=php_yaz.dll
;extension=php_zlib.dll

;Linux world
;
extension=imap.so
;extension=ldap.so
extension=mysql.so
;extension=odbc.so
;extension=pgsql.so
;extension=snmp.so
;extension=dbg.so


;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;

[debugger]
debugger.enabled                =       False   ; enables dbg extension
                                                ; May cause problems when
                                                ; being acessed through a
                                                ; firewall, if the debugging
                                                ; port isn't allowed through
                                                ; hense it is off by default
debugger.profiler_enabled       =       True    ; enables dbg profiler
debugger.JIT_enabled            =       True    ; enables JIT sessions
                                                ; (auto-activated)
debugger.JIT_port               =       7869    ; default port to be used this
                                                ; should be the same as the
                                                ; port number opened by the
                                                ; dbg listener
debugger.JIT_host               =       clienthost  ; either real client IP or
                                                ; a keyword "clienthost"
debugger.JIT_level              =       3       ; JIT activation level
                                                ;   0 - disables JIT,
                                                ;   1 - E_CORE,
                                                ;   2 - E_CORE | E_ERROR |
                                                ;       E_PARSE |
                                                ;       E_COMPILE_ERROR |
                                                ;       E_USER_ERROR
                                                ;   3 - E_ALL & ~(E_NOTICE |
                                                ;       E_USER_NOTICE)
                                                ;   4 - E_ALL


[Syslog]
; Whether or not to define the various syslog variables (e.g. $LOG_PID,
; $LOG_CRON, etc.).  Turning it off is a good idea performance-wise.  In
; runtime, you can define these variables by calling define_syslog_variables().
define_syslog_variables  = Off

.
.
.

[Session]
; Handler used to store/retrieve data.
session.save_handler = files

; Argument passed to save_handler.  In the case of files, this is the path
; where data files are stored. Note: Windows users have to change this
; variable in order to use PHP's session functions.

session.save_path = /tmp
```

```
; Whether to use cookies.
session.use_cookies = 1


; Name of the session (used as cookie name).
session.name = PHPSESSID

; Initialize session on request startup.
session.auto_start = 0

; Lifetime in seconds of cookie or, if 0, until browser is restarted.
session.cookie_lifetime = 0

; The path for which the cookie is valid.
session.cookie_path = /

; The domain for which the cookie is valid.
session.cookie_domain =

; Handler used to serialize data.  php is the standard serializer of PHP.
session.serialize_handler = php

; Percentual probability that the 'garbage collection' process is started
; on every session initialization.
session.gc_probability = 1

; After this number of seconds, stored data will be seen as 'garbage' and
; cleaned up by the garbage collection process.
session.gc_maxlifetime = 1440

; Check HTTP Referer to invalidate externally stored URLs containing ids.
; HTTP_REFERER has to contain this substring for the session to be
; considered as valid.
session.referer_check =

; How many bytes to read from the file.
session.entropy_length = 0

; Specified here to create the session id.
session.entropy_file =

;session.entropy_length = 16

;session.entropy_file = /dev/urandom

; Set to {nocache,private,public} to determine HTTP caching aspects.
session.cache_limiter = nocache

; Document expires after n minutes.
session.cache_expire = 180

; use transient sid support if enabled by compiling with --enable-trans-sid.
session.use_trans_sid = 1

url_rewriter.tags = "a=href,area=href,frame=src,input=src,form=fakeentry"
.
.
.

; Local Variables:
; tab-width: 4
; End:
```

Código 5 Configuración de php.

Haciendo un repaso de las líneas marcadas en este archivo (código 5), podemos ver que se ha activado la compresión de la salida de los archivos ejecutados por PHP, lo que conviene para

hacer más eficiente el sitio, a menor cantidad de datos a transmitir, menor tiempo de transmisión. Luego alteramos el límite de memoria disponible para la ejecución de los programas, porque la experiencia nos ha demostrado que, debido al tamaño y a la complejidad de algunos de ellos, el parámetro por omisión no resulta ser suficiente. Como deseamos enterarnos de ellos y guardarlos en bitácoras estamos prendiendo ambas opciones.

Debido a que como respuesta en algunas formas vamos a recibir archivos, necesitamos asegurarnos de que habrá memoria suficiente para recibirlos, tanto en el método POST como en los archivos temporales que crearemos para guardarlos ya en el servidor.

Aprovechando la capacidad de PHP de cargar módulos internos de forma dinámica, estamos trayendo el módulo que nos da acceso a MySQL y no estamos cargando más que ese módulo, ahorrándonos valiosa memoria en el proceso de apache. Está señalado también, que no está activo en este momento el depurador que podemos cargar dinámicamente y así identificar y corregir errores en nuestro sistema.

Por último le dijimos a PHP que para las sesiones queremos utilizar las facilidades naturales que él nos brinda y no programar las propias.

Configuración de Zend

```
[Zend]
zend_optimizer.optimization_level=15
zend_gui_password=e6c755ba4d14d649d488dff6fef2ed62
zps.install_dir=/usr/local/Zend
zend_accelerator.output_cache_dir=/tmp/cache
zend_accelerator.output_cache_config=/usr/local/Zend/etc/cache/zend_cache.ini
zend_accelerator.output_cache_enabled=1
zend_accelerator.compression=1
zend_accelerator.compress_all=1
zend_accelerator.httpd_uid=48
zend_accelerator.max_cached_filesize=1000
zend_accelerator.user_blacklist_filename=/usr/local/Zend/etc/cache/user_blacklist.ZendAccelerator
.txt
zend_accelerator.validate_timestamps=1
zend_accelerator.use_cwd=1
zend_optimizer.enable_loader=1
zend_accelerator.max_accelerated_files=2000
zend_accelerator.max_wasted_percentage=5
zend_accelerator.memory_consumption=64
zend_accelerator.perform_timings=1
zend_accelerator.max_cache_size=0
zend_accelerator.min_free_disk=197M
zend_accelerator.cache_cleaner_freq=10
zend_accelerator.compress_blacklist_filename=/tmp/compress_blacklist.ZendAccelerator.txt
zend_accelerator.consistency_checks=0
zend_extension_manager.optimizer=/usr/local/Zend/lib/Optimizer-2.1.0
zend_extension_manager.performance_suite=/usr/local/Zend/lib/ZPS-3.5.0
zend_extension=/usr/local/Zend/lib/ZendExtensionManager.so
```

Código 6 Configuración de Zend.

Hemos marcado aquellas líneas (código 6) que por su relevancia en el comportamiento del sistema son las más importantes.

Tenemos entonces que:

- En la línea 1 le estamos indicando a Zend Optimizer que queremos el máximo nivel posible de optimización, esto lo hacemos así, debido a que ya hemos probado la aplicación completa y sabemos que ninguna de las técnicas de optimización compromete la estabilidad del sistema.
- En la línea 7 le estamos pidiendo a Zend Accelerator que guarde una copia de los archivos que ya procesó en el cache y que lo utilice para hacer más rápido el sitio.

- A su vez en la 8 le estamos diciendo que habilite la compresión de la información entre el servidor y el cliente. Como una parte importante del tiempo de respuesta se va en la transmisión de la información al compactarla y por tanto es menor la cantidad que hay que mover del servidor al cliente, ganamos en la percepción que tiene el usuario.

- Debido a que, como parte del esquema de seguridad, vamos a compilar todo el código fuente de la aplicación, necesitamos indicarle a Zend Optimizer que habilite el cargador con el cual un archivo compilado puede ser ejecutado, línea 15.

- Gracias a que los equipos con los que contamos tienen mucha capacidad, varios gigabytes de memoria RAM, tenemos la posibilidad, sin ningún problema, de dedicarle al cache de los archivos de Zend Accelerator toda la memoria que se requiera, línea 20.

Con esta revisión terminamos el análisis en lo que se refiere al sistema base y concluimos el diseño del sistema en su conjunto.

El sistema de administración de contenido

Al igual que nuestra decisión de utilizar una distribución antes que construir el sistema elemento a elemento, es decir, por consideraciones de tiempo en el caso del sistema de administración de contenido (SAC) el proceso fue la evaluación o consulta de evaluaciones de SSAACC para seleccionar el SAC a utilizar.

Algunos de los SSAACC evaluados fueron[viii]:

- PHP-Nuke (*http://www.phpnuke.org/*)
- Drupal (*http://www.drupal.org/*)
- eZ publish (http://www.ez.no/)
- php(Reactor) (*http://phpreactor.org/articles/*)
- phpWebSite (*http://phpwebsite.appstate.edu/*)
- Bricolage (*http://www.bricolage.cc/*)
- Plone (*http://www.plone.org/*)
- Mambo (*http://www.mamboserver.com/*)
- phpWebThings (*http://www. phpdbform.com/*)
- PrattSAC/CMS (*http://prattSAC/CMS.sourceforge.net/*)
- XOOPS (*http://www.xoops.org*).

Selección

El SAC seleccionado fue eZ Publish, porque:

- Fue programado en PHP.
- Está programado utilizando orientación a objetos.
- Tiene una compañía que lo respalda.
- Es modular.
- Es extensible.
- Es internacionalizable.
- Es de fácil manejo.
- Tiene una herramienta independiente exclusivamente para el manejo del módulo de contenido[IX] que corre en Windows y es muy amigable con el usuario.

Pero hablemos más ampliamente de la herramienta seleccionada.

eZ Publish

eZ Publish es un sistema de administración de contenido para web, en otras palabras es un sistema que permite hacer seguimiento, organización y publicación de información de hecho su lema es "share your information". La información se guarda en una base de datos y se presenta como páginas web. Se puede utilizar cualquier tipo de navegador para editar el contenido de una página almacenada en el sistema.

Sistema de administración de contenido (SAC/CMS[X])

Los módulos del Sistema de administración de contenido (SAC/CMS) son:

- Contenido
- Tienda
- Anuncios
- Foros
- Ligas
- Encuestas
- Banners o anuncios
- Noticias (importadas de otros sitios que manejen el formato RSS o RDF)
- Reporte de errores
- Administración de contactos
- Pendientes
- Agenda
- Administrador de archivos
- Catálogo de imágenes
- Catálogo de archivos multimedia
- Administrador de formas
- Envío de correo a listas
- Estadísticas
- Administración de usuarios

- Herramientas
- Administración del sitio

¿A quién está dirigido?

Hay algunas personas que utilizan eZ Publish para sus páginas personales, sin embargo, eZ Publish está orientado más a construir sitios profesionales de todos los tipos, por ejemplo:

- Sitios de noticias.
- Portales.
- Sitios de comercio electrónico negocio a consumidor final.
- Sitios de comercio electrónico negocio a negocio.
- Sitios corporativos.
- Intranets.
- Extranets

La funcionalidad de eZ Publish se ha desarrollado en colaboración con profesionales que lo han usado para construir sitios de esos tipos. Gracias a sus ventajas, las personas que utilizan eZ Publish día a día para administrar o construir sitios no requieren conocimientos especiales sobre sistemas operativos, servidores de páginas, diseño o instalación del sistema.

eZ Publish es un paquete que se construyó alrededor de varios módulos. Los módulos controlan el acceso a los datos a través de distintas páginas. Cada uno de los módulos utiliza uno o más objetos para recuperar y almacenar los datos. Todos los datos son manipulados a través de objetos, lo cual garantiza que los datos se almacenan correctamente.

A continuación tenemos algunas características comunes a todos los módulos de eZ Publish.

Separación de contenido y código.

La presentación de los datos se hace a través de un motor de plantillas. La información almacenada en los objetos se recupera a través de las operaciones de cada módulo, posteriormente, utilizando el motor de plantillas, dichos datos se combinan con las plantillas. Cada operación tiene plantillas específicas. Por esa razón el diseñador puede trabajar en las plantillas cambiando la organización y presentación de la información sin necesidad de modificar el código del sistema. Eso también permite crear distintas plantillas para distintas necesidades.

Internacionalización.

Hay distintos paquetes de idiomas disponibles para eZ Publish. Cada paquete contiene información sobre la forma específica en la que se deben presentar fechas, hora, y moneda así como sobre el conjunto de caracteres que se utilizan en un cierto idioma, además de una traducción para todos y cada uno de los mensajes y etiquetas del sistema.

Las traducciones las realizan voluntarios[xi]. De forma tal que el número de traducciones disponibles depende totalmente de las personas que tengan interés en ayudar con el proceso de internacionalización de eZ Publish.

Independencia de plataforma y navegador.

La información que envía eZ Publish viaja en formato xhtml que puede ser interpretado por cualquier navegador. Las plantillas por omisión de eZ Publish se diseñaron de tal forma que se ven de forma muy similar en distintos navegadores y distintas plataformas.

Para poder instalar eZ Publish en un servidor de páginas es necesario que el servidor de páginas tenga la capacidad de ejecutar PHP. La recomendación natural es utilizar apache, que está disponible prácticamente para cualquier plataforma.

Velocidad y cache.

El diseño es tal que se utiliza el menor número posible de conexiones a la base de datos. De esta forma se reducen los tiempos necesarios para generar una página y un mayor número de personas pueden acceder a los sitios creados con eZ Publish.

Además PHP tiene varias opciones de compilación y cache que pueden aumentar significativamente el desempeño de un servidor si el administrador las utiliza adecuadamente.

Adicionalmente estamos utilizando Zend Encoder, Zend Accelerator y Zend Optimizer para obtener el máximo desempeño posible de nuestra infraestructura y de la aplicación.

Sin límites.

En eZ Publish nunca se presentará una situación en la que el sistema envíe un mensaje del tipo "no puede tener más de X número de Y objetos", donde X es un número ridículamente bajo y Y es el objeto con el que está trabajando en ese momento.

Preferencias del usuario y sesiones.

Las preferencias de los usuarios se manejan por sesiones que pueden estar basadas en "galletas" o no. Por esta razón un usuario puede o no aceptar las galletas, ser o no miembro del sitio, de todas maneras tendrá la oportunidad de gozar del privilegio de la personalización del sitio.

Especificaciones técnicas de eZ Publish.

Tecnologías que utiliza:

- Lenguaje de scripting PHP

- Base de datos SQL
- XHTML versión 1.0
- XML versión 1.0
- XML-RPC
- Sistemas operativos donde se puede utilizar:
- Linux,
- Solaris,
- HP-UX,
- FreeBSD,
- Microsoft Windows NT,
- Microsoft Windows 98,
- Microsoft Windows XP,
- Microsoft Windows 2000,
- Mac OS X.

Software que se necesita para ejecutarlo.

Un motor de bases de datos SQL; actualmente se puede correr utilizando MySQL o PostgreSQL.
ImageMagick.
Apache o algún otro servidor de páginas que pueda incluir PHP
PHP

Equipo necesario.

Cualquiera donde corra el software necesario.

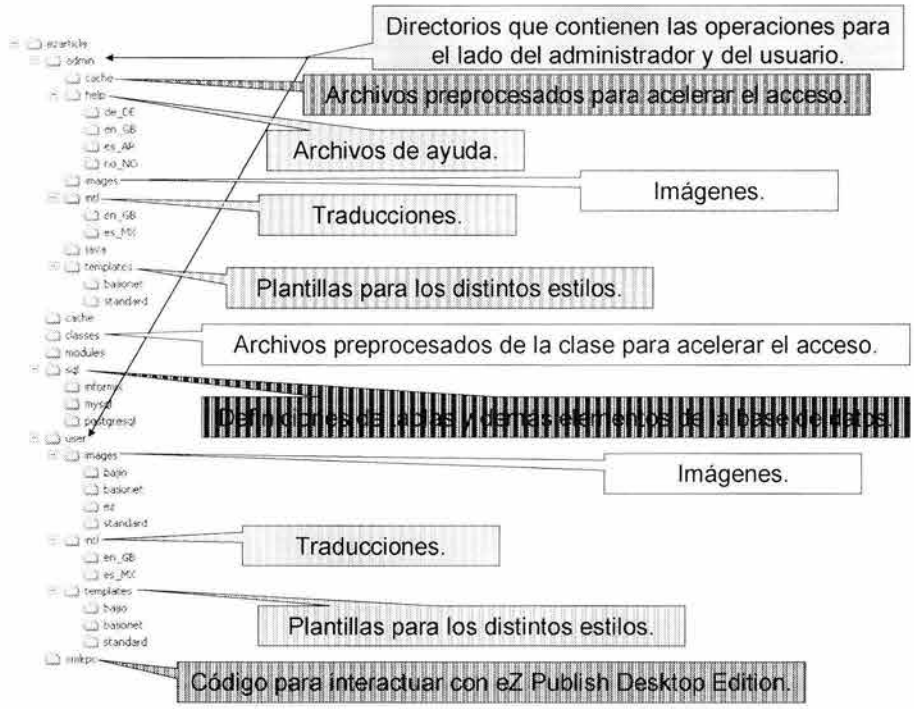
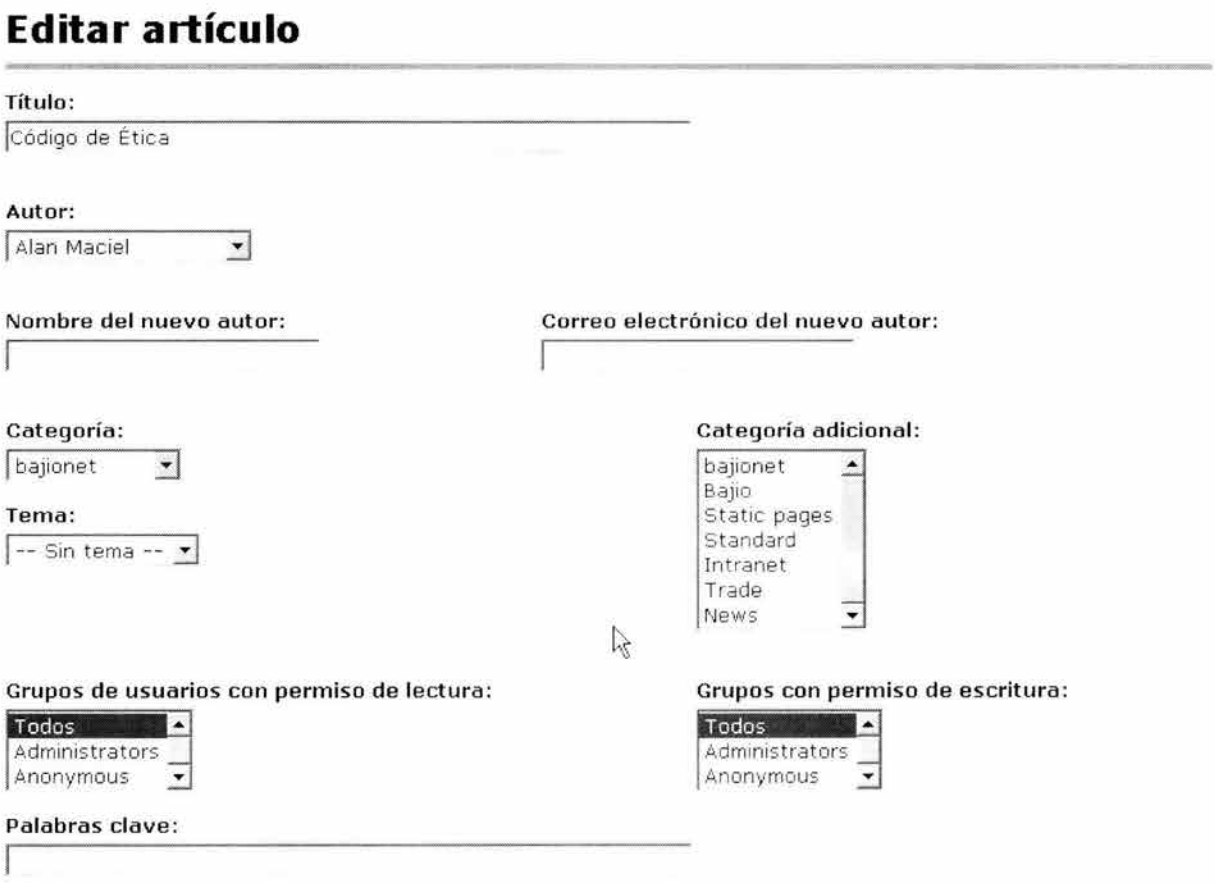


Diagrama 3 Estructura de módulos de eZ Publish.

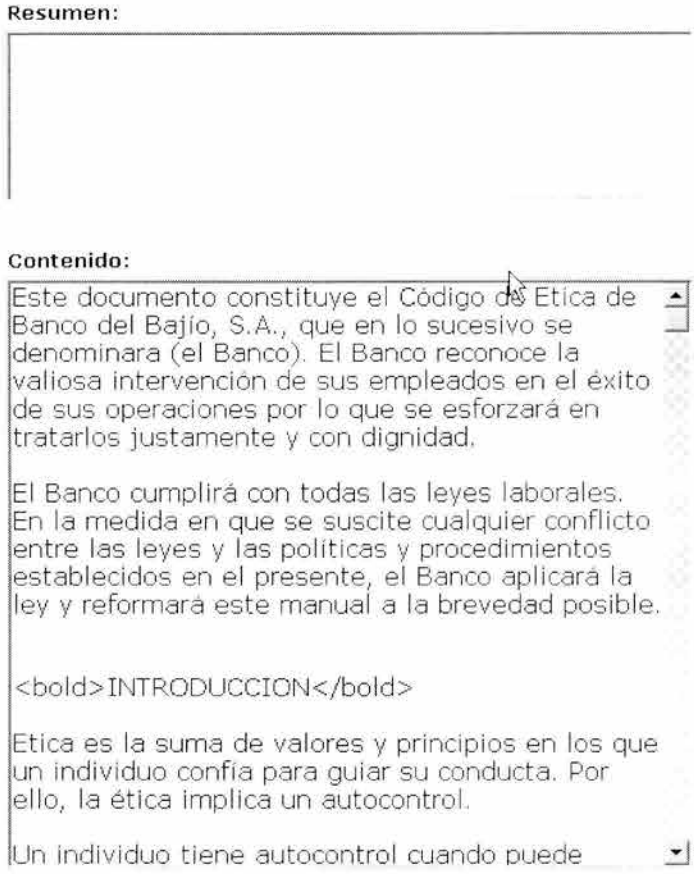
El diagrama (diagrama 3) de estructura de módulos nos muestra los distintos componentes de cada módulo. (user, admin., classes, templates, intl, images, cache, etc.).

Veamos un ejemplo de la interfase web del módulo de administración de contenido (pantalla 1 tres partes). Específicamente se trata de la operación de modificación del contenido de un artículo que ya existe.



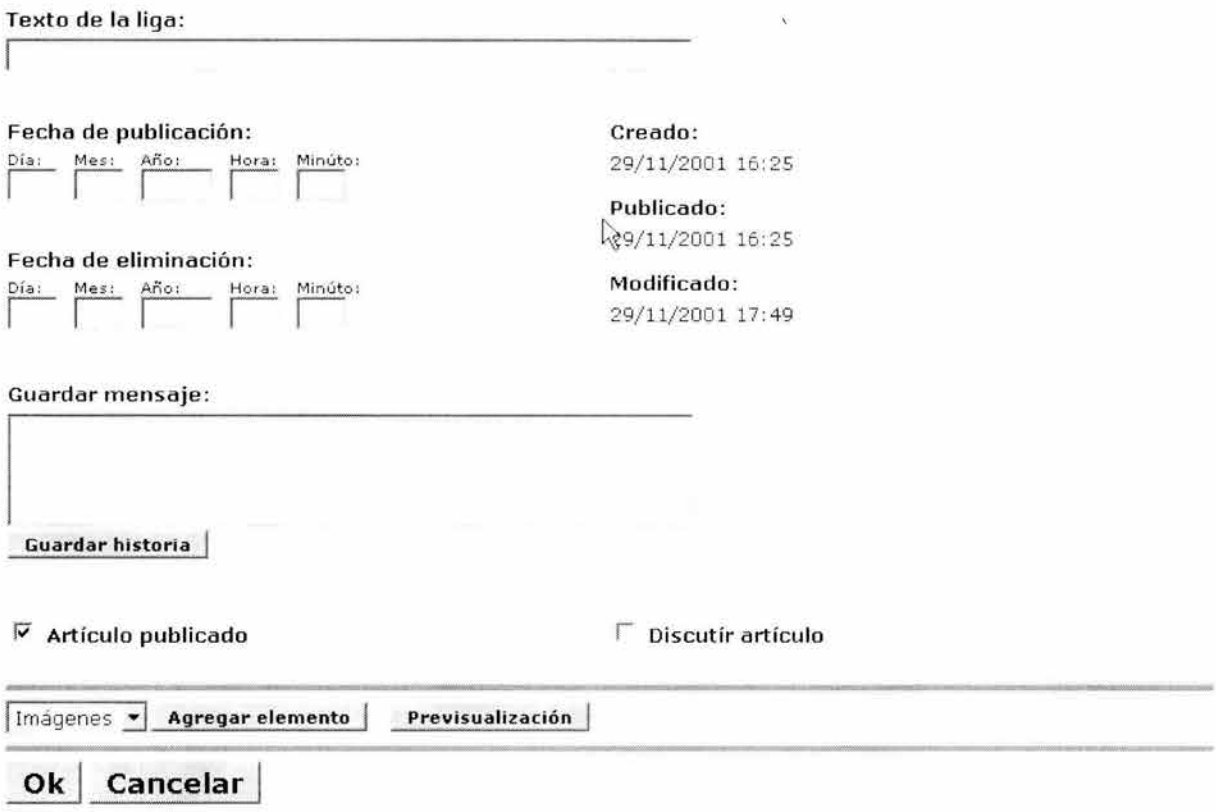
La primera parte del formato de captura o modificación de un artículo contiene información como el título, el autor, que se puede seleccionar de un catálogo de los autores que ya han contribuido con información o dar de alta uno nuevo. Gracias a la categoría, cada artículo tiene un lugar en la estructura de la información que hayamos definido para el sitio y también se le asocia un diseño o estilo. Con la asignación de grupos definimos quién o quiénes de los usuarios pueden leerlo y quién o quiénes pueden modificarlo.

Gracias a las palabras clave, el sistema crea automáticamente un índice. Este índice es independiente del que crea el motor de búsqueda por palabras. Este índice sólo contiene aquellas palabras que se han dado de alta en este campo, el motor crea un índice con todas las palabras que se encuentran en los artículos y que tienen un nivel de significancia por arriba del establecido en el parámetro correspondiente en el site.ini.



Esta segunda parte nos da oportunidad de trabajar con el contenido en si, con aquello que se les va a mostrar a los usuarios. Es decir el resumen, que se muestra por ejemplo en las categorías junto con el listado de los artículos de una categoría o al principio del artículo en la plantilla por omisión de eZArticle. Después viene el texto completo del artículo, para darle presentación se pueden utilizar un conjunto de marcadores que eZ Publish ha definido con anterioridad o bien se pueden agregar marcadores propietarios modificando la plantilla.

En el ejemplo que presentamos aquí la palabra INTRODUCCION, se va a mostrar en negritas, gracias al marcador <bold> que la rodea.

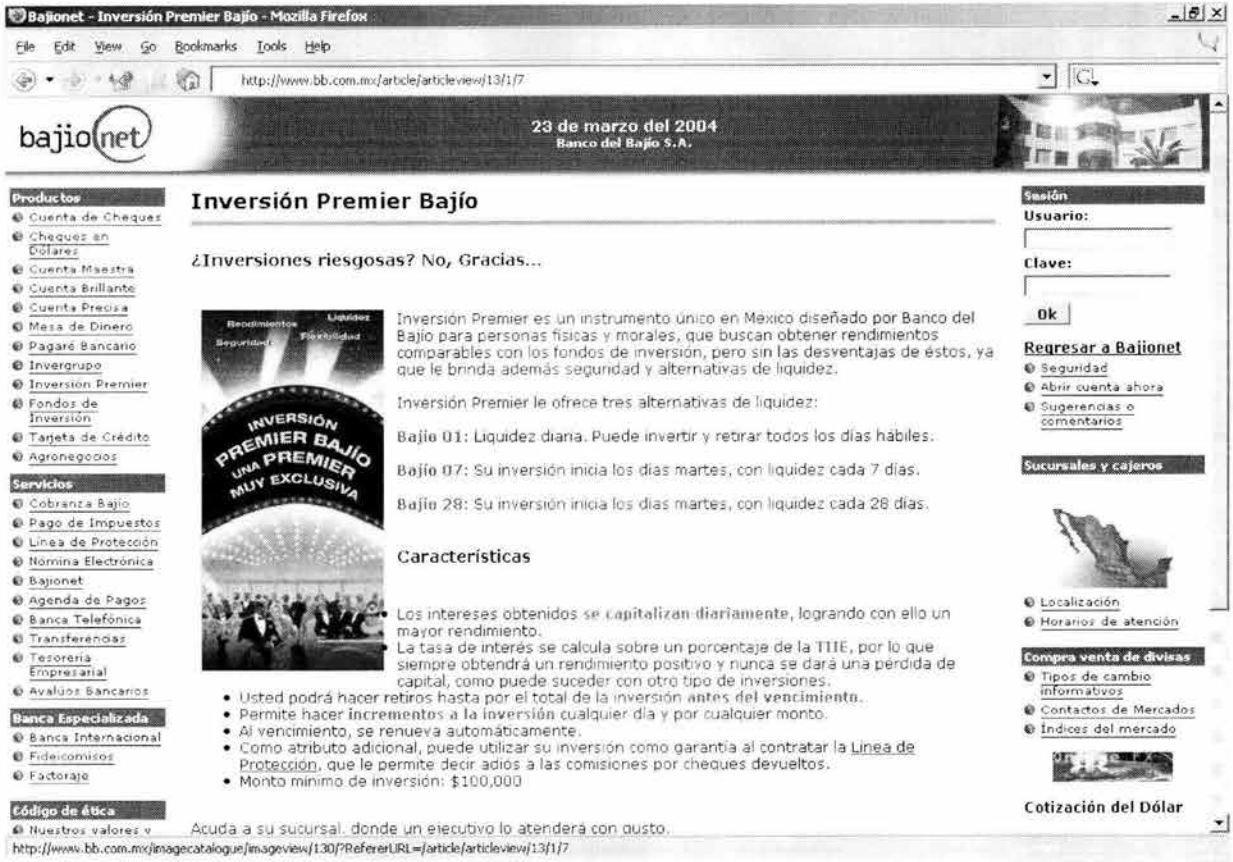


Pantalla 1 Módulo ezArticle, administración, alta artículo.

Y, finalmente, este bloque de la edición nos permite establecer parámetros como día y hora de su publicación, día y hora en que se deja de publicar, una bitácora de cambios, si el artículo está o no publicado, si se van o no a recibir comentarios de los usuarios sobre este artículo y algo muy importante, aunque no se aprecie aquí bien, se puede agregar elementos a este artículo como archivos, imágenes, pdf, etc.

Una vez que hemos vertido aquí todo el contenido y los elementos adicionales que deseamos, podemos previsualizar el artículo y ya sea que lo encontremos listo para su publicación y lo publiquemos o bien que deseemos regresar a hacer alguna modificación y volvamos a esta.

Ésta es una pantalla del lado del administrador, veamos a continuación cómo se refleja del lado del usuario un artículo (pantalla 2).



Pantalla 2 Módulo ezArticle, usuario, despliegue artículo.

Diseño gráfico

Para entender y poder hacer el diseño gráfico de un sitio administrado por eZ Publish debemos ver bastantes particularidades de eZ Publish, es por ello que a medida que vamos necesitando elementos para describir el diseño les hacemos una introducción.

Todo sitio administrado con eZ Publish tiene dos caras, la del lado del usuario, donde se muestra el contenido que se ha vertido en el sitio y la del lado del administrador, donde se modifica, agrega o elimina el contenido o algún otro elemento del sitio.

En general, a la cara del usuario de un sitio administrado con eZ Publish llegamos a través de un URL de la forma:

http://www.sitio.com/

y al lado del administrador a través de un URL de la forma:

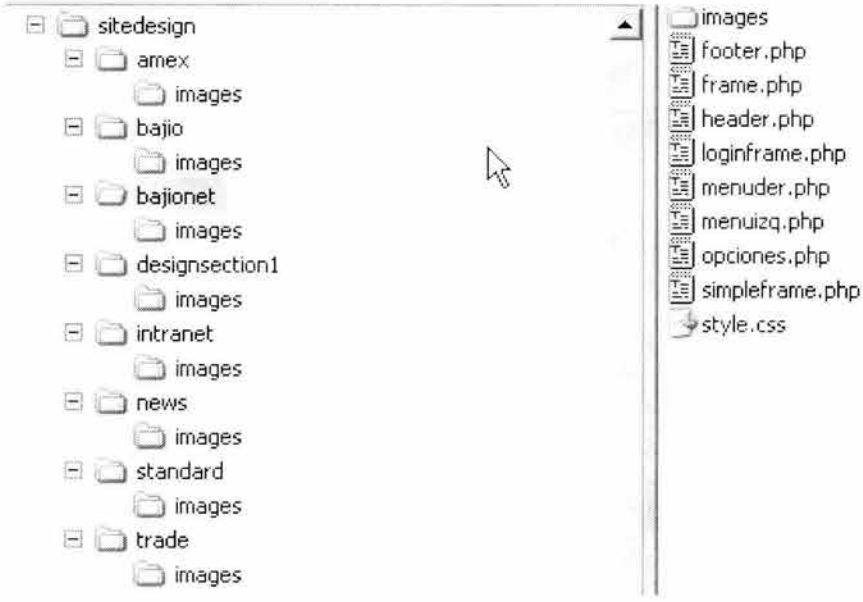
http://admin.sitio.com/

El diseño de un sitio, para el lado del usuario, se hace a través de los archivos que se encuentran en el directorio sitedesign/diseño/[xii].

Para entender un poco mejor esto, demos algunos antecedentes: en el módulo de contenido del SAC se pueden definir distintas categorías para el contenido. A cada categoría se le puede asociar una sección, que a su vez se define en el módulo de administración del sitio. Al momento de definir una sección le definimos un estilo de diseño que viene siendo en realidad una ruta donde encontraremos los archivos necesarios para darle forma, imagen y presentación al sitio. Estos archivos son estándar para los sitios hechos con eZ Publish y debemos proporcionar uno hecho por nosotros o bien una copia, si no nos interesa modificarlo, para cada uno de ellos y son:

- frame.php
- loginframe.php
- simpleframe.php

Veamos como se ve el directorio sitedesign de nuestro proyecto.



Además debemos incluir todas las gráficas u otros elementos que vayan a formar parte del diseño. Dentro del xhtml de nuestro diseño debemos poner rutas absolutas a todos los elementos que componen el diseño y, además, debemos asegurarnos de que por el tipo de elemento y extensión hemos añadido una excepción a la configuración de los filtros de mod_rewrite.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title><?php
// set the site title

$SiteTitle = $ini->read_var( "site", "SiteTitle" );
```

```
if ( isset( $SiteTitleAppend ) )
 print( $SiteTitle . " - " . $SiteTitleAppend );
else
 print( $SiteTitle );

?></title>
<link     rel="stylesheet"     type="text/css"     href="<?     print     $GlobalSiteIni->WWWDir;
?>/sitedesign/bajionet/style.css" />
<script type="text/javascript" language="JavaScript1.2">
<!--//

 function MM_swapImgRestore()
 {
  var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
 }

 function MM_preloadImages()
 {
  var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
  var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
  if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
 }

 function MM_findObj(n, d)
 {
  var p,i,x; if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
  d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
  if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
  for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document); return x;
 }

 function MM_swapImage()
 {
  var i,j=0,x,a=MM_swapImage.arguments; document.MM_sr=new Array; for(i=0;i<(a.length-2);i+=3)
  if ((x=MM_findObj(a[i]))!=null){document.MM_sr[j++]=x; if(!x.oSrc) x.oSrc=x.src; x.src=a[i+2];}
 }

//-->
</script>
<!-- set the content meta information desde site.ini -->
<meta name="description" content="<?php

if ( isset( $SiteDescriptionOverride ) )
{
 print( $SiteDescriptionOverride );
}
else
{
 $SiteDescription = $ini->read_var( "site", "SiteDescription" );
 print( $SiteDescription );
}

?>" />
<meta name="author" content="<?php

 $SiteAuthor = $ini->read_var( "site", "SiteAuthor" );
 print( $SiteAuthor );

?>" />
<meta name="copyright" content="<?php

 $SiteCopyright = $ini->read_var( "site", "SiteCopyright" );
 print( $SiteCopyright );

?>" />
<meta name="keywords" content="<?php
if ( isset( $SiteKeywordsOverride ) )
{
 print( $SiteKeywordsOverride );
```

```
}
else
{
 $SiteKeywords = $ini->read_var( "site", "SiteKeywords" );
 print( $SiteKeywords );
}

?>" />

<meta name="MSSmartTagsPreventParsing" content="TRUE">
</head>

<body bgcolor="#5A419c" topmargin="0" marginheight="0" leftmargin="0" rightmargin="0"
marginwidth="0"
onload="MM_preloadImages('/images/redigerminimrk.gif','/images/slettminimrk.gif','/images/downloa
dminimrk.gif','/images/addminimrk.gif')">
<?
include( "sitedesign/bajionet/header.php" );
?>

<table width="100%" border="0" cellspacing="0" cellpadding="0">
<tr>
 <td>
<!-- color utilizado "#5A419c"-->
<!-- Tabla Principal -->
<table width="100%" border="0" cellspacing="0" cellpadding="4">
<tr valign="top">
 <td width="1%" bgcolor="#ffffff">
 <!-- menu izquierdo inicia agregado por Alan Maciel 06112001 -->
 <?
 if ( $url_array[1] == "transaccion" )
 {
  include( "eztransaccion/user/userbox.php" );
 } else {
  include( "sitedesign/bajionet/menuizq.php" );
 }
 ?>
 <!-- menu izquierdo termina -->
 <img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif" width="130" height="8" border="0"
alt="" /><br />
 </td>

 <td width="1%" bgcolor="#ffffff"><img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif"
width="2" height="1" border="0" alt="0" /></td>
 <td width="96%" bgcolor="#ffffff">

 <!-- Main content view start -->
 <?
 print( $MainContents );
 ?>
 <!-- Main content view end -->

 <br />
 </td>
 <td width="1%" bgcolor="#ffffff"><img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif"
width="2" height="1" border="0" alt="0" /></td>

 <?php
 if ( $url_array[1] != "transaccion" )
 {
 ?>
 <td width="1%" bgcolor="#ffffff">

<!-- menu derecho inicia agregado por Alan Maciel 09112001 -->
 <!-- Right menu start -->
 <?
  include( "ezuserbb/user/userbox.php" );
 ?>
 <!-- dos opciones del menu derecho agregadas por Alan Maciel 14112001 -->
 <?
```

```
  include( "sitedesign/bajionet/opciones.php" );
 ?>
 <!-- dos opciones termina -->
 <?
  include( "ezarticle/user/tipocambio.php" );
 ?>
 <?
 include( "sitedesign/bajionet/menuder.php" );
 ?>

 <?
  //include( "ezform/user/formview.php" );
 ?>
<!-- menu derecho termina -->

 <!-- Right menu end -->

 <img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif" width="130" height="20" border="0"
alt="" /><br />

 </td>
 <?php
 ) // De si poner o no poner menu asociado a estar o no en las transacciones
 ?>
 </tr>
</table>
 </td>
 </tr>
</table>
<!--
<?

// Store the statistics with a callback image.
// It will be no overhead with this method for storing stats
//

$StoreStats = $ini->read_var( "eZStatsMain", "StoreStats" );

if ( $StoreStats == "enabled" )
{
 // callback for storing the stats
 $imgSrc = "/stats/store" . $REQUEST_URI . "1x1.gif";
 print(   "<img   src=\"$GlobalSiteIni->WWWDir$imgSrc\"   height=\"1\"   width=\"1\"   border=\"0\"
alt=\"\" />" );
}

?>

 <?
 $session =& eZSession::globalSession();


if ( $session->fetch() == false )
{
 $session =& eZSession::globalSession();
 $session->store();
}

if ( $Design == 1 )
{
 $session->setVariable( "SiteDesign", "intranet" );
 include_once( "classes/ezhttptool.php" );
 eZHTTPTool::header( "Location: $REQUEST_URI" );
 exit();
}

if ( $Design == 2 )
{
 $session->setVariable( "SiteDesign", "trade" );
 include_once( "classes/ezhttptool.php" );
```

```
 $redir = "/";
 if ( isset( $REQUEST_URI ) && ( $REQUEST_URI != "" ) )
 {
  $redir = $REQUEST_URI;
 }

 eZHTTPTool::header( "Location: $redir" );
 exit();
}

if ( $Design == 3 )
{
 $session->setVariable( "SiteDesign", "news" );
 include_once( "classes/ezhttptool.php" );

 $redir = "/";
 if ( isset( $REQUEST_URI ) && ( $REQUEST_URI != "" ) )
 {
  $redir = $REQUEST_URI;
 }

 eZHTTPTool::header( "Location: $redir" );
 exit();
}
 ?>
-->
<!-- footer inicia agregado por Alan Maciel 06112001 -->
<?
include( "sitedesign/bajionet/footer.php" );
?>
<!-- footer termina -->
</body>
</html>
```

Código 7 El archivo frame.php tal como se adecuó para el proyecto.

Como se ve, frame.php (código 7) es una combinación de php y xhtml. Su finalidad es ser el marco donde se despliegue la información que proviene tanto del resultado de una operación en un módulo como de las necesidades de navegación del sitio y del acceso a las operaciones de los módulos que se han considerado necesarios, todo esto dentro de la imagen gráfica que se haya definido.

El diseño que se ha utilizado en este caso y que le da estructura a la página es una tabla xhtml con 5 columnas. De estas 5 columnas dos son sólo para separar las restantes tres y de esas tres las dos de los extremos izquierdo y derecho son más angostas, la columna central es la más importante y será ahí donde se presente el contenido o el resultado de alguna operación de algún módulo.

Aprovechemos que estamos hablando de la operación de un módulo para definir aquí a qué nos referimos. La operación es para nosotros la capacidad que tiene algún módulo de realizar una tarea específica y que, en general, involucra un conjunto de parámetros en la solicitud de la operación y una página con el resultado de la realización de la tarea. Son ejemplos de operaciones, en el caso del módulo de contenido (article), el despliegue de un artículo en particular (articleview) y son parámetros para dicha operación, el identificador del artículo que se quiere ver, la página del artículo que se desea ver, la sección en la que se está desplegando, si el despliegue debe ser para impresión o normal, etc. En el caso del módulo de transacciones (transaccion), la consulta de los saldos de todas las cuentas del cliente (saldos).

La invocación de las operaciones y el paso de parámetros se realizan a través del URL de la solicitud, así, pues, la sintaxis en general es:

http://sitio/módulo/operacion/parametro/parametro…/

De aquí podríamos construir los siguientes UURRLL para las operaciones que dimos como ejemplo

http://sitio/article/articleview/id/pagina/

y

http://sitio/transaccion/saldos/

El flujo del proceso completo de atención a una solicitud es el siguiente (diagrama 4):

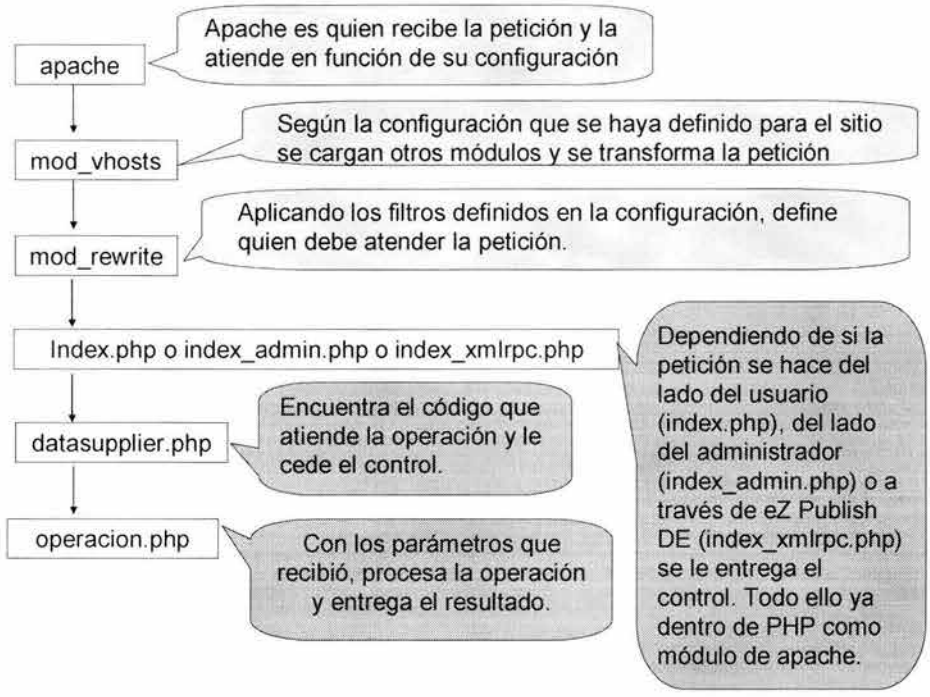


Diagrama 4 Flujo de la atención a una petición.

Debido a que eZ Publish se construyó utilizando el patrón MVC[xiii], una operación está compuesta por varios archivos, en el caso general tres, que pudieran ser, operacion.php que corresponde al controlador, operacion.tpl y operacion.php.ini que corresponden la presentación y, finalmente, la clase modulo.php que provee lo que sería el modelo.

La presentación de la información se realiza a través de un motor de plantillas que sirve para hacer las substituciones necesarias para la internacionalización y aquéllas que corresponden a la presentación. Una plantilla es un archivo que contiene xhtml, estructuras simples de control y variables de reemplazo. La estructura de control más común es BEGIN-END. Las variables de

reemplazo tienen la forma {intl-label} en el caso de etiquetas que han sido internacionalizadas para su traducción y {variable} en el caso de variables que serán reemplazadas por valores desde el controlador.

Es importante mencionar que cada módulo tiene su propio directorio a la vez que los archivos que forman el módulo están distribuidos en distintos directorios el criterio de distribución es el tipo del archivo. La distribución es la siguiente:

De los tres directorios que existen en un primer nivel de un módulo los archivos de control (datasupplier.php u operacion.php) se localizan, ya sea en *admin.*, *ya sea* en *user* según si atienden peticiones del lado administrador o del lado del usuario y las clases del módulo están en *classes*. Sin importar si es del lado del administrador o del usuario tenemos un directorio *intl* que a su vez contiene directorios del tipo *xx_XX* donde xx es la abreviatura para algún idioma y XX es la abreviatura para algún país y en su interior tenemos archivos del tipo *operacion.php.ini*. Igualmente tenemos un directorio *templates* que contiene un directorio *standard* que contiene los archivos del tipo operacion.tpl. Es muy importante señalar que en el caso de las plantillas el directorio *standard* corresponde a la sección standard. Así, pues, el contenido que se encuentre en una categoría que se haya definido como perteneciente a la sección standard se procesará para su presentación utilizando las plantillas que se encuentran en este directorio. Si se definen nuevas secciones, debemos crear directorios para ellas y poner al interior las plantillas que se encargarán de definir la presentación.

Veamos entonces algunos fragmentos importantes que nos ejemplifican tanto la construcción de la imagen como la navegación y la presentación del contenido o del resultado de una operación.

Para el despliegue de imágenes podemos utilizar las rutas que se han definido por configuración

```
<img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif" width="2"
height="1" border="0" alt="0" />
```

Para la presentación de elementos de navegación como los menús tenemos las dos columnas angostas que se encuentran del lado izquierdo y derecho. Se definió que el comportamiento fuera el siguiente:

Cuando el cliente esté consultando información, verá dos menús, izquierdo y derecho, en la parte superior del menú del lado derecho estará el acceso a la parte transaccional y el resto será información financiera. El menú del lado izquierdo serán ligas a la información de los productos y servicios del Banco y esta información desaparecerá para dar paso a las distintas transacciones a las que el usuario tenga derecho cuando se haya establecido una sesión para realizar operaciones.

El código que produce el menú izquierdo se ve así:

```
<?
if ( $url_array[1] == "transaccion" ) {
 include( "eztransaccion/user/userbox.php" );
} else {
 include( "sitedesign/bajionet/menuizq.php" );
}
?>
```

En cuanto al código del menú derecho este se ve así:

```
<?php
if ( $url_array[1] != "transaccion" )
{
?>
<td width="1%" bgcolor="#ffffff">
<?
 include( "ezuserbb/user/userbox.php" );
?>
<?
 include( "sitedesign/bajionet/opciones.php" );
?>
<?
 include( "ezarticle/user/tipocambio.php" );
?>
<?
include( "sitedesign/bajionet/menuder.php" );
?>
<img src="<? print $GlobalSiteIni->WWWDir; ?>/images/1x1.gif" width="130"
height="20" border="0" alt="" /><br />
```

```
</td>
<?php
}
?>
```

La inclusión de funcionalidad de otros módulos a nivel de la página principal o del resultado del procesamiento de alguna operación se logra a través de código como el que sigue:

```
<?
  include( "ezarticle/user/tipocambio.php" );
?>
```

En este caso lo que estamos presentando aquí al usuario es el tipo de cambio para el dólar norteamericano.

Sin duda, la parte más importante, aunque muy sencilla, dentro de frame.php es aquélla que presenta el resultado de la operación invocada.

```
<?
 print( $MainContents );
?>
```

Finalmente, aquello que le da homogeneidad al sitio y que nos permite cumplir con algunas premisas que se establecieron en los objetivos, son el encabezado y el pie de página. Al incluirlos en frame.php logramos que todo el sitio los comparta. El código para el encabezado y para el pie de página es muy similar. Presentamos aquí el del encabezado:

```
<?
include( "sitedesign/bajionet/header.php" );
?>
```

Esta revisión del diseño gráfico nos ha permitido familiarizarnos más con eZ Publish, de manera que ya podemos proceder a revisar el diseño que se hizo para los dos módulos de contenido que se agregaron a eZ Publish y que son eZBancos y eZTasas.

La necesidad que nos llevó a construir ambos fue el interés que tenía el área de mercadotecnia en resaltar una de las cualidades del Banco: el pago de tasas de interés a los inversionistas significativamente mayores a los de la competencia. El objetivo es presentar una página con un resumen de las tasas que paga la competencia, la tasa que está pagando el Banco y un porcentaje

de la diferencia entre el promedio de las tasas de la competencia y la tasa que paga el Banco. Así pues lo primero que se necesita es un catálogo de bancos competidores[xiv].

eZBancos

Se decidió hacer un módulo para el catálogo de los bancos en lugar de hacer uno solo que realizara las comparaciones y administrara el catálogo, porque se consideró que el catálogo de bancos pudiera ser, en un futuro, necesario en más de un módulo.

El diagrama (diagrama 5) de caso de uso que se obtuvo fue:

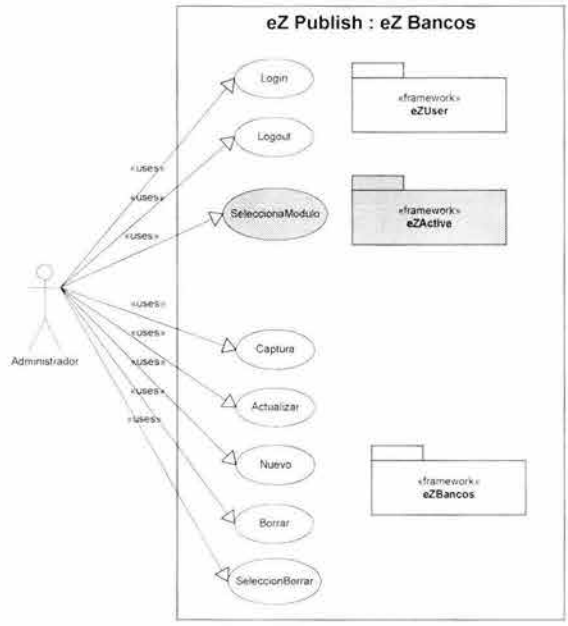


Diagrama 5 Caso de uso eZ Bancos.

Este módulo sólo tiene interfase del lado del administrador, puesto que la información que administra la procesan otros módulos y no se presenta directamente a los usuarios.

eZTasas

Por su parte eZTasas aprovecha el catálogo de bancos y nos permitirá capturar la tasa correspondiente a cada banco y seleccionar aquéllos contra los que se va a efectuar la comparación. Además, capturará la fecha con base en la cual se está haciendo la comparación de la información.

El diagrama (diagrama 6) de caso de uso que se obtuvo fue:

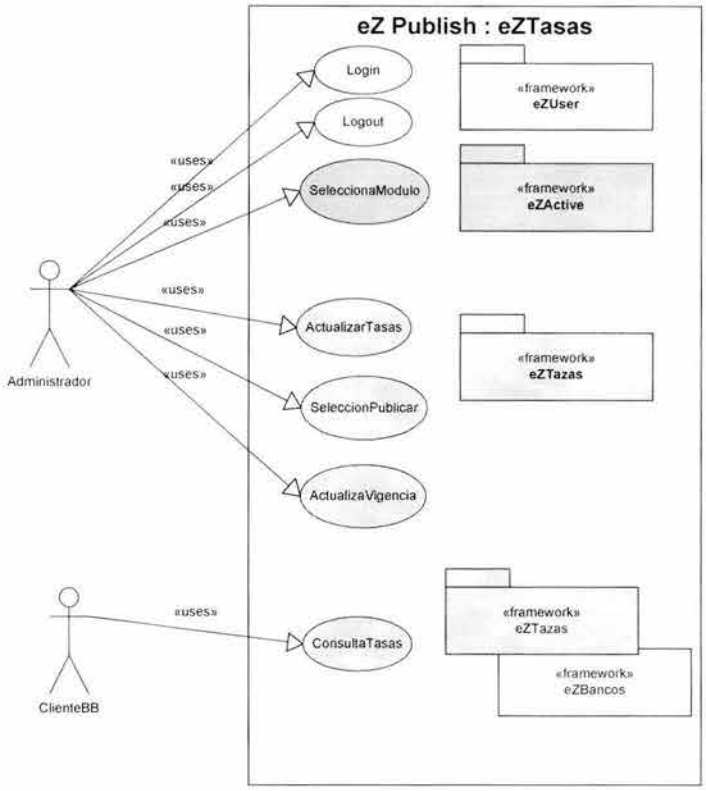


Diagrama 6 Caso de uso eZTasas.

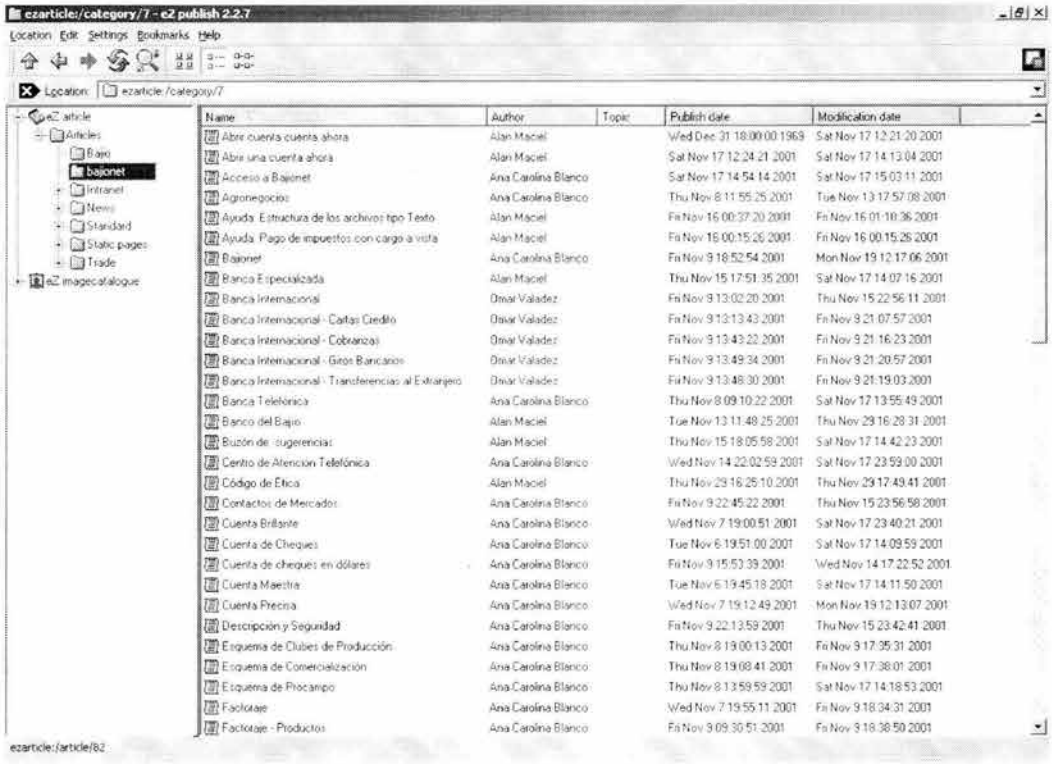
Finalmente, podemos aquí subrayar que gracias al diseño basado en patrones y a una buena implementación en programación orientada a objetos, eZ Publish tiene una buena jerarquización[xv], separa las funciones, los datos, los objetos, etc.

eZ Publish Desktop Edition[xvi]

Como sabemos, una de las razones importantes para seleccionar eZ Publish sobre las otra herramientas disponibles fue el hecho de que eZ Publish tiene una aplicación que corre nativamente y que sirve para la administración de todo lo que es contenido (eZArticle) y de lo que son las imágenes del sitio (eZImageCatalogue).

Veamos rápidamente un poco de esta herramienta eZ Publish Desktop Edition.

A continuación tenemos la aplicación mostrándonos (pantalla 3) el contenido de la categoría bajionet del módulo eZArticle:

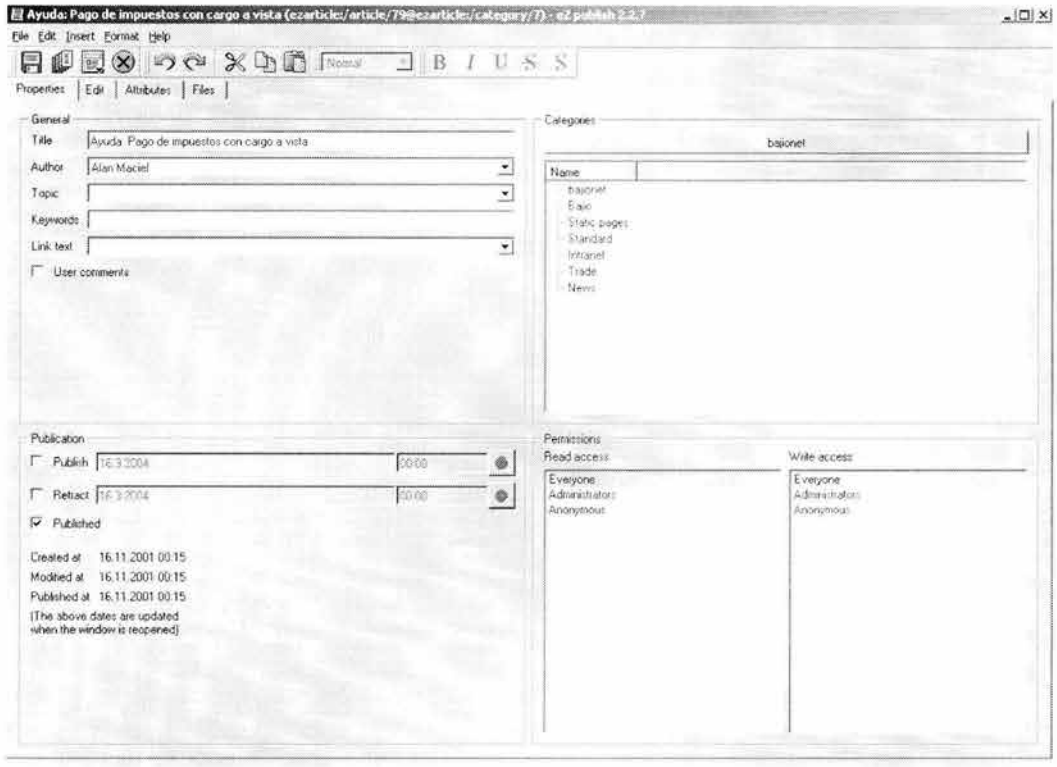


Pantalla 3 eZ Publish Desktop Edition, administración, listado de artículos en bajionet.

La aplicación (pantalla 3) mantiene, por principio, una ventana principal, que es la que vemos aquí, y abre nuevas ventanas para la edición tanto de artículos como de imágenes. Si revisamos esta pantalla, encontramos que está dividida en dos, del lado izquierdo dos árboles expandibles correspondientes a los dos módulos que nos permite administrar. Del lado derecho un listado del contenido disponible en la categoría que estamos administrando, artículos si estamos administrando contenido e imágenes si estamos administrando el catálogo de imágenes.

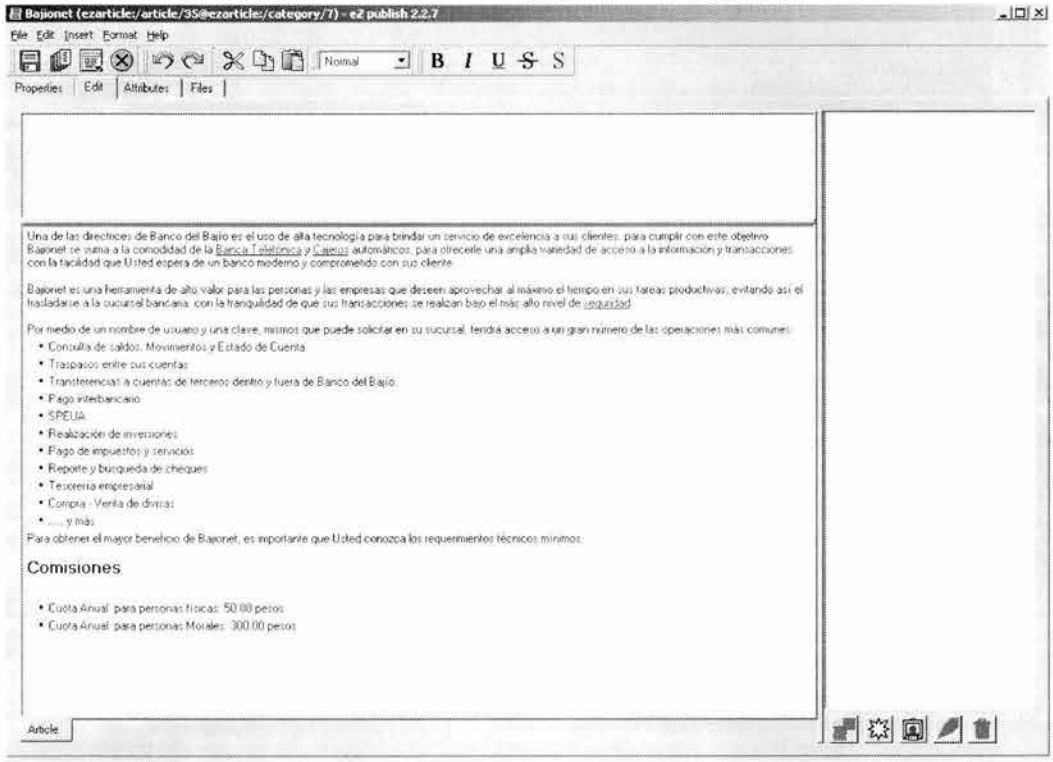
Si hacemos doble click sobre un artículo, obtenemos la siguiente pantalla (pantalla 4) como una ventana aparte. De esa pantalla podemos decir que es una analogía a lo que vemos en la página, con la diferencia de que aquí la información está dividida en varios tabuladores y en la página se encuentra continua.

Estamos viendo entonces las propiedades del artículo que le pedimos al sistema que nos dejara editar, así pues vemos y podemos modificar título, autor, tema, palabras clave, liga, categoría, programación de su publicación y permisos de acceso y modificación.



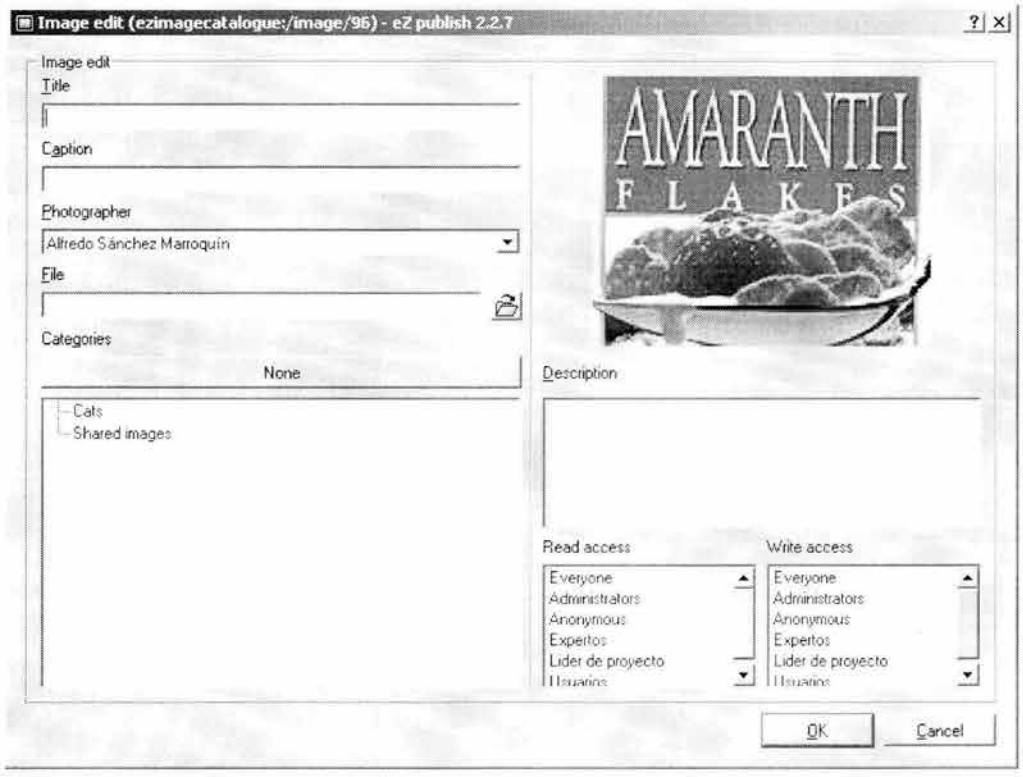
Pantalla 4 eZ Publish Desktop Edition, administración, propiedades de un artículo.

Si nos cambiamos a la pestaña de edición (pantalla 5) tenemos aquí acceso a modificar el contenido de este artículo, por ejemplo su resumen, su contenido mismo o las imágenes asociadas a él. En la parte inferior del recuadro del lado derecho tenemos unos botones que nos permiten agregar imágenes al artículo. Estas imágenes pueden estar en el catálogo o las podemos agregar específicamente para este artículo. Las herramientas de la barra de herramientas nos hacen más fácil la edición y la definición del formato. A través del menú podemos agregar elementos especiales como tablas, ligas, etc.



Pantalla 5 eZ Publish Desktop Edition, administración, modificación del contenido de un artículo.

La edición de una imagen (pantalla 6) se lleva a cabo desde una ventana a la que tenemos acceso desde el catálogo. Si lo deseamos, podemos modificar el título, el pie, el autor, la imagen misma, la categoría, la descripción y los permisos.



Pantalla 6 eZ Publish Desktop Edition, administración, modificación de una imagen.

Si lo que estamos haciendo es trabajar con el catálogo de imágenes lo que veremos al navegar entre las categorías es un listado como el siguiente (pantalla 7):

Pantalla 7 eZ Publish Desktop Edition, administración, listado de imágenes de una categoría.

Utilizando la barra de herramientas, podemos modificar el listado para que nos muestre las imágenes junto con sus características, las imágenes en su tamaño original, o, como lo tenemos ahora, las imágenes en forma reducida para ver más por pantalla.

El manejo de esta herramienta es muy fácil e intuitivo, es por ello que se recomienda, y así lo hizo BB, que si el personal que va a administrar el contenido del sitio no tiene preparación técnica utilice eZ Publish Desktop Edition en lugar de trabajar directamente con eZ Publish, dado que así que se ahorra, entre otras cosas, aprender la sintaxis de las instrucciones de formato e inclusión de elementos.

El sistema aplicativo o transaccional

Desafortunadamente, para poder cumplir con los compromisos de confidencialidad que se tienen con BB no vamos a poder ver con el detalle que nos gustaría presentarlo aquí, ni el diseño ni la construcción de lo que es la parte transaccional de la solución. Esto no nos impedirá ver todo lo necesario para comprender su funcionamiento y apreciar su flexibilidad.

Con la idea de cumplir con los objetivos de seguridad marcados, toda la comunicación que se realice con los clientes de BB en relación con las operaciones financieras, se hará utilizando un canal seguro de comunicaciones, es decir, a través del protocolo https que implementa SSL sobre el protocolo http, que es el que comúnmente utilizan los navegadores.

Una primera decisión es que vamos a utilizar eZ Publish como marco de construcción. De esta manera el módulo de transacciones financieras se integra con el módulo de administración de contenido y no separa las cosas. Utilizando eZ Publish como framework tenemos además bibliotecas para internacionalización, un motor de plantilla, el control de las sesiones y el soporte aplicativo, entre otras cosas.

Utilicemos un caso de uso genérico (diagrama 7) para revisar el diseño:

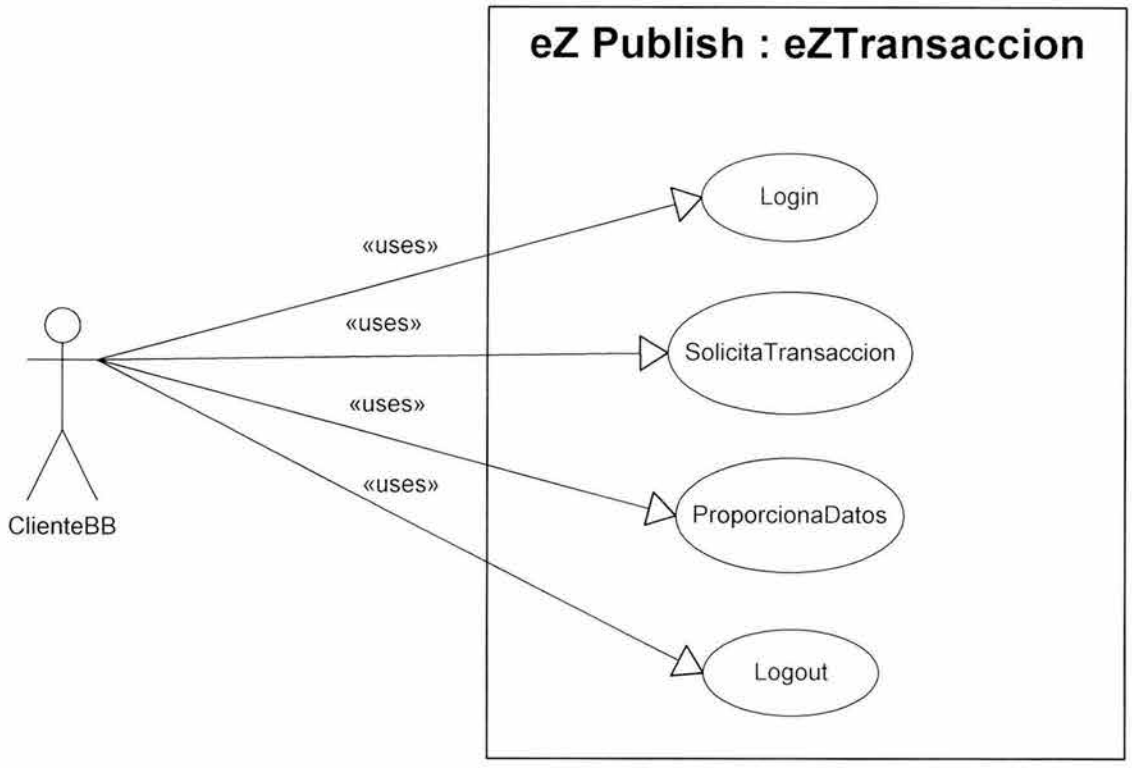


Diagrama 7 Caso de uso genérico de una transacción.

Como vemos, la realización de toda transacción tiene que pasar por un proceso de autenticación del usuario. Esta autenticación nos deberá devolver, además, los permisos para el usuario a fin de que se construya una lista dinámica de las operaciones que puede realizar.

Para autenticar a los usuarios podríamos utilizar el módulo de administración con el que cuenta eZ Publish. Sin embargo, tenemos que realizar una transacción con Ovation, puesto que, como una regla de seguridad, el sistema no almacenará información sobre los usuarios, para que en el caso de que haya una intrusión, no se vean comprometidos y además para que no se tenga una base de usuarios duplicada y se tenga que darle mantenimiento a cada usuario en dos lugares. Esto confirma el papel del sistema transaccional como middleware o gateway transaccional.

Los diálogos con Ovation se tienen que realizar a través del protocolo http dado que eso es lo que él ofrece. Como Ovation no será el único backend bancario con el que tendremos que realizar transacciones, llegamos a la conclusión de que debemos construir nuestro middleware a través de una clase que nos dé la flexibilidad necesaria para poder usar distintos protocolos con distintos back ends bancarios. Es decir nuestro módulo tendrá un núcleo que encapsule los distintos protocolos y la complejidad inherente, así como las comunicaciones y la bitácora, para satisfacer el requisito de auditabilidad que nos exige la seguridad de un sistema.

Esto lo lograremos conceptualizando el módulo transaccional como un API que utilizarán las distintas operaciones financieras para llevar al cabo su tarea. El modelo en el que una operación financiera es equivalente a una operación en eZ Publish nos permite hacer uso del mismo patrón de desarrollo que tiene el resto de eZ Publish lo que nos da la ventaja de hacer homogéneo

nuestro módulo con el resto de los módulos, ganando así en familiaridad, mantenimiento y sencillez de desarrollo.

El hecho de que Ovation utilice http para la realización de sus transacciones nos lleva a implementar al menos los métodos POST y GET de dicho protocolo. Por esta razón, en el análisis, el diseño y la construcción veremos primero el módulo de eZTransaccion y posteriormente nuestro módulo de autenticación, eZUserBB.

Dado que tenemos operaciones financieras que son de uno, de dos y de tres pasos dejaremos que el control de flujo se lleve en el nivel de la operación y no en el nivel del núcleo.

Éste es el marco general que nos sirve para describir el detalle de cada uno de los dos módulos que se desprenden de nuestras necesidades.

eZTransaccion

Para empezar veamos como queda el diagrama (diagrama 8) una vez que hemos hecho la precisión sobre la autenticación de los usuarios:

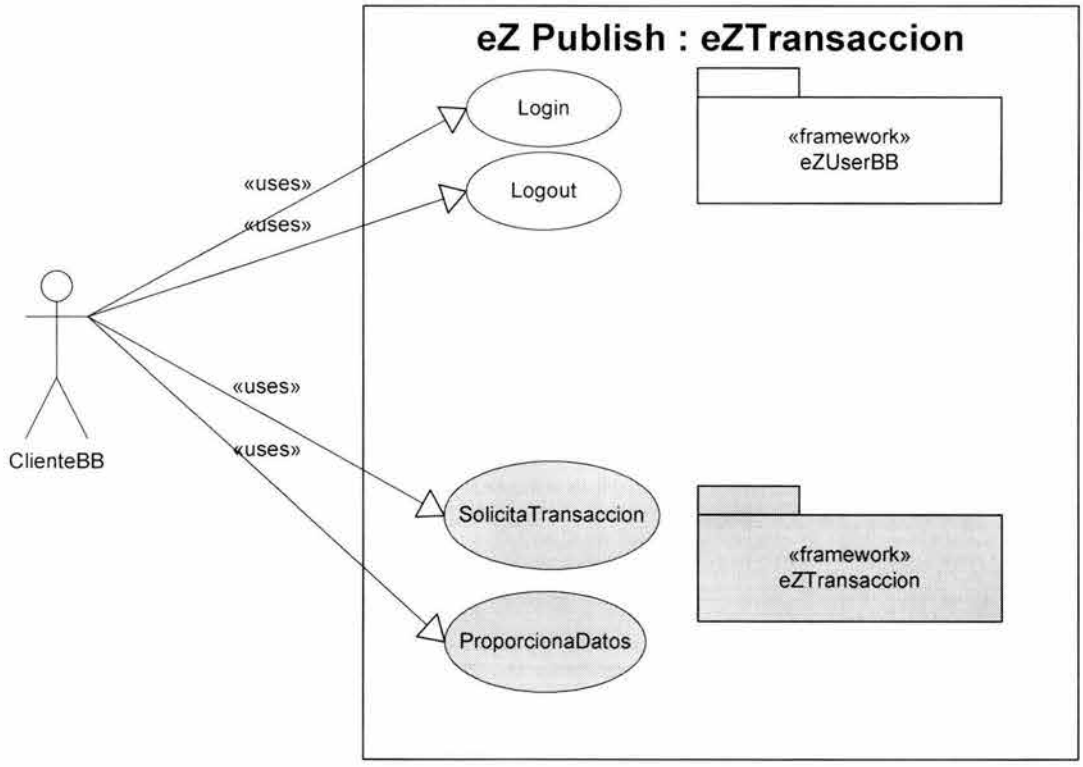


Diagrama 8 Un caso de uso genérico de una transacción que incluye los módulos encargados de su atención.

En resumen, podemos decir que el módulo eZTransaccion tomará las solicitudes de los clientes, las hará llegar al sistema bancario al que le corresponde atenderlas y tomará los resultados que le proporcione dicho backend bancario para presentarlos al usuario.

Se deduce entonces que eZTransaccion va a tomar las peticiones, construir los mensajes adecuados en el protocolo necesario, establecer el diálogo, enviar y recibir la información, terminar el diálogo, hacer las transformaciones necesarias para la respuesta y presentarla al usuario. Por cada petición que atienda el módulo debe crear un registro en la bitácora.

eZUserBB

Por su parte, este módulo debe construir un mensaje con los datos del usuario, hacer una solicitud de autenticación al backend bancario y, en caso de obtener una respuesta positiva, crear una sesión para el usuario y ponerla a disposición para el resto de los módulos. En caso de que la autenticación no sea positiva debe enviar un mensaje al usuario informándole del problema. En ambos casos se deberá guardar un registro en la bitácora.

Lo que hace necesaria una transacción especial y distinta del resto de las transacciones bancarias es, precisamente, la necesidad de tener una sesión del usuario y evitar así que para cada transacción financiera se deba volver a proporcionar el usuario y la clave del cliente.

Como una medida de seguridad, una sesión que ha estado inactiva por más de 5 minutos se marca como inválida, será necesario que el usuario vuelva a proporcionar sus credenciales para poder seguir realizando operaciones.

Usaremos como base eZUser, dado que ya tiene todo el soporte para las sesiones y los reintentos. Cambiaremos únicamente la función que comparaba los datos proporcionados por el cliente con los almacenados en la base de datos de eZ Publish, para que ahora, en lugar de hacerlo así, realice una transacción proporcionándole al backend bancario dichos datos y que reciba y procese la respuesta correspondiente.

La implementación del diseño de ambos módulos la veremos en el capítulo de construcción dentro de la sección correspondiente a cada uno de los módulos.

La seguridad

Con el fin de tenerlos frescos repasemos rápidamente los objetivos sobre seguridad que nos hemos marcado:

- Debe abarcar todos los aspectos de la solución.
- Que la solución nunca sufra una intrusión.
- El contenido nunca deberá ser modificado por alguien sin autorización.
- Nunca se debe permitir realizar una transacción a alguien que no se haya autenticado como el legítimo cliente.
- La información de los clientes y su información financiera nunca debe ser vista por alguien distinto del cliente mismo.

Otra referencia que necesitamos para determinar los servicios de seguridad que necesitamos es la organización de BB: por esta razón a continuación presentamos una relación de las áreas que intervienen en bajio*net* y sus responsabilidades.

Auditoría.

Responsabilidad: Auditoría, resguardo, verificación.

Reporta a: Dirección General.

Rol: Resguarda las claves de máxima seguridad y aquéllas que involucran la identidad del Banco.

Claves bajo su resguardo: Frase clave del certificado digital del banco y frase clave de LIDS.

Desarrollo de sistemas.

Responsabilidad: Programación y mantenimiento de los sistemas del banco.

Reporta a: Dirección de Sistemas.

Rol: Constructor de sistemas. Entrega a Aseguramiento de Calidad los sistemas que han sido terminados de acuerdo a las especificaciones y previa aceptación del área solicitante.

Claves bajo su resguardo: *root* de los servidores de desarrollo.

Aseguramiento de Calidad de sistemas.

Responsabilidad: Pruebas y validación de los sistemas del banco.

Reporta a: Dirección de Sistemas.

Rol: Pase a producción de los sistemas que se deben utilizar. Pase a producción del contenido del sitio.

Claves bajo su resguardo: *root* de los servidores de aseguramiento de calidad.

Producción.

Responsabilidad: Operación de los sistemas, respaldo de datos.

Reporta a: Dirección de Sistemas.

Rol: Se encarga de la operación de los equipos y sistemas que brindan los servicios a los clientes. Son responsables de la disponibilidad cotidiana de los sistemas, de los respaldos y de su alta y su baja.

Claves bajo su resguardo: *root* de los servidores de producción.

Infraestructura.

Responsabilidad: Instalación y mantenimiento de servidores.

Reporta a: Dirección de Sistemas.

Rol: Se encarga de la instalación y del mantenimiento de servidores y sistemas que necesitan las distintas áreas.

Claves bajo su resguardo: Ninguna.

Redes.

Responsabilidad: Instalación y mantenimiento de redes de área locales, corporativa y enlace a Internet. Instalación, configuración y mantenimiento de equipos de red.

Reporta a: Dirección de Sistemas.

Rol: Se encarga de la configuración de los equipos de seguridad de red que intervienen en bajio*net*.

Claves bajo su resguardo: Equipo de red y de seguridad en red.

Mercadotecnia.

Responsabilidad: Definición de productos y servicios del banco. Promoción y difusión de los productos y servicios del banco.

Reporta a: Dirección General.

Rol: Administración y mantenimiento del contenido del sitio.

Claves bajo su resguardo: Usuario de eZ Publish con privilegios de administración de contenido.

Si combinamos estos dos bloques de información, los requisitos y las áreas obtendríamos el siguiente cuadro:

Necesidad	Solución	Herramienta
Debe abarcar todos los aspectos de la solución.	Análisis individual de la seguridad de: • Sistema operativo • Servidor de páginas • Aplicación	
Sistema operativo seguro.	Instalación siguiendo estándares de seguridad. Actualización constante.	Instalador hecho para BB. Responsabilidad de Infraestructura.
Servidor de páginas.	Instalación siguiendo estándares de seguridad. Actualización constante.	Instalador hecho para BB. Responsabilidad de Infraestructura.
Aplicación.	Auditoría de código por el equipo de desarrollo y aseguramiento de calidad.	El uso de Zend Studio en esta fase ayudó con la base del análisis ya que ofrece un nivel automatizado de verificación de código; no es un análisis de seguridad es sólo un análisis estático.
	Cifrado del código fuente.	Zend Encoder hizo una compilación y el cifrado de todos y cada uno de los programas de la aplicación.
	Creación de una base de datos con información para detectar modificaciones.	Tripwire creó una base de datos que permite verificar si algún archivo que existe en la base de datos ha sido modificado.
	El código de toda la aplicación se ocultó a todos los usuarios del equipo con excepción del usuario con el que corre el servidor de páginas.	LIDS nos sirve para ocultar e impedir de esta manera el acceso a información residente en el servidor.
Que la solución nunca sufra una intrusión.	La base para alcanzar este objetivo es un sistema	Libsafe. Con libsafe implementamos un esquema

Necesidad	Solución	Herramienta
	operativo seguro y que tanto el servidor de páginas como la aplicación, aun cuando tengan una vulnerabilidad, ésta no derive en que comprometan a al sistema de forma que se logre una intrusión.[xvii]	de contención para aplicaciones vulnerables que evita que una vulnerabilidad no conocida o no atendida se convierta en un riesgo.
	Además se requiere monitorear las actividades que se llevan a cabo en el servidor.	Hostsentry. Nos permite identificar actividades de riesgo.
	Y también es necesario monitorear la actividad de red en la que está involucrado.	Portsentry. Puesto que detecta la actividad de red en relación con el equipo protegido y reacciona conforme a lo indicado.
	Dado que las aplicaciones y los servicios de seguridad reportan tanto su actividad normal, sus errores y sus alarmas a las bitácoras del sistema su supervisión es parte de los servicios de seguridad necesarios.	Log check facilita la labor de supervisión de las bitácoras.
El contenido nunca deberá ser modificado por alguien sin autorización.	El contenido del sitio es responsabilidad de mercadotecnia, por definición. Por ello el único autorizado para modificar contenido será el usuario del sistema de administración de contenido que tenga mercadotecnia.	eZ Publish. En su administración de usuarios se definirá un solo usuario con la capacidad de modificar contenido y será el de mercadotecnia.
	Creación de una base de datos con información para detectar modificaciones.	Tripwire creo una base de datos que permite verificar si algún archivo que existe en la base de datos ha sido modificado.
	El código de toda la aplicación se ocultó a todos los usuarios del equipo con excepción del usuario con el que corre el	LIDS nos sirve para ocultar e impedir de esta manera el acceso a información residente en el servidor.

Necesidad	Solución	Herramienta
	servidor de páginas.	
Nunca se debe permitir realizar una transacción a alguien que no se haya autenticado como el legítimo cliente.	Este es un requisito que se debe satisfacer a nivel aplicativo, por ello se construirá un módulo, eZUserBB, que será el encargado de satisfacerlo.	eZUserBB, se encargará de validar las credenciales presentadas por los usuarios ante Ovation, el sistema que tiene la base maestra de clientes de BB.
La información de los clientes y su información financiera nunca debe ser vista por alguien distinto del cliente mismo.	Para dar cumplimiento a este objetivo toda la información del cliente y la información financiera que se transmita entre los servidores de BB y el equipo del cliente viajará cifrada. Como el protocolo de transporte para dicha información será http y el cifrado estándar para http es SSL utilizaremos una de las implementaciones que hay para ello.	mod_ssl es una implementación del protocolo SSL para Apache.

Vale la pena hacer notar que en el capítulo 4, Construcción de la solución, hay una descripción de cada una de las herramientas y de su configuración. La configuración fue hecha como parte de este trabajo y para hacerla se consideraron los parámetros de diseño definidos aquí.

El lema que podríamos aplicar siempre que hablamos de este tema es *seguridad con funcionalidad* puesto que deseamos un sistema lo más seguro posible sin perder nada de la funcionalidad que es necesaria. Teniendo esto en cuenta veamos cómo se puede alcanzar en la práctica.

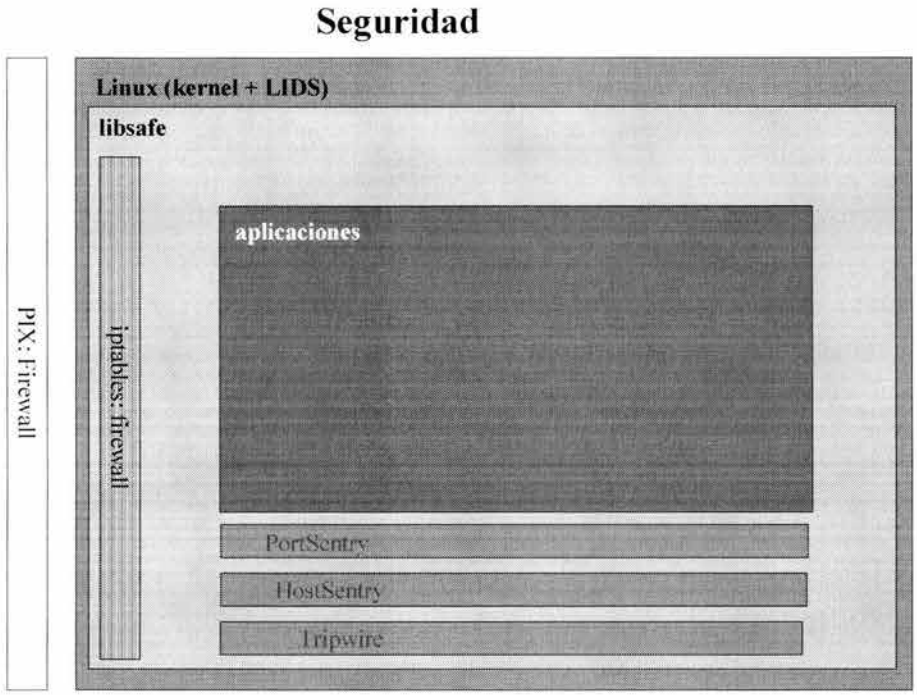


Diagrama 9 Diagrama conceptual del diseño de seguridad.

En este diagrama (diagrama 9) hemos puesto una representación de los elementos que estaremos integrando. Una primera lectura que se le puede dar es por capas. Pensemos en el kernel de Linux como la capa inferior; sobre ella pondremos una herramienta LIDS que nos ayude a hacer del kernel un kernel más seguro, entendiendo aquí seguridad como el control de las funciones que puede llevar a cabo un proceso más allá de las restricciones que puedan existir por el usuario que lo ejecuta, las restricciones que puedan existir sobre el acceso a un directorio o archivo más allá de las que proporciona el sistema operativo, es decir, a nivel de usuario y grupo y de lectura, escritura y ejecución y la definición de estos parámetros a través de una frase clave distinta a la del administrador. En el nivel del kernel también tenemos el firewall que controla la conectividad. Luego todas las bibliotecas de sistema forman una siguiente capa; para aumentar su seguridad pondremos libsafe. En el nivel aplicativo tenemos a PortSentry, HostSentry, Logcheck y Tripwire que están supervisando las actividades de las aplicaciones (diagrama 10).

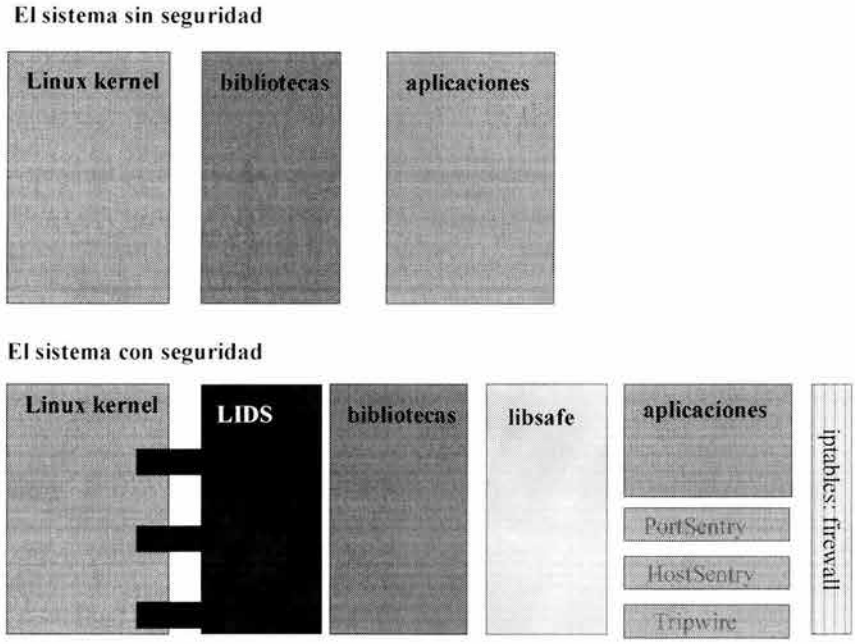


Diagrama 10 Integración de la seguridad.

Para hacer más claro el diseño, lo hemos dividido en tres grandes áreas, sistema operativo, aplicación y datos.

Sistema Operativo

En el nivel del sistema operativo, nuestra mayor preocupación es el hecho de que la cuenta de administración, *root*, es todopoderosa entiéndase por "todo poder" el hecho de que un usuario que ha establecido una sesión utilizando esta cuenta puede ejecutar cualquier programa, ver, modificar o borrar cualquier archivo y administrar usuarios es decir no hay ninguna actividad que esté restringida para él. Por la parte de los usuarios no administradores del sistema, que en principio es un número muy reducido ya que, como una recomendación de seguridad, no se crean cuentas de usuario en los equipos que forman parte de la infraestructura de banca por Internet, queremos saber cuándo alguna de sus actividades en el equipo es de alguna manera sospechosa. Adicionalmente, queremos saber cuándo alguien realiza una revisión remota del equipo buscando vulnerabilidades o servicios disponibles a fin de atacarnos.

Así, pues, para proteger el sistema operativo vamos a ponerle LIDS, que nos ayudará al control del todopoderoso administrador, PortSentry para que se detecten y bloqueen los escaneos, HostSentry para monitorear las actividades de los usuarios normales y, finalmente, logcheck para que se emitan alertas cuando en las bitácoras exista un reporte que así lo amerite.

LIDS

LIDS es un conjunto de cambios, parches al kernel de Linux, que le permiten un control granular sobre las capacidades de los usuarios y de los procesos. Gracias a su integración con el kernel, se

tiene una solución que corre en el nivel más esencial de un sistema operativo, siendo ideal para el tipo de tareas que se le encomiendan. En LIDS se define una clave, distinta a la del administrador, que nos permite configurar privilegios, permisos, etc. y que se almacena utilizando el algoritmo RIP160.

Se seleccionó LIDS porque es la única herramienta encontrada durante la investigación que cumple con nuestras necesidades.

PortSentry

Gracias a sus avanzados algoritmos de detección de escaneos y a su capacidad de reacción mediante el bloqueo de los puertos y de las rutas de comunicación con el atacante, es la herramienta adecuada cuando se desea estar prevenido contra los ataques remotos.

Se seleccionó PortSentry porque es parte de un conjunto de herramientas, Abacus, del cual una de ellas, HostSentry es la única conocida en su género y, dado que al utilizar el conjunto se obtiene una mejor integración, se prefirió sobre otras alternativas. Además es de las pocas herramientas que tienen un carácter reactivo, no sólo informativo.

HostSentry

En los asuntos de seguridad, el principio correcto es sospechar hasta de nuestra propia sombra, por ello importa poder monitorear las actividades de los usuarios de nuestro sistema, aun cuando nosotros les hayamos dado las cuentas y los permisos para utilizarlas. HostSentry es ideal para detectar cuándo alguna de ellas ha sido comprometida o bien cuándo hay un usuario que está llevando al cabo acciones contrarias a lo que se supone.

Se seleccionó HostSentry porque es la única conocida en su género.

Log Check

Una vez que el resto de las herramientas han hecho su parte y la han reportado a las bitácoras, log check está aquí para comunicarnos cuándo hay algún evento que por su relevancia puede llegar a requerir de nuestra atención.

Aplicaciones

Las acciones para proteger las aplicaciones son las siguientes:
Debido a que la solución la integramos utilizando muchas distintas aplicaciones y a que no es factible hacer una revisión en el nivel del código de todas y cada una de ellas, vamos a poner libsafe[xviii] para interceptar y protegernos de los ataques más comunes, *buffer overflow* y *string format*, a las aplicaciones.

Como nuestros sistemas de administración de contenido y de transacciones bancarias estarán ambos escritos en PHP, y PHP es normalmente un lenguaje interpretado, resulta que el código fuente está siempre disponible cuando la aplicación corre. Dado que tener el código fuente disponible y a la vista de cualquiera que pudiera lograr una intrusión es peligroso, se decidió recurrir a las herramientas de Zend para lograr la compilación del código fuente de la aplicación.

Y en términos de programación, aparte de haber auditado el código por parte de las herramientas de Zend y de todos los miembros del equipo de BB, se implementó la caducidad de sesión, para que se minimice el riesgo de que una sesión donde un usuario ya se haya autenticado sea secuestrada[xix] o se quede inadvertidamente disponible.

Datos

En el sistema integral de banca por Internet tenemos dos tipos de datos, aquéllos concernientes a las transacciones financieras que se están realizando y aquéllos relativos a la información de productos y servicios del Banco. Por su naturaleza y por perseguir objetivos de protección distintos, requieren tratamientos distintos.

Veamos primero los datos de productos y servicios del banco. Nuestro objetivo aquí es evitar que sean modificados. Obviamente, a ningún banco le gustaría ver su página afectada por el vandalismo de algún intruso.

Como la información de productos y servicios del banco está almacenada en la base de datos del sistema de administración de contenido, lo que tenemos que hacer es restringir el acceso en el nivel de la base de datos de forma que su modificación no sea viable.

Sabemos que la base de datos, MySQL, nos ofrece la capacidad de definir permisos de acceso a nivel base, tabla y equipo. Definiremos entonces que sólo usuarios con clave y conectados desde el mismo equipo podrán tener acceso al servidor de bases de datos. Adicionalmente, diremos que sólo un usuario con una clave definida para cumplir con los más altos estándares de seguridad[xx] pueda tener acceso a la base de datos del sistema. Configuraremos también el motor de bases de datos para que guarde la información de las claves de los usuarios utilizando el algoritmo md5. Así, si alguna llegara a ser comprometida, no será posible obtener la clave sino sólo la versión cifrada de la clave.

Adicional a la información sobre productos y servicios que tenemos en la base de datos, están todos los elementos gráfico, tanto los que dan forma al sitio, sitedesign/xxx/, como aquéllos que ilustran los artículos, ezimagecataloge/files/. Es por esta razón que, apoyándonos en LIDS, ocultaremos cuando menos esos dos directorios, para que no sean visibles. Adicionalmente, a través de los permisos para los archivos que establece el sistema operativo, éstos estarán restringidos para que no sean modificables.

Para la protección de los datos de las transacciones financieras, debido a que éstos residen en el backend bancario y podríamos decir que sólo son responsabilidad nuestra mientras los entregamos a los clientes, bastará, para no comprometerlos, que cifremos toda comunicación que haya entre nosotros y los clientes de BB.

Para ello nos apoyaremos en la capacidad de apache de incorporar capacidades para cifrar las comunicaciones http utilizando el protocolo SSL.

Cubiertos así los requisitos de seguridad que necesitamos resolver a nivel del diseño, pasemos, pues, a ver la construcción del sistema integral de banca por Internet.

Capítulo 4 Construcción de la solución

Implementación del IVA

La implementación del IVA involucra la realización de las siguientes actividades:

- Instalación del software base y de la infraestructura.
- Implantación del sistema modular de transacciones financieras.
- Implantación de las herramientas de administración del Internet Virtual Appliance.
- Aspectos de seguridad, de presentación y navegabilidad.
- Afinación y puesta a punto.

Adecuación y ampliación

En lo que se refiere a la adecuación de eZ Publish necesitamos dos cosas, una selección de módulos adecuada y que esté en español. En cuanto a lo que es ampliación, tenemos que ofrecer lo necesario para que el área de mercadotecnia pueda hacer la comparación de tasas que desea.

Por ello, para satisfacer las necesidades de BB en cuanto a la administración de contenido, debemos, antes que nada, contar con un sistema en el idioma natural para los usuarios. Así, pues, la primera parte de la adecuación será ponerlo en español.

Traducción

Se hizo la traducción al español del sistema eZ Publish y de eZ Publish Desktop Edition.

eZ Publish, viene listo para ser internacionalizado y, de hecho, viene naturalmente en dos idiomas: noruego e inglés.

Los archivos (código 8) que contienen las etiquetas son como el que se presenta a continuación. En su forma original se ve así:

```
[strings]
head_line=Edit Article
article_name=Title
article_author=Author
article_author_email=Author Email
link_text=Link text
category=Category
additional_category=Additional categories
intro=Lead in
contents=Content
pictures=Images
media=Media
preview=Preview
error_parsing_xml=Couldn't parse xml, check your &lt;tags&gt;
article_is_published=Publish article
files=Files
cancel=Cancel
ok=OK
none=None
groups=Groups with read access
```

```
groups_write=Groups with write access
all=Everyone
owner_group=Owner group
discuss_article=Enable user comments
keywords=Keywords
article_topic=Topic
no_topic=-- No topic --
log_message=Log message
log_history=Log history
attributes=Attributes
start_date=Publish date
stop_date=Retract date
day=Day
month=Month
year=Year
hour=Hour
minute=Minute
forms=Form
add_item=Add Item
created=Created
modified=Modified
un_published=Unpublished
published=Published
article_is_pending=Article is pending
new_author_name=New author name
new_author_email=New author email
```

Código 8 Ejemplo de un archivo .ini.

Una vez traducido (código 9) se ve así:

```
[strings]
head_line=Editar articulo
article_name=Titulo
article_author=Autor
article_author_email=Direccion de correo electrónico del autor
link_text=Texto de la liga
category=Categoría
additional_category=Categoria adicional
intro=Resumen
contents=Contenido
pictures=Imágenes
media=Medio
preview=Previsualización
error_parsing_xml=No fué posible validar el archivo xml, por favor verifique su tags &lt; &gt;
article_is_published=Articulo publicado
files=Archivos
cancel=Cancelar
ok=Ok
none=Ningún
groups=Grupos de usuarios con permiso de lectura
groups_write=Grupos con permiso de escritura
all=Todos
owner_group=Grupo dueño
discuss_article=Discutir articulo
keywords=Palabras clave
article_topic=Tema
no_topic=-- Sin tema --
log_message=Guardar mensaje
log_history=Guardar historia
attributes=Atributos
start_date=Fecha de publicación
stop_date=Fecha de eliminación
day=Dia
month=Mes
year=Año
hour=Hora
```

```
minute=Minúto
forms=Forma
add_item=Agregar elemento
created=Creado
modified=Modificado
un_published=No publicado
published=Publicado
article_is_pending=El articulo está pendiente
new_author_name=Nombre del nuevo autor
new_author_email=Correo electrónico del nuevo autor
```

Código 9 Ejemplo de un archivo .ini traducido.

El formato interno del traductor (código 10) es una forma especial de XML. El ejemplo que sigue nos lo muestra cuando estamos hablando del archivo interno para la traducción de inglés a español.

```
<!DOCTYPE TS><TS>
<context>
    <name>admin/intl/en_GB/error.ini [Error]</name>
    <message>
        <source>You can not add articles on this site!</source>
        <comment>Key: 1</comment>
        <translation>!Usted no puede agregar articulos en este sitio!</translation>
    </message>
    <message>
        <source>A file with this name already exist on the server!</source>
        <comment>Key: 2</comment>
        <translation>!Un archivo con ese nombre ya existe en este servidor!</translation>
    </message>
    <message>
        <source>You can not delete articles on this site!</source>
        <comment>Key: 3</comment>
        <translation>!Usted no puede borrar articulos en este sitio!</translation>
    </message>
    <message>
        <source>This article does not exist!</source>
        <comment>Key: 4</comment>
        <translation>!Este articulo no existe!</translation>
    </message>
    <message>
        <source>You can not edit articles on this site!</source>
        <comment>Key: 5</comment>
        <translation>!Usted no puede editar articulos en este sitio!</translation>
    </message>
    <message>
        <source>You can not edit preferences for this site!</source>
        <comment>Key: 6</comment>
        <translation>!Usted no puede cambiar las preferencias en este sitio!</translation>
    </message>
</context>
```

Código 10 Ejemplo de un archivo .ts (fragmento).

El proceso de traducción es el siguiente:

1. Instalar las herramientas, ezlupdate, ezlrelease y qtlinguist.
2. Ejecutar. ezlupdate en el directorio donde está nuestra instalación de eZ Publish. Esto genera o actualiza, según sea el caso, un archivo tipo .ts propio para hacer traducciones con QT Linguist.
3. Ejecutar qtlinguist y hacer la traducción.

4. Correr ezlrelease en el mismo directorio donde hicimos la corrida de ezlupdate para que el contenido traducido del archivo .ts se vierta en nuevos .php.ini en los directorios correspondientes.
5. Opcionalmente se puede enviar la traducción a los creadores de eZ Publish, la empresa eZ Systems, para que la pongan a disposición de otros usuarios de eZ Publish.
6. Durante el proceso de traducción, hablando concretamente del paso 3, contamos con la valiosa ayuda de QT Linguist. Veamos por qué hablamos de que QT Linguist nos brinda una valiosa ayuda.

El primer paso del proceso al interior de QT Linguist es armar una lista de todas las cadenas distintas a traducir. Posteriormente presenta una pantalla (pantalla 8) como la que se muestra a continuación. Revisemos la información que nos presenta. En el panel izquierdo pone un listado de todos los archivos a traducir así como por cuántas cadenas está compuesto cada archivo, cuántas han sido traducidas y, si está totalmente traducido, nos muestra una palomita verde.

El panel superior del lado derecho muestra todas las cadenas y su traducción, si es que existe, para el archivo que esté seleccionado en el panel izquierdo. Al igual que en el anterior en este panel una palomita verde significa "traducido".

En el panel de en medio de la columna de la derecha es donde debemos teclear la traducción correspondiente a cada cadena. Para hacer más sencillo este proceso, el programa nos ofrece en el panel inferior del lado derecho una lista de sugerencias de lo que podría ser la traducción. Esta lista la construye el sistema con la misma traducción que nosotros hemos venido haciendo, así que es muy posible que la traducción que nos ofrezca coincida con lo que necesitamos.

Pantalla 8 Herramienta de traducción: QtLinguist.

QT Linguist también ofrece varias combinaciones de teclas para hacer más rápido el movimiento al interior de la aplicación. Por ejemplo oprimiendo simultáneamente Ctrl-Enter el sistema acepta la traducción que hemos hecho y nos trae la siguiente cadena a traducir. Otra de las ventajas de QT Linguist es que, al momento que le pedimos que acepte una traducción, hace una validación de la puntuación de la cadena y sólo acepta la traducción si la puntuación que hemos usado en la traducción coincide con la original.

Pantalla 9 Página de traducciones de eZ Publish.

Ahora que ya hemos visto el proceso de traducción y el listado de traducciones disponibles (pantalla 9) hablemos sobre cómo construir soluciones utilizando eZ Publish, es decir, entremos en la segunda parte, la ampliación.

Introducción a la construcción de módulos en eZ Publish.

eZ Publish como marco de construcción (framework)

eZ Publish es, además de un SAC, un conjunto de herramientas para construir soluciones dinámicas para Internet. Algunas de las áreas donde se puede utilizar como una poderos a plataforma son: publicación en Internet, comercio electrónico, portales corporativos, intranets, extranets, sitios corporativos y portales. eZ Systems de Noruega tiene los derechos de autor sobre eZ Publish y lo liberó bajo dos esquemás de licencias distintos, GPL y eZ Publish professional license. Como se sabe, GPL es una licencia de tipo software libre. Por su parte, eZ Publish professional license es una licencia de tipo comercial que permite construir aplicaciones utilizando eZ Publish y después comercializarlas bajo un modelo de licencias cerrado o comercial.

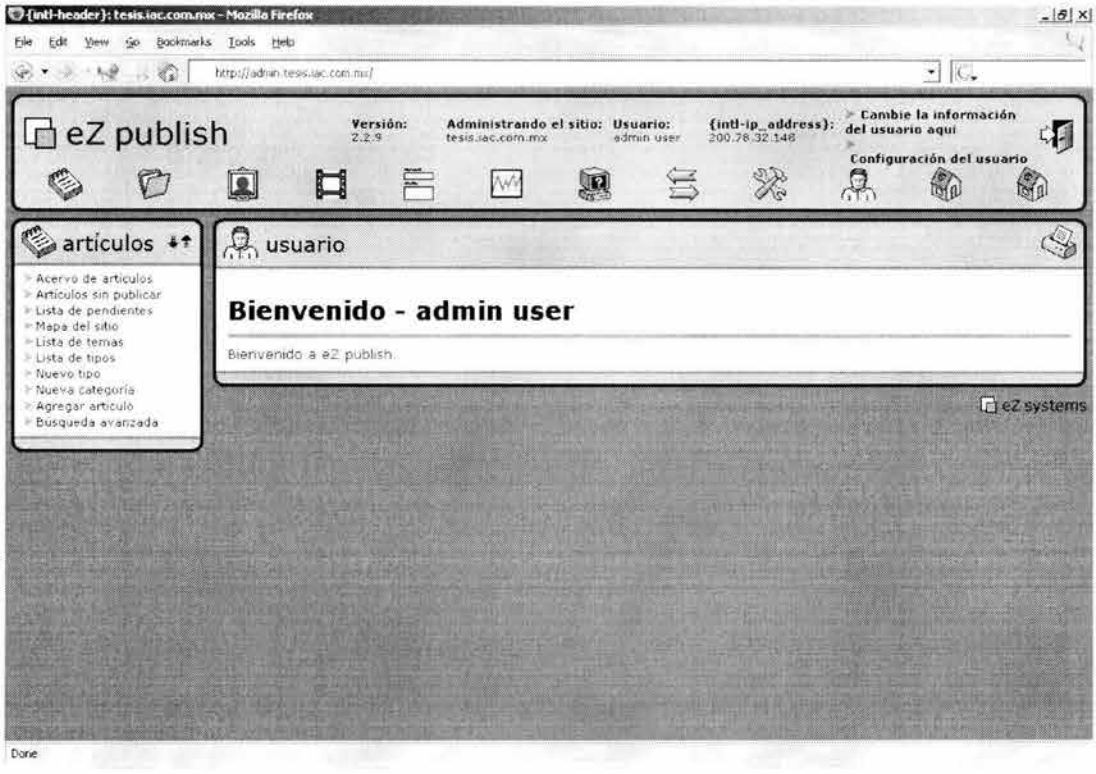
Sistema de manejo de contenido

Como se dijo en la parte de diseño de la solución, no vamos a programar un SAC completo sólo agregaremos dos módulos, especiales para el banco, y que por procesar la información en contraposición con simplemente mostrarla, no tenían cabida en el módulo de manejo de contenido.

Y como parte de la adecuación, un cambio importante que se le hizo fue en cuanto a su configuración: se deshabilitaron una gran cantidad de módulos debido a que no eran necesarios en el esquema inicial del trabajo. Esto quiere decir que en cualquier momento se pueden activar todos los que se requieran.

Se presenta a continuación un comparativo de los módulos normalmente activos (pantalla 10) y de los módulos activos en la configuración de BB (pantalla 11).

Pantalla 10 Módulos activos en una configuración normal.



Pantalla 11 Módulos activos en la configuración de BB.

Cada módulo se puede identificar como un ícono en la parte superior. A mayor número de íconos mayor número de módulos activos.

ezBancos

Descripción

Este módulo administra un catálogo de bancos. Basándonos en los resultados obtenidos en el diseño, construiremos este módulo de tal forma que satisfaga lo especificado.

Clase

La clase que implementa el modelo para este módulo es la siguiente (código 11):

```
<?php
//
// Created on: <15-Jun-2001 15:24:47 br>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
//

include_once( "classes/ezdb.php" );
include_once( "classes/ezdatetime.php" );
include_once( "eztasas/classes/eztasas.php" );

class eZBancos
{
    /*!
      Constructs a new eZBancos object
     */
    function eZBancos( $id=-1 )
    {
        if ( $id != -1 )
        {
            $this->ID = $id;
            $this->get( $this->ID );
        }
    }

    /*!
      Fetches the Text from the database.
    */
    function get( $id=-1 )
    {
```

```
        $db =& eZDB::globalDatabase();
        $ret = false;
        if ( $id != -1  )
        {
            $db->array_query( $text_array, "SELECT * FROM eZBancos WHERE ID='$id'" );

            if ( count( $text_array ) > 1 )
            {
                die( "Error: Text with the same ID was found in the database. This shouldn't
happen." );
            }
            else if ( count( $text_array ) == 1 )
            {
                $this->ID =& $text_array[0][$db->fieldName("ID")];
                $this->Text =& $text_array[0][$db->fieldName("Banco")];
                $this->Created =& $text_array[0][$db->fieldName("Created")];
                $ret = true;
            }
        }
        return $ret;
    }

    /*!
      Retrieves all Text fields from the database.
    */
    function &getAll()
    {
        $db =& eZDB::globalDatabase();

        $return_array = array();
        $url_array = array();

        $db->array_query( $url_array, "SELECT ID FROM eZBancos ORDER BY ID ASC"  );

        for ( $i=0; $i<count($url_array); $i++ )
        {
            $return_array[$i] = new eZBancos( $url_array[$i][$db->fieldName("ID")] );
        }

        return $return_array;
    }


    /*!
      Stores/updates the Text.
    */
    function store()
    {
        $db =& eZDB::globalDatabase();


        $text = $db->escapeString( $this->Text );
        $timeStamp =& eZDateTime::timeStamp( true );

        $db->begin();
        $db->lock( "eZBancos" );

        $nextID = $db->nextID( "eZBancos", "ID" );

        if ( !isset( $this->ID ) )
        {
            $ret = $db->query( "INSERT INTO eZBancos
                        ( ID,
                          Banco,
                          Created )
                        VALUES
                        ( '$nextID',
                          '$text',
                          '$timeStamp')
                        " );
```

```
                    $this->ID = $nextID;
                    $tasadb = new eztasas( );
                    $tasadb->setBanco( $nextID );
                    $tasadb->setTasa( "0.0" );
                    $tasadb->setPublicado( "0" );
                    $tasadb->store();
        }
        else
        {
            $ret = $db->query( "UPDATE eZBancos SET
                                Banco='$text'
                          WHERE ID='$this->ID'" );
        }
        $db->unlock();

        if ( $ret == false )
            $db->rollback();
        else
            $db->commit();

        return $ret;
    }


    /*!
      Deletes a Text from the database.
    */
    function delete( $id )
    {
        $db =& eZDB::globalDatabase();
        if ( is_numeric( $id ) )
        {
             $this->ID = $id;
        }

        $db->begin();
        $ret = $db->query( "DELETE FROM eZBancos WHERE ID='$this->ID'" );
               $tasadb = new eztasas( $id );
               $tasadb->delete( $id );

        if ( $ret == false )
            $db->rollback( );
        else
            $db->commit( );

        return $ret;
    }

    /*!
      Returns the object ID to the option. This is the unique ID stored in the database.
    */
    function id()
    {
       return $this->ID;
    }

    /*!
      Returns the Text From the database.
    */
    function text()
    {
        return $this->Text;
    }

    /*!
      Sets the text in the database.
    */
    function setText( $value )
    {
        $this->Text = $value;
```

```
    }

    var $ID;
    var $Text;
    var $Created;
}
?>
```

Código 11 La clase eZBancos.

Esta clase se encarga de almacenar y recuperar los datos de la base de datos. Tiene los siguientes atributos:

- ID
- Text
- Created

Y los siguientes métodos:

- *eZBancos* .- el constructor de la clase.
- *get*.- para obtener un banco de la base de datos.
- *getAll*.- para obtener todos los bancos que hay en la base de datos.
- *Store*.- para guardar el contenido de una instancia de un objeto de esta clase en la base de datos.
- *delete*.- para eliminar un registro de la base de datos.
- *id*.- para obtener el identificador de una instancia.
- Text.- para obtener el contenido del atributo Text de una instancia, el nombre del banco.
- setText.- para establecer el contenido del atributo Text de una instancia.

Como se puede ver, la clase implementa métodos de consulta y fijación (setters y getters) del valor para los atributos públicos, de creación, almacenamiento y recuperación de las instancias, dándoles persistencia.

La base de datos

El modelo de datos utilizado en este módulo es:

	Field	Type	Attributes	Null	Default	Extra	Action
☐	ID	int(11)		No	0		
☐	Banco	varchar(100)		Yes	*NULL*		
☐	Created	int(11)		Yes	*NULL*		

Check All / Uncheck All *With selected:*

Indexes : [Documentation]

Keyname	Type	Cardinality	Action	Field
PRIMARY	PRIMARY	11	Drop Edit	ID

Create an index on 1 columns Go

Space usage :

Type	Usage
Data	280 Bytes
Index	2,048 Bytes
Total	2,328 Bytes

Row Statistic :

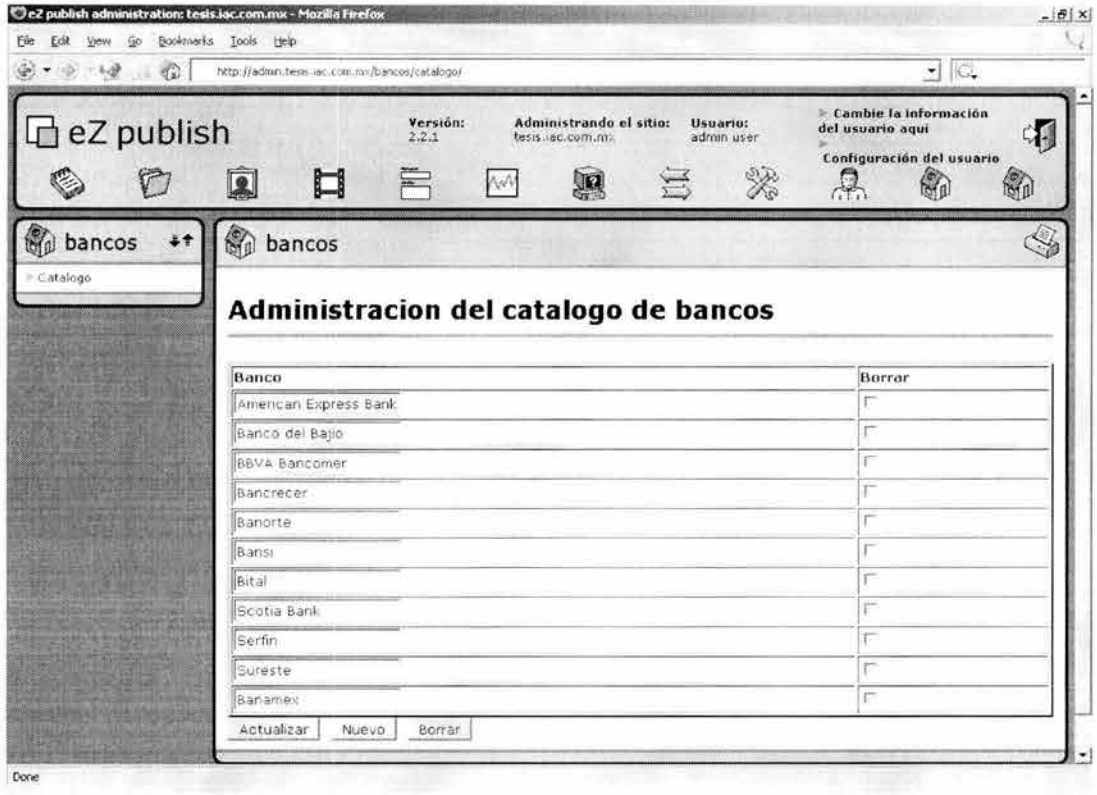
Statements	Value
Format	dynamic
Rows	11
Row length ø	25
Row size ø	212 Bytes
Creation	Mar 11, 2004 at 11:32 AM
Last update	Mar 11, 2004 at 11:32 AM

Y el contenido de la tabla, en este momento es:

←T→	ID	Banco	Created
	1	American Express Bank	1003537573
	4	BBVA Bancomer	1003543000
	3	Banco del Bajio	1003537609
	5	Bancrecer	1005937089
	6	Banorte	1005948126
	7	Bansi	1005948328
	8	Bital	1005948819
	9	Scotia Bank	1005948840
	10	Serfin	1005948854
	11	Sureste	1005948874
	12	Banamex	1005948928

Pantallas

Por su naturaleza este módulo sólo tiene interfase del usuario para el caso del administrador. La interfase es una sola pantalla (pantalla 12) y se muestra a continuación.



Pantalla 12 Módulo eZBancos, administración, administración de la relación de bancos.

Código

El controlador de este módulo (su datasupplier) es el siguiente (código 12):

```
<?php
//
// $Id: datasupplier.php,v 1.3 2001/07/19 12:48:35 jakobn Exp $
//
// Created on: <23-Oct-2000 17:53:46 bf>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
//

switch ( $url_array[2] )
{
    case "catalogo":
    {
```

```
        include( "ezbancos/admin/catálogo.php" );
    }
    break;

    default :
    {
        // go to default module page or show an error message
        print( "Error: your page request was not found" );
    }
}
?>
```

Código 12 El controlador del módulo eZBancos.

Como se puede ver, debido a que al interior de la estructura de control switch que está en la línea 28 y que termina en la línea 41 sólo hay un "case", este módulo de momento sólo tiene una operación "catálogo" y el código para atender todas las acciones que se necesitan está al interior del archivo ezbancos/admin/catálogo.php.

Veamos ahora la operación (código 13) para conocer el uso de la clase.

```
<?php
//
// $Id: catálogo.php,v 1.2 2001/07/19 12:48:35 jakobn Exp $
//
// Created on: <22-Jun-2001 13:24:18 br>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
//

// include the class files.

include_once( "classes/eztemplate.php" );
include_once( "ezbancos/classes/ezbancos.php" );

$ini =& INIFile::globalINI();
$Language = $ini->read_var( "ezbancosMain", "Language" );

$tpl = new eZTemplate( "ezbancos/admin/" . $ini->read_var( "eZBancosMain", "AdminTemplateDir" ),
                       "ezbancos/admin/" . "intl", $Language, "catálogo.php" );
$tpl->setAllStrings();

// Check which button is pressed.

if ( isset( $New ) )
{
    $banco = new ezbancos( );
    $banco->setText( "" );
```

```
    $banco->store();
    updateValues( $IDArray, $TextArray );
}

if ( isset( $Update ) )
{
    updateValues( $IDArray, $TextArray );
}

if ( isset( $Delete ) )
{
    foreach( $DeleteArrayID as $id )
    {
        ezbancos::delete( $id );
    }
}

// get all fields from the database.

$textfield = new ezbancos( );
$textfieldArray =& $textfield->getAll();

$tpl->set_file( "catálogo_tpl", "catálogo.tpl" );
$tpl->set_block( "catálogo_tpl", "row_tpl", "row" );
$tpl->set_var( "row", "" );

for( $i=0; $i< count($textfieldArray); $i++ )
{
    $tpl->set_var( "row_text", $textfieldArray[$i]->Text() );
    $tpl->set_var( "row_id", $textfieldArray[$i]->id() );
    $tpl->parse( "row", "row_tpl", true );
}

$tpl->pparse( "output", "catálogo_tpl" );

/*!
  Update all fields in the database.
*/
function updateValues( $idArray, $textArray )
{
    $i=0;
    if ( count( $idArray ) > 0 )
    foreach( $idArray as $id )
    {
        $banco = new ezbancos( );
        if ( $banco->get( $id ) )
        {
            $banco->setText( $textArray[ $i ] );
            $banco->store();
        }
        $i++;
    }
}
?>
```

Código 13 La operación catálogo del módulo eZBancos.

Para entender mejor la operación veamos primero la plantilla (código 14).

Plantilla

```
<form method="post">
<h1>{intl-title}</h1>
<hr noshade="noshade" size="4" />
<br />
<table width="100%" border="2">
<tr>
```

```
<th>{intl-bank}</th>
<th>{intl-delete}</th>
</tr>
<!-- BEGIN row_tpl -->
<tr>
<td>
<input type="text" name="TextArray[]" value="{row_text}" />
<input type="hidden" name="IDArray[]" value="{row_id}" />
</td>
<td>
<input type="checkbox" name="DeleteArrayID[]" value="{row_id}" />
</td>
</tr>
<!-- END row_tpl -->
</table>
<input type="submit" name="Update" value="{intl-update}" /> 
<input type="submit" name="New" value="{intl-new}" /> 
<input type="submit" name="Delete" value="{intl-delete}" />
</form>
```

Código 14 La plantilla para la operación catálogo del módulo eZBancos.

Como nos lo revela la línea 1 lo que tenemos es una forma autocontenida. Gracias a esta característica es que en las líneas 42, 50 y 55 del código de la operación estamos verificando cuál de los botones que ofrece la forma fue presionado. Los nombres de los botones se establecen en las líneas 22, 23 y 25 de la plantilla.

Analicemos entonces cada una de las tres acciones posibles, actualizar, nuevo y borrar.

En el caso de Nuevo las líneas 42 a 48 se encargan de atenderlo. Lo primero es crear una nueva instancia de la clase bancos (44), posteriormente asignarle un valor provisional a su atributo público (45), y, finalmente, guardar esa instancia en la base de datos (46) para que al invocar a la función updateValues (47) el despliegue de la relación de los bancos nos incluya un renglón más. Éste estará en blanco, y podremos capturar el nuevo banco y, posteriormente, darla orden de actualizar para llevar ese valor ya como definitivo y no como temporal a la base de datos.

El caso de la actualización es mucho más sencillo, basta invocar la función updateValues (52) y eso llevará todos los valores que estén en ese momento en pantalla a la base de datos.

Finalmente, con borrar entramos en un ciclo, líneas 57 a 60, eliminando todos aquellos registros que hayan sido marcados para su eliminación (59) a través de la invocación directa del método "delete" de la clase.

Analicemos ahora la integración del procesamiento con la plantilla. Las líneas 36 y 37 establecen como se llama la plantilla que vamos a utilizar. La 38 realiza la traducción de la plantilla, 69 relaciona el archivo de la plantilla con un nombre en el motor de reemplazo, la 70 define que dentro de la plantilla hay un bloque, de nombre row_tpl y con elementos tipo row. La 71 inicializa un elemento de tipo row con una cadena vacía.

En el ciclo de las líneas 73 a 78 vamos a tomar los objetos que recuperamos de la base de datos mediante la línea 67 y los vamos a introducir en la plantilla en las líneas 75 y 76, para, en la 77, agregar uno nuevo a los elementos tipo row que ya habíamos integrado a la plantilla. La línea 80 finaliza la ejecución del motor de plantillas y envía el resultado para que a través de frame.php se le muestre al usuario.

Archivo de localización

```
[strings]
module_name=bancos
update=Actualizar
delete=Borrar
bank=Banco
new=Nuevo
title=Administracion del catálogo de bancos
```

Código 15 El archivo de internacionalización para la operación catálogo del módulo eZBancos.

Éste es un archivo (código 15) muy simple, contiene dos elementos por renglón, del lado izquierdo el nombre de la etiqueta en la plantilla, que en la plantilla encontraremos precedido de intl, y del derecho el valor por el que se debe reemplazar.

ezTasas

Descripción

Recordemos que la misión de ezTasas es, aprovechando el catálogo de bancos, permitir la captura de la tasa correspondiente a cada banco y seleccionar aquéllos contra los que se va a efectuar la comparación. Además, capturará la fecha con base en la cual se está haciendo la comparación de la información.

Clase

Siguiendo el modelo de programación que se usa en eZ Publish, la clase (código 16) se va a encargar de la persistencia de los objetos.

```
<?php
//
// Created on: <15-Jun-2001 15:24:47 br>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
//
```

```
include_once( "classes/ezdb.php" );
include_once( "classes/ezdatetime.php" );

class eZTasas
{
    /*!
      Constructs a new eZTasas object
     */
    function eZTasas( $id=-1 )
    {
        if ( $id != -1 )
        {
            $this->ID = $id;
            $this->get( $this->ID );
        }
    }

    /*!
      Fetches the Text.
    */
    function get( $id=-1 )
    {
        $db =& eZDB::globalDatabase();
        $ret = false;
        if ( $id != -1  )
        {
            $db->array_query( $text_array, "SELECT * FROM eZTasas WHERE ID='$id'" );

            if ( count( $text_array ) > 1 )
            {
                die( "Error: Text with the same ID was found. This shouldn't happen." );
            }
            else if ( count( $text_array ) == 1 )
            {
                $this->ID =& $text_array[0][$db->fieldName("ID")];
                $this->Banco =& $text_array[0][$db->fieldName("Banco")];
                $this->Tasa =& $text_array[0][$db->fieldName("Tasa")];
                $this->Publicado =& $text_array[0][$db->fieldName("Publicado")];
                $this->Created =& $text_array[0][$db->fieldName("Created")];
                $ret = true;
            }
        }
        return $ret;
    }

    /*!
      Retrieves all Text fields.
    */
    function &getAll()
    {
        $db =& eZDB::globalDatabase();

        $return_array = array();
        $url_array = array();

        $db->array_query( $url_array, "SELECT ID FROM eZTasas ORDER BY ID ASC"  );

        for ( $i=0; $i<count($url_array); $i++ )
        {
            $return_array[$i] = new eZTasas( $url_array[$i][$db->fieldName("ID")] );
        }

        return $return_array;
    }


    /*!
      Retrieves fecha de vigencia.
    */
    function &getVigencia()
```

```
{
    $db =& eZDB::globalDatabase();

    $return_array = array();
    $url_array = array();

    $db->array_query( $url_array, "SELECT Fecha FROM eZTasas_Vigencia" );

    for ( $i=0; $i<count($url_array); $i++ )
    {
        $return_array[$i] = new eZTasas( $url_array[$i][$db->fieldName("Fecha")] );
    }

    return $return_array;
}


/*!
  Stores/updates the Text.
*/
function store()
{
    $db =& eZDB::globalDatabase();


    $tasa = $db->escapeString( $this->Tasa );
    $banco = $db->escapeString( $this->Banco );
    $publicado = $db->escapeString( $this->Publicado );
    $timeStamp =& eZDateTime::timeStamp( true );

    $db->begin();
    $db->lock( "eZTasas" );

    $nextID = $db->nextID( "eZTasas", "ID" );

    if ( !isset( $this->ID ) )
    {
        $ret = $db->query( "INSERT INTO eZTasas
                    ( ID,
                      Banco,
                      Tasa,
                      Publicado,
                      Created )
                    VALUES
                    ( '$nextID',
                      '$banco',
                             '$tasa',
                             '$publicado',
                      '$timeStamp')
                    " );
                   $this->ID = $nextID;
    }
    else
    {
        $ret = $db->query( "UPDATE eZTasas SET
                             Tasa='$tasa', Publicado='$publicado'
                      WHERE ID='$this->ID'" );
    }
    $db->unlock();

    if ( $ret == false )
        $db->rollback();
    else
        $db->commit();

    return $ret;
}


/*!
```

```
  Stores/updates the Text.
*/
function storeVigencia()
{
    $db =& eZDB::globalDatabase();


    $vigencia = $db->escapeString( $this->Vigencia );

    $db->begin();
    $db->lock( "eZTasas_Vigencia" );

    $ret = $db->query( "UPDATE eZTasas_Vigencia SET Fecha='$vigencia'" );

    $db->unlock();

    if ( $ret == false )
        $db->rollback();
    else
        $db->commit();

    return $ret;
}


/*!
  Deletes a record.
*/
function delete( $id )
{
    $db =& eZDB::globalDatabase();
    if ( is_numeric( $id ) )
    {
         $this->ID = $id;
    }

    $db->begin();
    $ret = $db->query( "DELETE FROM eZTasas WHERE ID='$this->ID'" );

    if ( $ret == false )
        $db->rollback( );
    else
        $db->commit( );

    return $ret;
}

/*!
  Returns the object ID to the option. This is the unique ID stored.
*/
function id()
{
   return $this->ID;
}

/*!
  Returns the tasa.
*/
function tasa()
{
    return $this->Tasa;
}

/*!
  Sets the tasa.
*/
function setTasa( $value )
{
    $this->Tasa = $value;
}
```

```
    /*!
      Returns the value of publicado.
    */
    function publicado()
    {
        return $this->Publicado;
    }

    /*!
      Sets the value of publicado.
    */
    function setPublicado( $value )
    {
        $this->Publicado = $value;
    }


    /*!
      Returns the value of banco.
    */
    function banco()
    {
        return $this->Banco;
    }

    /*!
      Sets the value of banco.
    */
    function setBanco( $value )
    {
        $this->Banco = $value;
    }

    /*!
      Returns the value of vigencia.
    */
    function vigencia()
    {
        return $this->Vigencia;
    }

    /*!
      Sets the value of banco.
    */
    function setVigencia( $value )
    {
        $this->Vigencia = $value;
    }

    var $ID;
    var $Banco;
    var $Tasa;
    var $Publicado;
    var $Vigencia;
    var $Created;
}
?>
```

Código 16 La clase eZTasas.

La base de datos

El modelo para este módulo es:

La tabla para almacenar las tasas.

	Field	Type	Attributes	Null	Default	Extra	Action
☐	ID	int(11)		No	0		
☐	Banco	int(11)		Yes	*NULL*		
☐	Tasa	float(6,2)		Yes	*NULL*		
☐	Publicado	int(1)		Yes	*NULL*		
☐	Created	int(11)		Yes	*NULL*		

Check All / Uncheck All *With selected:*

Indexes : [Documentation]

Keyname	Type	Cardinality	Action	Field
PRIMARY	PRIMARY	11	Drop Edit	ID

Create an index on 1 columns Go

Space usage :

Type	Usage
Data	231 Bytes
Index	2,048 Bytes
Total	2,279 Bytes

Row Statistic :

Statements	Value
Format	fixed
Rows	11
Row length ø	21
Row size ø	207 Bytes
Creation	Mar 11, 2004 at 11:34 AM
Last update	Mar 11, 2004 at 11:34 AM

La tabla para almacenar la vigencia de las tasas.

	Field	Type	Attributes	Null	Default	Extra	Action
☐	Fecha	varchar(50)		Yes	*NULL*		

Check All / Uncheck All *With selected:*

Indexes : [Documentation]

No index defined!

Create an index on 1 columns Go

Space usage :

Type	Usage
Data	32 Bytes
Index	1,024 Bytes
Total	1,056 Bytes

Row Statistic :

Statements	Value
Format	dynamic
Rows	1
Row length ø	32
Row size ø	1,056 Bytes
Creation	Mar 11, 2004 at 11:34 AM
Last update	Mar 11, 2004 at 11:34 AM

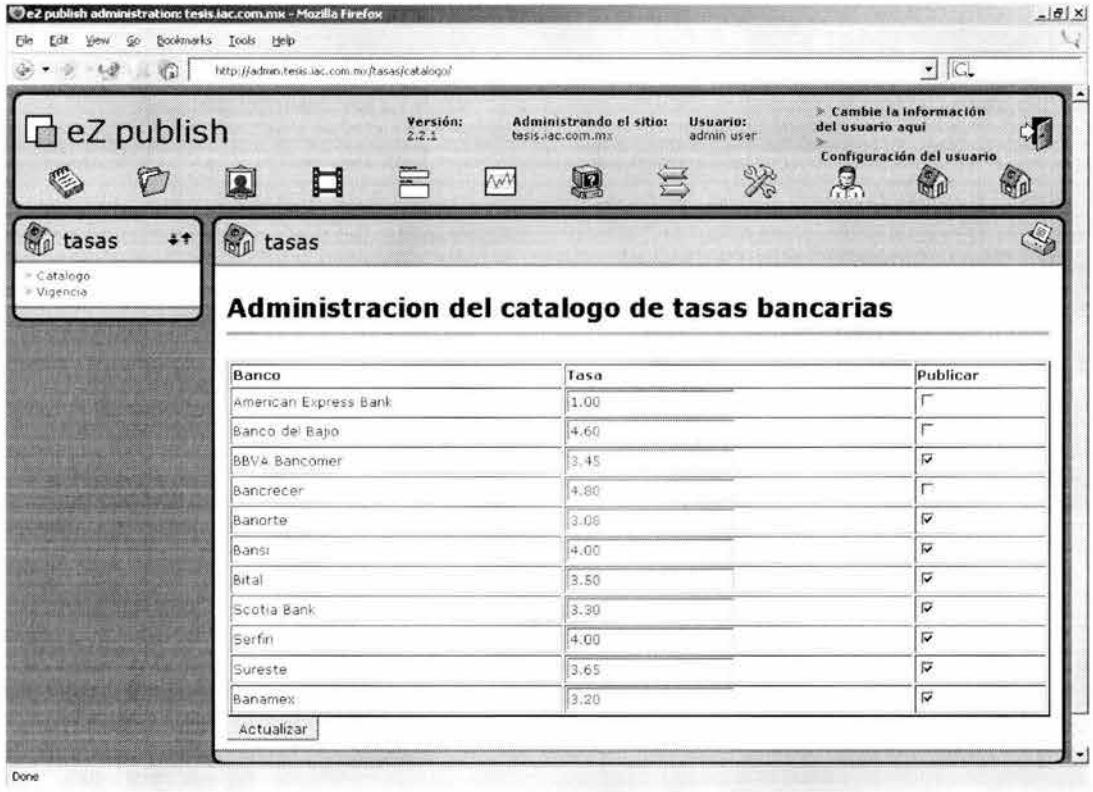
Y el contenido de la tabla de tasas es:

←T→	ID	Banco	Tasa	Publicado	Created
	1	1	1.00	0	1003537573
	4	4	3.45	1	1003543000
	3	3	4.60	0	1003537609
	5	5	4.80	0	1005937089
	6	6	3.08	1	1005948126
	7	7	4.00	1	1005948328
	8	8	3.50	1	1005948819
	9	9	3.30	1	1005948840
	10	10	4.00	1	1005948854
	11	11	3.65	1	1005948874
	12	12	3.20	1	1005948928

Pantallas

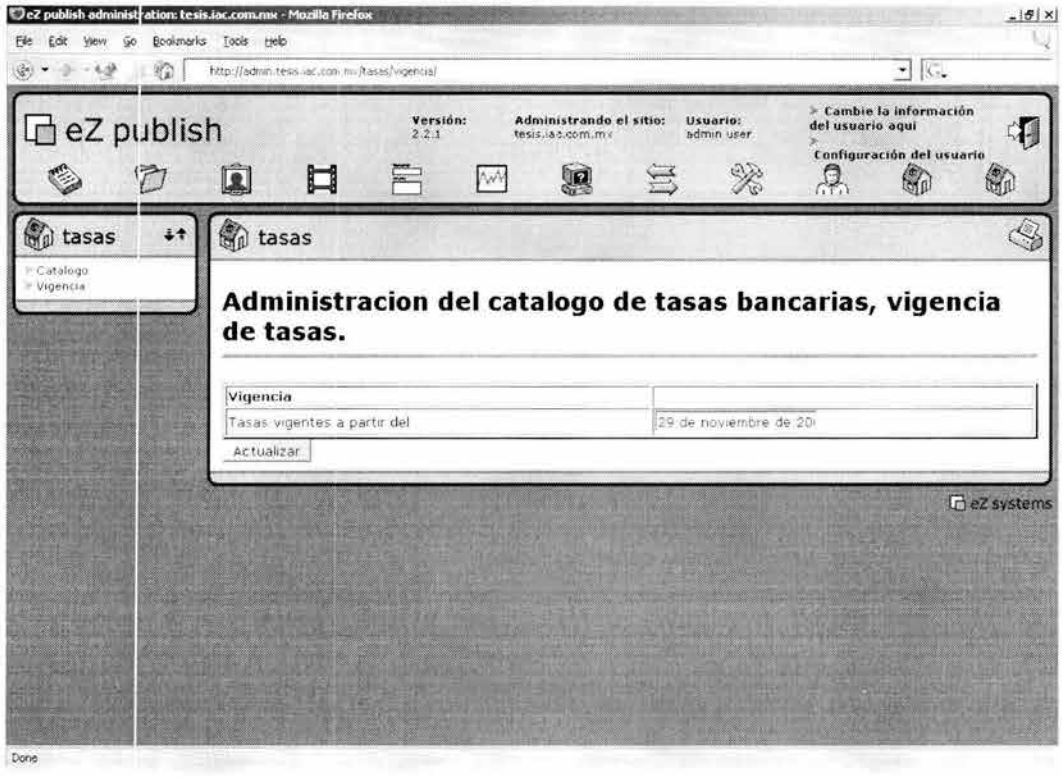
A diferencia del módulo anterior, este módulo sí tiene una interfase de usuario, precisamente aquélla donde se presenta el resultado de la comparación.

Pero veamos primero las dos correspondientes a la administración. La primera de ellas (pantalla 13) es donde se dan de alta las tasas y se seleccionan aquéllas a comparar.



Pantalla 13 Módulo ezTasas, administración, alta tasas.

La segunda (pantalla 14), mucho más simple es donde se establece la fecha de vigencia de las tasas.

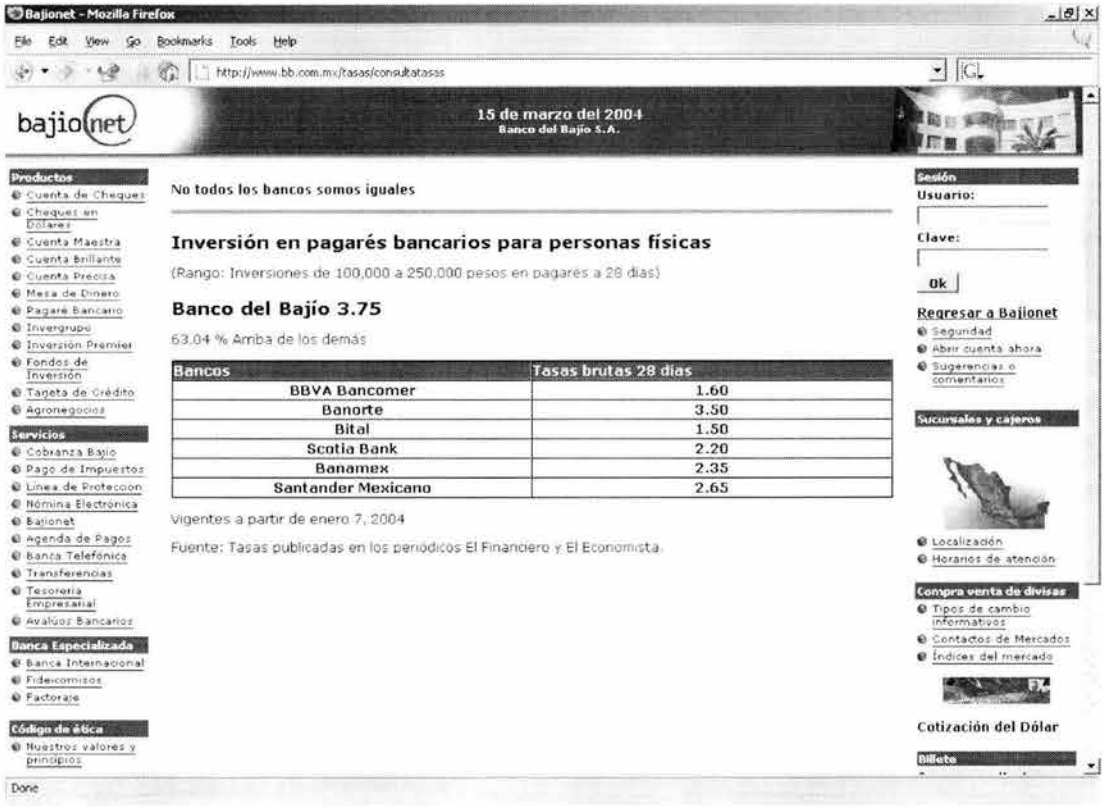


Pantalla 14 Módulo ezTasas, administración, vigencia de las tasas.

Ahora viene la pantalla interesante.

Esta pantalla (pantalla 15) tiene por un lado las especificaciones de qué tasas de inversión se están comparando. En este caso inversiones de 100,000 a 250,000 en pagarés a 28 días.

Luego presenta la tasa que está ofreciendo BB y, a continuación, el porcentaje en el que es mayor la tasa de BB en comparación con el promedio de las tasas de la competencia.



Pantalla 15 Módulo ezTasas, usuario, comparativo de tasas.

Código

Por ser, probablemente, lo más interesante veamos el código de la operación (código 17) que construye la pantalla (pantalla 15) anterior.

```
<?php
//
// $Id: consultatasas.php,v 1.2 2001/07/19 12:48:35 smb Exp $
//
// Created on: <22-Jun-2001 13:12:22 br>
//
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
```

```
//

// include the class files.

include_once( "classes/ezhttptool.php" );
include_once( "classes/INIFile.php" );
include_once( "classes/eztemplate.php" );
include_once( "classes/ezlocale.php" );
include_once( "eztasas/classes/eztasas.php" );
include_once( "ezbancos/classes/ezbancos.php" );

$ini =& INIFile::globalINI();

$Language = $ini->read_var( "eZTasasMain", "Language" );
$TemplateDir = $ini->read_var( "eZTasasMain", "TemplateDir" );

$tpl = new eZTemplate( "eztasas/user/" . $ini->read_var( "eZTasasMain", "TemplateDir" ),
                       "eztasas/user/" . "intl", $Language, "consultatasas.php" );
$tpl->setAllStrings();

// get all fields from the database.
$bancostextfield = new ezbancos( );
$bancostextfieldArray =& $bancostextfield->getAll();

// get all fields from the database.
$field = new eztasas( );
$fieldArray =& $field->getAll();
$vigenciaArray =& $field->getVigencia();

// parse the template.

$tpl->set_file( "consultatasas_tpl", "consultatasas.tpl" );
$tpl->set_block( "consultatasas_tpl", "row_tpl", "row" );
$tpl->set_block( "consultatasas_tpl", "vigencia_tpl", "vigencia" );
$tpl->set_block( "consultatasas_tpl", "diferencia_tpl", "diferencia" );
$tpl->set_var( "row", "" );
$tpl->set_var( "vigencia", "" );
$tpl->set_var( "diferencia", "" );

$j = 0;
for( $i=0; $i < count($bancostextfieldArray); $i++ )
{
        if ( $fieldArray[$i]->Publicado( ) ) {
                $j++;
                if ( $bancostextfieldArray[$i]->id() != 3 ) {
                        $tpl->set_var( "row_banco", $bancostextfieldArray[$i]->Text() );
                        $tpl->set_var( "row_tasa", $fieldArray[$i]->Tasa() );
                        $tpl->parse( "row", "row_tpl", true );
                        $tasa_acumulada += $fieldArray[$i]->Tasa();
                }
        }
}

$tpl->set_var( "vigen", $vigenciaArray[0]->id() );
$tpl->parse( "vigencia", "vigencia_tpl" );


if ( $i != 0 ) {
        $tasa_promedio = $tasa_acumulada / $j;
        $banco_bajio = $bancostextfieldArray[1]->Text(); // Ojo los arreglos empiezan en 0 no en 1
        $tasa_banco_bajio = $fieldArray[1]->Tasa();
        $dif = $tasa_banco_bajio - $tasa_promedio;
        $res = $dif / $tasa_promedio;
        $tpl->set_var( "banco", $banco_bajio );
        $tpl->set_var( "tasa", $tasa_banco_bajio );
        $tpl->set_var( "diferencial", sprintf("%01.2f %%", $res * 100) );
        $tpl->parse( "diferencia", "diferencia_tpl" );

}
```

```
$tpl->pparse( "output", "consultatasas_tpl" );
?>
```

Código 17 La operación consultatasas del módulo eZTasas.

Sistema aplicativo o transaccional

ezTransaccion

Empecemos por mencionar que este módulo no tiene interfase en el lado del administrador. En las conclusiones veremos algo más sobre esto. Y tampoco tiene base de datos, dado que no almacena ninguna información. Si alguna información pudiera necesitar ésta es la de la sesión, pero de ella se encarga el soporte a sesiones que nos proporciona eZ Publish y dicha clase sí hace uso de la base de datos.

Dado que vamos a implementar al menos una parte del protocolo http hablemos un poco de él con la idea de familiarizarnos más con los detalles.

En Internet, las comunicaciones tiene lugar sobre conexiones de tipo TCP/IP. Esto hace que http esté naturalmente orientado a este tipo de conexiones y mapea las estructuras de las solicitudes y las respuestas en unidades de la capa de transporte. Sin embargo, no es imposible implementar http sobre algún otro tipo de conexiones.

http es un protocolo con el peso y la velocidad necesarias en un sistema de información distribuido y con capacidad de hipermedios. Es genérico, sin estados, orientado a objetos, se puede utilizar para muchas tareas, por ejemplo, servidores de nombres y sistemas distribuidos orientados a objetos, simplemente expandiendo los métodos base de su especificación. Una característica de http es la negociación de la representación del los datos, lo que le da la flexibilidad para ser utilizado en nuevos sistemas que integran representaciones que no existían antes.

Un ciclo de comunicaciones http es como se muestra a continuación:

HTTP

Conexión
: El establecimiento de una conexión de un cliente con un servidor – si se utilice TCP/IP el puerto que se esperaría se utilizará es el 80, pero se pueden utilizar otros puertos y esto se pueden especificar en el URL.

Solicitud
: El envío, por parte del cliente, de un mensaje de solicitud al servidor.

Respuesta
: El envío, por parte del servidor, de una respuesta al cliente.

Cierre
: La terminación de la conexión por ambas partes.

Ahora bien, pasemos de este nivel de detalle a una visión más abstracta.

Descripción

Cuando un cliente hace una solicitud de transacción, el camino que dicha solicitud recorre es el siguiente (diagrama 11). En varias ocasiones se establecen conexiones tipo http y puede haber una o más conexiones que impliquen protocolos distintos.

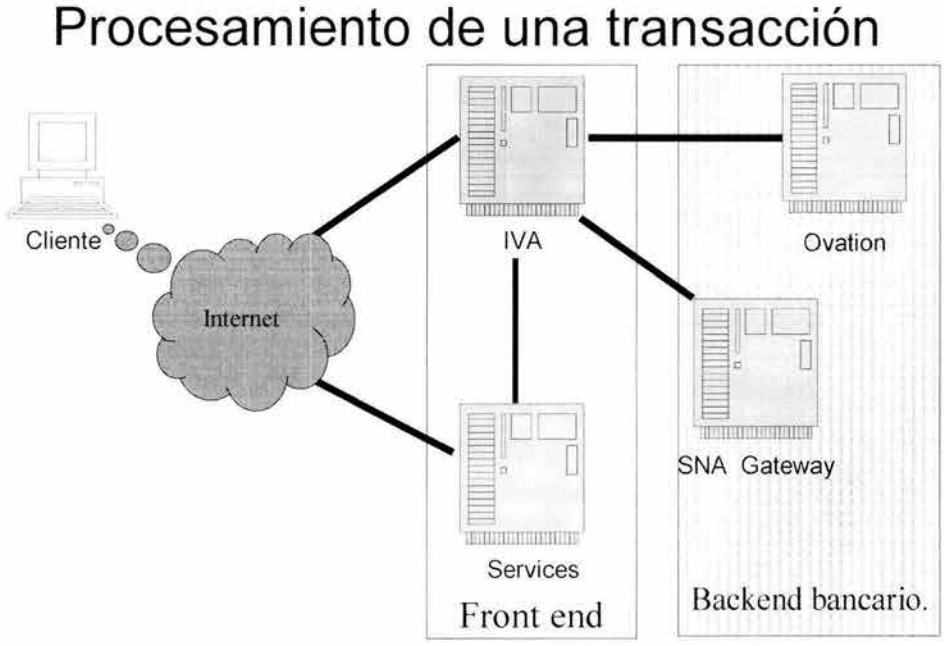


Diagrama 11 Funcionamiento general de una transacción.

Ahora que ya hemos visto el flujo de una transacción a nivel protocolos, veamos cómo es su atención en el nivel aplicativo (diagrama 12).

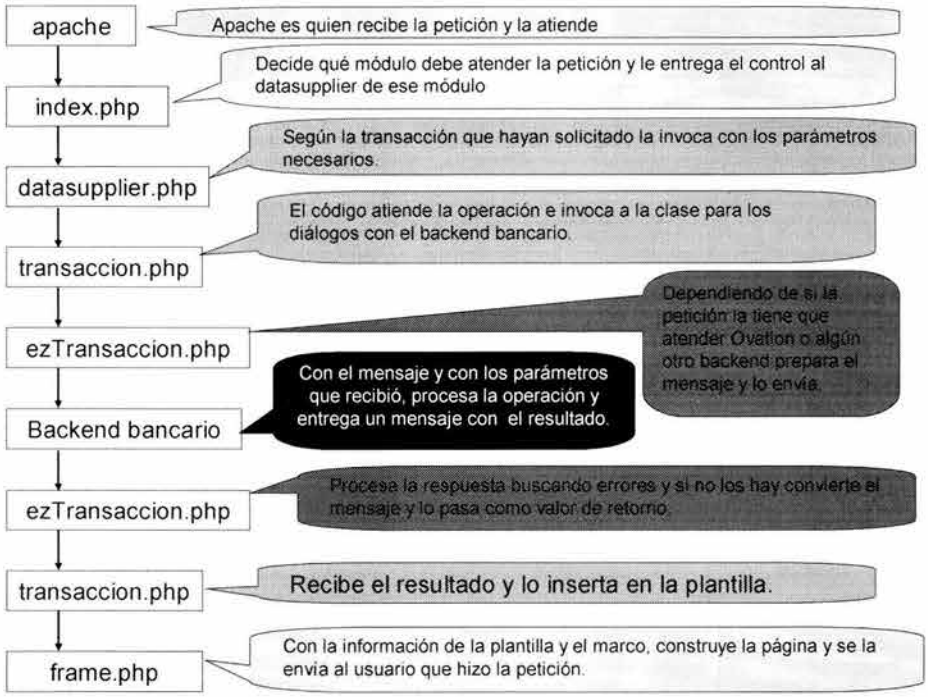


Diagrama 12 Procesamiento de una transacción.

Código

Por las razones de confidencialidad que ya hemos mencionado veremos ahora sólo algunos fragmentos de las partes más importantes de este módulo. A continuación, un fragmento de su controlador (datasupplier) (código 18).

```
switch ( $url_array[2] )
{
 case "saldos" :
 {
  include( "eztransaccion/user/saldos.php" );
 }
 break;

 case "estadosdecuenta" :
 {
  include( "eztransaccion/user/estadosdecuenta.php" );
 }
 break;

 case "movimientos" :
 {
  include( "eztransaccion/user/movimientos.php" );
 }
 break;

 case "busquedacheques" :
 {
  include( "eztransaccion/user/busquedacheques.php" );
 }
 break;
```

```
case "clave" :
{
 include( "eztransaccion/user/clave.php" );
}
break;
```

Código 18 Programa datasupplier.php para el módulo ezTransaccion (fragmento).

Aquí se puede apreciar perfectamente como es ese mapeo del que hablábamos en el diseño; una transacción será igual a una operación.

De la clase eZTransaccion tomemos uno de los métodos más relevantes, aquél que implementa el método POST del protocolo http, con una característica importante: reconoce y atiende algunas desviaciones del backend Ovation con respecto a la especificación formal.

```
function PostToHost($host, $path, $data_to_send, $cookie_to_send, &$usr_to_receive,
&$cookie_to_receive, &$priv_to_receive, &$transaccion_buffer) {

  $fp = fsockopen($host, 80, &$errno, &$errstr);
  if($fp==FALSE) {
    $transaccion_buffer = "Error ".$errno.": ".$errstr;
    return -1;
  }
  fputs($fp, "POST $path HTTP/1.0\n");
  if(IsSet($cookie_to_send)) {
    fputs($fp, "Cookie: ".$cookie_to_send."\n");
  }
  fputs($fp, "Content-type: application/x-www-form-urlencoded\n");
  fputs($fp, "Content-length: ".strlen($data_to_send)."\n");
  fputs($fp, "\n");
  fputs($fp, $data_to_send."\n");
  $header=1;
  $ret_code=0;
  magic_quotes_runtime(0);
  while(!feof($fp)) {
    $str = trim(fgets($fp, 512));
    if($header!=0 && ereg("^[\t ]*$", $str)) {
     $header = 0;
     continue;
    }
    if($header!=0 && ereg("^[\t ]*<", $str)) { // ATENCION: este bloque existe porque el GW no es
capaz de enviar http de verdad (no separa con nl)
     $header = 0;
    }
    if(ereg("^Set-Cookie: ([^;]+)", $str, $regs)) {
     $cookie_to_receive = $regs[1];
    }
    if(eregi("\"CadPriv\" VALUE=\"(.*)\"", $str, $regs)) {
     $priv_to_receive = $regs[1];
    }
    if(eregi("\"CustID\" VALUE=\"(.*)\"", $str, $regs)) {
     $usr_to_receive = $regs[1];
    }
    if(ereg("digo: \((.*)\)", $str, $regs)) { // ATENCION que pasa con () etc..
     $ret_code = $regs[1];
    }
    if(ereg("\"mailto:(.*)\"", $str, $regs)) {
     $mailto = trim($regs[1]);
    }
    if(!$header) {
     $transaccion_buffer = $transaccion_buffer . $str;
    }
  }
  fclose($fp);
```

```
  return $ret_code;
 }
```

Código 19 Método PostToHost de la clase ezTransaccion, del módulo ezTransaccion.

En este método (código 19) estamos también atrapando las respuestas de error, no sólo transaccionales, sino aquéllas que se deben a un problema de comunicaciones, ya sea a nivel de red, ya sea a nivel de la aplicación del backend.

Plantilla

```
<h1>{intl-transaccion_operacion}</h1>
<hr noshade="noshade" size="4" />
<p>{transaccion_buffer}</p>
```

Código 20 Plantilla para una transacción.

Otro código (código 21) interesante dentro de este módulo es el del menú, puesto que construye la lista de las transacciones disponibles para el usuario de forma dinámica y en función de los privilegios que se encuentran almacenados en la sesión del usuario que ya fue autenticado.

```
<?php
//
// $Id: userbox.php,v 1.0 2001/11/01 11:22:30 smb Exp $
//
// Created on: <1-Nov-2001 17:37:53 smb>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2001 Internet de Alta Calidad, S.A. de C.V.
// All rights reserved.
// Programó: Sebastián Mantilla Beniers

include_once( "classes/INIFile.php" );
include_once( "classes/eztemplate.php" );
include_once( "classes/ezlog.php" );
include_once( "classes/ezhttptool.php" );

$ini =& INIFile::globalINI();
$Language = $ini->read_var( "eZTransaccionMain", "Language" );

include_once( "ezuserbb/classes/ezuser.php" );
include_once( "ezuserbb/classes/ezusergroup.php" );
include_once( "ezuserbb/classes/ezmodule.php" );
include_once( "ezuserbb/classes/ezpermission.php" );
include_once( "ezsession/classes/ezsession.php" );

$session =& eZSession::globalSession();

if( !$session->fetch() )
 $session->store();

$user =& eZUserBB::currentUser();

// DebugBreak();

if ( !$user )
{
 eZHTTPTool::header("Location: http://www.bb.com.mx/article/articleview/86/1/7");
```

```
 exit();
}
else
{
 $session =& eZSession::globalSession();

 if ( !$session->fetch() )
 {
  $session->store();
 }

 $session->refresh();

 $priv = "00000000000000000000000000000000";
 $priv = $session->variable( "r_priv" );

 $t = new eZTemplate( "eztransaccion/user/" . $ini->read_var( "eZTransaccionMain", "TemplateDir"
),
        "eztransaccion/user/intl", $Language, "userbox.php" );
 $t->setAllStrings();

 $t->set_file( "userbox_tpl", "userbox.tpl" );
 $t->set_block( "userbox_tpl", "menu_tpl", "menu" );
 $t->set_block( "menu_tpl", "header_tpl", "header" );
 $t->set_block( "menu_tpl", "row_tpl", "row" );

 $t->set_var( "row", "" );
 $t->set_var( "header_menu_bloque", "" );
 $t->set_var( "menu", "" );

 $t->set_var( "header_menu_bloque", "Operaciones" );
 $t->parse( "header", "header_tpl" ); // Atencion, no lleva TRUE porque es elemento unico de su
tipo en el bloque

 if(substr($priv, 0, 1)=="1") { // pro
  $t->set_var( "menu_liga", "/transaccion/saldos/" );
  $t->set_var( "menu_nombre_liga", "Saldos" );
  $t->parse( "row", "row_tpl", true );
 }

 if(substr($priv, 2, 1)=="1") { // hst
  $t->set_var( "menu_liga", "/transaccion/movimientos/" );
  $t->set_var( "menu_nombre_liga", "Movimientos" );
  $t->parse( "row", "row_tpl", true );
 }
.
.
.
.
.
 $t->parse( "menu", "menu_tpl", true );

 $t->set_var( "row", "" );
 $t->set_var( "header_menu_bloque", "" );

 $t->set_var( "header_menu_bloque", "Servicios" );
 $t->parse( "header", "header_tpl" );

 $t->set_var( "menu_liga", "/transaccion/clave/" );
 $t->set_var( "menu_nombre_liga", "Cambio de clave" );
 $t->parse( "row", "row_tpl", true );

 $t->set_var( "menu_liga", "/userbb/login/logout/" );
 $t->set_var( "menu_nombre_liga", "Salir" );
 $t->parse( "row", "row_tpl", true );

 $t->parse( "menu", "menu_tpl", true );

 $t->pparse( "output", "userbox_tpl" );
```

```
}

?>
```

Código 21 Del menú de las transacciones (fragmento).

Este código sólo se aprecia bien si vemos la plantilla (código 22) que se encarga de su atención.

```
<!-- BEGIN menu_tpl -->
<table width="100%" border="0">
 <!-- BEGIN header_tpl -->
<tr>
       <td colspan="2" bgcolor="#5A419c"><font color="#ffffff" size="1" face="verdana, arial,
helvetica, sans-serif"><b>{header_menu_bloque}</b></font></td>
</tr>
 <!-- END header_tpl -->
<!-- BEGIN row_tpl -->
<tr>
 <td    width="1%"    valign="top"><img    src="/sitedesign/bajionet/images/dot.gif"    width="10"
height="12"><br /></td>
 <td   width="99%"><a   href="{menu_liga}"><font   face="Verdana,   Arial,   Helvetica,   sans-serif"
size="1">{menu_nombre_liga}</font></a></td>
</tr>
<!-- END row_tpl -->
</table>
<!-- END menu_tpl -->
```

Código 22 De la plantilla del menú.

Con eso hemos hecho ya una revisión tan detallada como nos lo permiten las circunstancias.

Veamos a continuación el módulo validador de usuarios.

ezUserBB

Descripción

Por tratarse del módulo sobre el que mayores restricciones de confidencialidad existen, aquí prácticamente no vamos a ver código. Sin embargo, repasemos qué es lo que estamos construyendo.

De la forma que se encuentra en el menú del lado derecho de la página, mediante un POST, utilizando https haremos una solicitud de operación de login del módulo eZUser. Este módulo internamente construirá un mensaje con los datos del usuario, hará una solicitud de autenticación al backend bancario y en caso de obtener una respuesta positiva, creará una sesión para el usuario y la pondrá a disposición para el resto de los módulos. En caso de que la autenticación no sea positiva, enviará un mensaje al usuario informándole del problema. En ambos casos se deberá guardar un registro en la bitácora.

Para la programación utilizaremos como base el código de eZUser, dado que ya tiene todo el soporte para las sesiones y los reintentos, y cambiaremos únicamente la función que comparaba los datos proporcionados por el cliente con los almacenados en la base de datos de eZ Publish,

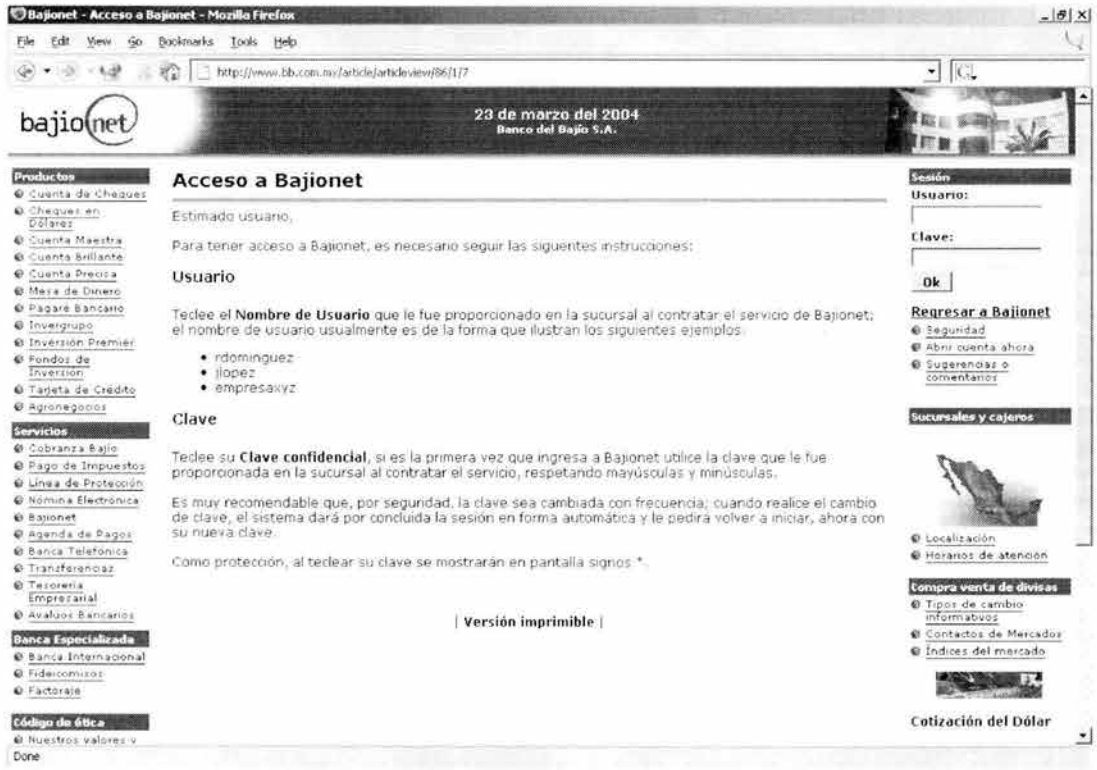
para que ahora, en lugar de hacerlo así, realice una transacción proporcionándole al backend bancario dichos datos y que reciba y procese la respuesta correspondiente.

Pantallas

Ésta es la página principal del banco (pantalla 16). Como se puede ver, a la derecha existe una forma para que el usuario capture sus datos y solicite el inicio de una sesión.

Pantalla 16 Módulos ezUserBB, usuario, pantalla para establecer sesión.

Ayuda que recibe el cliente (pantalla 17) en el caso de que durante su intento por establecer una sesión cometa algún error, a diferencia de si comete un error con los datos que proporciona como su usuario y con su clave.



Pantalla 17 Módulos ezUserBB, usuario, que aparece cuando se intenta acceder a las transacciones sin haber establecido previamente una sesión.

Ahora bien, si el problema es que se equivocó con los datos de usuario y en la clave que proporcionó, el mensaje de error es (pantalla 18):

Pantalla 18 Módulos ezUserBB, usuario, cuando los datos de usuario o clave no son válidos.

Código

A continuación dos fragmentos de código, el primero es el de la operación que realiza la transacción con el backend bancario y crea la sesión (código 23). El segundo es un fragmento del código de alguna operación que implementa una transacción bancaria y que aprovecha la sesión que ya había sido creada para llevar al cabo sus diálogos con el backend (código 24).

```
function validateUser( $login, $password )
{
 $db =& eZDB::globalDatabase();
 $ret = false;
 // DebugBreak();

 $session =& eZSession::globalSession();

 if ( !$session->fetch() )
 {
   $session->store();
 }

 $session->refresh();

 $uelogin = urlencode($login);
 $uepassword = urlencode($password);
 $received_usr = "";
```

```
  $received_qki = "";
  $received_priv = "";
  $transaccion_buffer = "";
  $tr = new eZTransaccion( );
  $ini =& $GLOBALS["GlobalSiteIni"];
  $backend = $ini->read_var( "eZTransaccionMain", "Backend" );
  $ret_code                =                $tr->PostToHost($backend,              "/IBnkIIS.dll",
"Trxn=ver&CustID=".$uelogin."&Passwd=".$uepassword,      "",      $received_usr,      $received_qki,
$received_priv, $transaccion_buffer); // Login
  if($ret_code == 0 ) {
    $transaccion_buffer = "";
    $ret = new eZUserBB( "3" );
    $ret->setUsr( $received_usr );
    $session->setVariable( "r_usr", $received_usr );
    $ret->setQki( $received_qki );
    $session->setVariable( "r_qki", $received_qki );
    $ret->setPriv( $received_priv );
    $session->setVariable( "r_priv", $received_priv );
    $GLOBALS["eZCurrentUserObject"] =& $ret;
  }

  return $ret;
 }
```

Código 23 Fragmento del código de validación de usuarios con el servidor bancario.

Al interior de una operación recuperamos los datos de sesión, para poder establecer un diálogo con el backend bancario para un usuario que ya haya sido previamente autenticado.

```
if ( $user )
{
    $t   =   new   eZTemplate(   "eztransaccion/user/"   .   $ini->read_var(   "eZTransaccionMain",
"TemplateDir" ),
                          "eztransaccion/user/intl/", $Language, "saldos.php" );

    $t->setAllStrings();

    $t->set_file( array(
        "saldos_tpl" => "saldos.tpl"
        ) );


    $session =& eZSession::globalSession();

    if ( !$session->fetch() )
    {
        $session->store();
    }

    $session->refresh();

    $tr = new eZTransaccion( );
    $usr = $session->variable( "r_usr" );
    $qki = $session->variable( "r_qki" );
    $priv = $session->variable( "r_priv" );
```

Código 24 Manejo de las variables de sesión.

Seguridad

El proceso de construcción de la seguridad del sistema (diagrama 13) son dos pasos, selección de la herramienta o herramientas a utilizar y configuración de cada una de ellas. Por ello vamos a

ver en el desarrollo de esta sección del trabajo el mismo esquema, la descripción de la herramienta y su configuración.

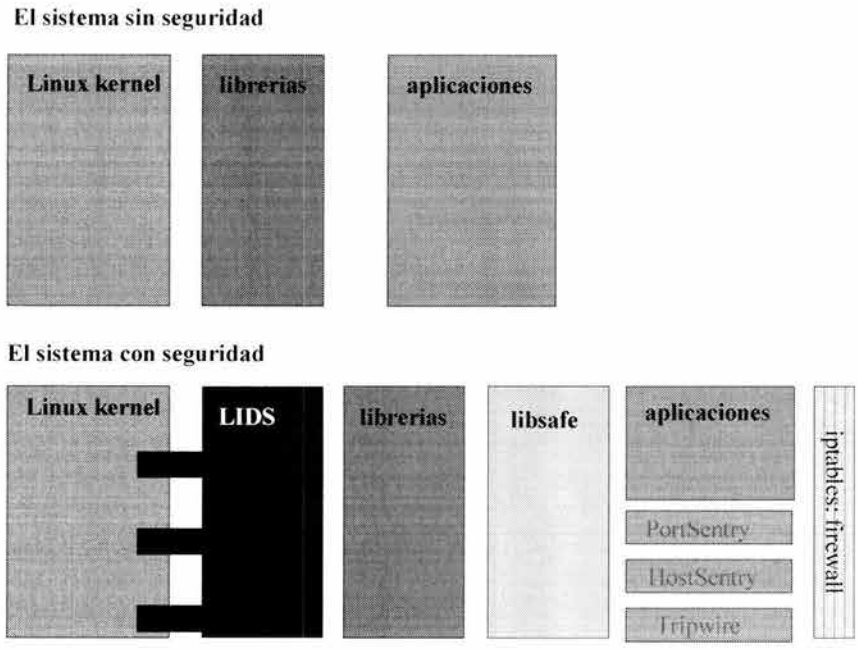


Diagrama 13 La seguridad en la solución.

Sistema Operativo

Como veíamos en el diseño, a nivel sistema operativo nuestra mayor preocupación es el hecho de que la cuenta de administración, *root*, es todopoderosa, por ello, para proteger el sistema operativo, utilizaremos LIDS que nos ayudará a controlar al todopoderoso administrador.

LIDS

Descripción

LIDS nace como un proyecto para subsanar las siguientes deficiencias de los sistemas que utilizan el kernel de Linux:

- Los sistemas de archivos están desprotegidos.
- Los procesos están desprotegidos.
- La administración del sistema está desprotegida.
- El administrador puede abusar de sus privilegios de administración.
- El modelo de control de acceso no es suficiente.

LIDS es hoy en día un conjunto de cambios al kernel (diagrama 14) y unas herramientas de administración que le permiten a un administrador tener un kernel que resuelve la problemática planteada.

¿Cuáles son sus características?

- Protección de archivos. Nadie, ni siquiera el administrador, puede modificar archivos protegidos por LIDS. Los archivos se pueden esconder.
- Protección de procesos. Nadie, ni siquiera el administrador, puede modificar o matar procesos protegidos por LIDS. Los procesos se pueden esconder.
- Control de acceso granular, incluyendo listas de control de acceso.
- Capacidades de uso y extensión para el sistema completo.
- Detección de escaneo de puertos directamente en el kernel.
- Alertas de seguridad directamente desde el kernel.

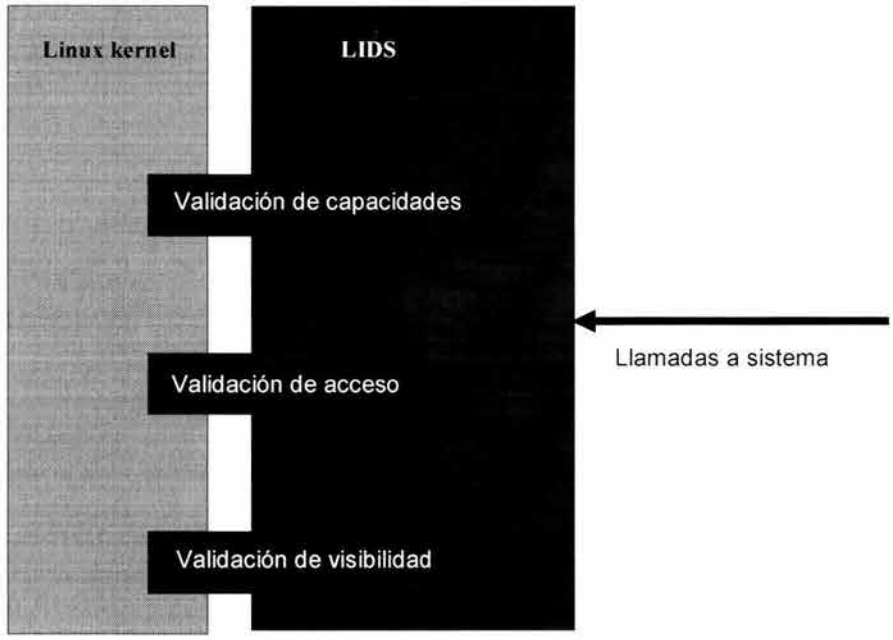


Diagrama 14 Kernel + LIDS.

Configuración

```
#!/bin/bash
# Version 0.86
```

```
##############################################################################
#
# LIDS CONFIGURATION FILE - kerne 2.4.19 - lids 1.1.2rc4
#
#  If you have comment/questions/suggestions about this script, please
#  drop me a line at:
#
#  sebas@iac.com.mx
#
#  I welcome suggestions!
#
#  I know some of my setting are a little relaxed, like for courier-imap.
#  This is because I'm not too familiar with it and haven't had the time
#  to research what the minimum necessary requirements are.
#
##############################################################################

##############################################################################
#
# NOTES:
#
#  /lib/modules/<kernel version>/modules.dep
#      This file doesn't have to be created at each boot.  You only need
#      to recreate it if you add/change modules.
#
#  /etc/mtab
#      Modify startup scripts to use the `-n' option when mounting.  Remove
#      /etc/mtab and create a symbolic link from /etc/mtab to /proc/mounts
#
#  /etc/HOSTNAME
#      Modify rc.sysinit so that the hostname isn't echoed into the file.
#
##############################################################################

rm -f /etc/mtab
ln -s /proc/mounts /etc/mtab

# Flush old rules
#
/sbin/lidsconf -Z

# Hide this file!
#
echo ""
echo "You should hide this stuff!"

/sbin/lidsconf -A -o /root/lids          -j DENY
/sbin/lidsconf -A -o /etc/lids           -j DENY


# If you grant privileges to crond based on time restrictions, it is highly recommended that you
hide your crontabs from
# everyone (including root), and only allow crond to read them. Otherwise, someone could figure
out what time of day
# they should try and exploit something by looking at your crontabs. Remember to protect the
system crontabs as well as
# the user crontabs.
# /sbin/lidsconf -A -s /bin/login -o /etc/shadow -t 0900-1800 -j READONLY

echo ""
echo "Protect crontab"
/sbin/lidsconf -A -o /var/spool/cron             -j DENY
/sbin/lidsconf -A -o /etc/crontab                -j DENY
/sbin/lidsconf -A -o /etc/cron.hourly            -j DENY
/sbin/lidsconf -A -o /etc/cron.daily             -j DENY
/sbin/lidsconf -A -o /etc/cron.weekly            -j DENY
/sbin/lidsconf -A -o /etc/cron.monthly           -j DENY
/sbin/lidsconf -A -o /etc/cron.d                 -j DENY

# Protect System Binaries
```

```
#

echo ""
echo "Protect System Binaries"
/sbin/lidsconf -A -o /sbin                          -j READONLY
/sbin/lidsconf -A -o /bin                           -j READONLY
/sbin/lidsconf -A -o /usr/bin                       -j READONLY
/sbin/lidsconf -A -o /usr/sbin                      -j READONLY

echo ""
echo "Adjusting system logs"
/sbin/lidsconf -A -o /var/log                       -j READONLY
/sbin/lidsconf -A -s /sbin/syslogd -o /var/log      -j WRITE

# Protect all of /usr and /usr/local
# (This assumes /usr/local is on a separate file system).
#

echo ""
echo "Protect all of /usr and /usr/local"
/sbin/lidsconf -A -o /usr                           -j READONLY
/sbin/lidsconf -A -o /usr/local                     -j READONLY

# Protect the System Libraries
#(/usr/lib is protected above since /usr/lib generally isn't
# on a separate file system than /usr)
#

echo ""
echo "Protect the System Libraries"
/sbin/lidsconf -A -o /lib                           -j READONLY
/sbin/lidsconf -A -o /usr/lib                       -j READONLY

# Protect System Configuration files
#

echo ""
echo "Protect System Configuration files"
/sbin/lidsconf -A -o /etc                                 -j READONLY
/sbin/lidsconf -A -o /usr/local/etc                       -j READONLY
/sbin/lidsconf -A -o /etc/shadow                          -j DENY
/sbin/lidsconf -A -o /etc/rc0.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc1.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc2.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc3.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc4.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc5.d                           -j READONLY
/sbin/lidsconf -A -o /etc/rc6.d                           -j READONLY
/sbin/lidsconf -A -o /etc/init.d                          -j READONLY
/sbin/lidsconf -A -o /etc/rc                              -j READONLY
/sbin/lidsconf -A -o /etc/rc.local                        -j READONLY
/sbin/lidsconf -A -o /etc/rc.sysinit                      -j READONLY
/sbin/lidsconf -A -o /boot/grub/grub.conf                 -j DENY
/sbin/lidsconf -A -s /sbin/init -o /etc/ioctl.save        -j WRITE
/sbin/lidsconf -A -o /etc/mtab                            -j IGNORE
# /sbin/lidsconf -A -s /sbin/init -o /etc/initrunlvl      -j WRITE
# /sbin/lidsconf -A -o /etc/mtab                          -j READONLY
# /sbin/lidsconf -A -s /bin/umount -o /etc/mtab           -j WRITE
# /sbin/lidsconf -A -o /etc/mtab                          -j READONLY
# /sbin/lidsconf -A -s /bin/mount -o /etc/mtab            -j WRITE
# /sbin/lidsconf -A -s /bin/umount -o /etc/mtab           -j WRITE
/sbin/lidsconf -A -s /bin/bash -o /etc/ld.so.cache        -j READONLY
/sbin/lidsconf -A -s /sbin/depmod -o /lib/modules/2.4.19-tolkien1smp/modules.dep        -j WRITE

# Enable system authentication
#

echo ""
echo "Enable system authentication"
/sbin/lidsconf -A -s /bin/login -o /etc/shadow              -j READONLY
```

```
/sbin/lidsconf -A -s /bin/su -o /etc/shadow              -j READONLY
/sbin/lidsconf -A -s /bin/su -o CAP_SETUID               -j GRANT
/sbin/lidsconf -A -s /bin/su -o CAP_SETGID               -j GRANT

# Protect the boot partition
#
echo ""
echo "Protect the boot partition"
/sbin/lidsconf -A -o /boot                               -j READONLY

# Protect root's home dir, but allow bash history
#
echo ""
echo "Protect root's home dir, but allow bash history"
/sbin/lidsconf -A -o /root                               -j READONLY
/sbin/lidsconf -A -s /bin/bash -o /root/.bash_history    -j WRITE

# Protect system logs
#
echo ""
echo "Protect system logs"
/sbin/lidsconf -A -o /var                                                -j READONLY
/sbin/lidsconf -A -o /var/log                                            -j APPEND
/sbin/lidsconf -A -o /var/run                                            -j WRITE
/sbin/lidsconf -A -o /var/lock/subsys                                    -j WRITE
/sbin/lidsconf -A -s /bin/login -o /var/log/wtmp                         -j WRITE
/sbin/lidsconf -A -s /bin/login -o /var/log/btmp                         -j WRITE
/sbin/lidsconf -A -s /bin/login -o /var/log/lastlog                      -j WRITE
/sbin/lidsconf -A -s /sbin/mingetty -o /var/log/wtmp                     -j WRITE
/sbin/lidsconf -A -s /sbin/mingetty -o /var/log/lastlog                  -j WRITE
/sbin/lidsconf -A -s /sbin/init -o /var/log/wtmp                         -j WRITE
/sbin/lidsconf -A -s /sbin/init -o /var/log/lastlog                      -j WRITE
/sbin/lidsconf -A -s /sbin/halt -o /var/log/wtmp                         -j WRITE
/sbin/lidsconf -A -s /sbin/halt -o /var/log/lastlog                      -j WRITE
/sbin/lidsconf -A -s /bin/dmesg -o /var/log/dmesg                        -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/wtmp -i 1          -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/lastlog -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.0 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.1 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.2 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.3 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.4 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.5 -i 1       -j WRITE
/sbin/lidsconf -A -s /etc/rc.d/rc.sysinit -o /var/log/ksyms.6 -i 1       -j WRITE

# Startup
#
echo ""
echo "Startup"
/sbin/lidsconf -A -s /sbin/hwclock -o /etc/adjtime       -j WRITE


# Shutdown
#
echo ""
echo "Shutdown"
/sbin/lidsconf -A -s /sbin/init -o CAP_KILL              -j GRANT

# Give the following init script the proper privileges to kill processes and
# unmount the file systems.  However, anyone who can execute these scripts
# by themselves can effectively kill your processes.  It's better than
# the alternative, however.
#
# Any ideas on how to get around this are welcome!
#

/sbin/lidsconf -A -s /etc/rc.d/init.d/halt -o CAP_KILL -i 1          -j GRANT
/sbin/lidsconf -A -s /etc/rc.d/init.d/halt -o CAP_NET_ADMIN -i 1     -j GRANT
/sbin/lidsconf -A -s /etc/rc.d/init.d/halt -o CAP_SYS_ADMIN -i 1     -j GRANT
```

```
# Other
#
/sbin/lidsconf -A -s /sbin/update -o CAP_SYS_ADMIN       -j GRANT

# As of version 0.10.1 for 2.2.19 and version 1.0.11 for 2.4.6, you can limit the privileged
ports that a program can bind
# to. When granting CAP_NET_BIND_SERVICE to a program, specify the port or ports that the program
is allowed to
# bind to after the capability. Or, if you also need to bind to port 443 for SSL:
echo ""
echo "Apache"
/sbin/lidsconf -A -s /usr/sbin/httpd -o CAP_NET_BIND_SERVICE 80-80,443-443  -j GRANT
/sbin/lidsconf -A -s /usr/sbin/httpd -o CAP_SETUID                          -j GRANT
/sbin/lidsconf -A -s /usr/sbin/httpd -o CAP_SETGID                          -j GRANT

# Config files
/sbin/lidsconf -A -o /etc/httpd                                  -j DENY
/sbin/lidsconf -A -s /usr/sbin/httpd -o /etc/httpd               -j READONLY

# Server Root
/sbin/lidsconf -A -o /var/www                                   -j DENY
/sbin/lidsconf -A -o /var/cache                                 -j DENY
/sbin/lidsconf -A -s /usr/sbin/httpd -o /etc/httpd/conf/httpd.conf -j READONLY
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/cache              -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www                -j READONLY
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/classes/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/error.log -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezaddress/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezarticle/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezarticle/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezbancos/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezcontact/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezfilemanager/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezfilemanager/files -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezform/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezimagecatalogue/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezimagecatalogue/catalogue -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezimagecatalogue/catalogue/variations
-j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezmediacatalogue/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezmediacatalogue/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezmediacatalogue/catalogue -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezpoll/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezpoll/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezsitemanager/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezstats/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezsysinfo/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/eztasas/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/eztransaccion/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/eztransaccion/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezlink/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezurltranslator/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezuser/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/ezuserbb/admin/cache -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/log/sna.log -j WRITE
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/www/html/bajio/log/usuarios.log -j WRITE

# Log Files
/sbin/lidsconf -A -o /var/log/httpd                                  -j DENY
/sbin/lidsconf -A -s /usr/sbin/httpd -o /var/log/httpd               -j WRITE

echo ""
echo "OpenSSH"
/sbin/lidsconf -A -s /etc/init.d/sshd -o /var/log/wtmp               -j WRITE -i -1
/sbin/lidsconf -A -s /etc/init.d/sshd -o /var/empty/sshd             -j WRITE -i -1
/sbin/lidsconf -A -s /etc/init.d/sshd -o /var/log/lastlog            -j WRITE -i -1
/sbin/lidsconf -A -o /etc/ssh/                                       -j READONLY
/sbin/lidsconf -A -s /usr/sbin/sshd -o /etc/shadow                   -j READONLY
/sbin/lidsconf -A -s /usr/sbin/sshd -o /etc/ssh/                     -j READONLY
/sbin/lidsconf -A -o /var/log/wtmp                                   -j READONLY
```

```
/sbin/lidsconf -A -s /usr/sbin/sshd -o /var/log/wtmp                    -j WRITE
/sbin/lidsconf -A -s /usr/sbin/sshd -o /var/empty/sshd                  -j WRITE
/sbin/lidsconf -A -s /usr/sbin/sshd -o /var/log/lastlog                 -j WRITE
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_SETUID                       -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_SETGID                       -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_FOWNER                       -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_CHOWN                        -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_DAC_OVERRIDE                 -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_SYS_CHROOT                   -j GRANT
/sbin/lidsconf -A -s /usr/sbin/sshd -o CAP_NET_BIND_SERVICE 22          -j GRANT

echo ""
echo "MC"
/sbin/lidsconf -A -s /usr/bin/mc -o /root                                       -j WRITE
/sbin/lidsconf -A -s /usr/bin/mc -o /root/.mc                                   -j WRITE -i -1

echo ""
echo "MySQL"
/sbin/lidsconf -A -s /etc/logrotate.d/mysqld -o /var/log                        -j WRITE
# /etc/rc.d/init.d/mysqld
# /usr/bin/mysqladmin
/sbin/lidsconf -A -s /usr/bin/safe_mysqld -o /var/lib/mysql                     -j WRITE
/sbin/lidsconf -A -s /usr/bin/safe_mysqld -o /var/run/mysqld                    -j WRITE
/sbin/lidsconf -A -s /usr/bin/safe_mysqld -o /var/log/mysqld.log                -j WRITE
/sbin/lidsconf -A -s /usr/libexec/mysqld -o /var/lib/mysql                      -j WRITE
/sbin/lidsconf -A -s /usr/libexec/mysqld -o /var/run/mysqld                     -j WRITE
/sbin/lidsconf -A -s /usr/libexec/mysqld -o /var/log/mysqld.log                 -j WRITE
/sbin/lidsconf -A -s /etc/init.d/mysqld -o /var/log/mysqld.log                  -j WRITE -i -1
/sbin/lidsconf -A -s /etc/init.d/mysqld -o /var/lib/mysqld                      -j WRITE -i -1
/sbin/lidsconf -A -s /bin/touch -o /var/log/mysqld.log                          -j WRITE
/sbin/lidsconf -A -s /bin/touch -o /var/lib/mysqld                              -j WRITE
/sbin/lidsconf -A -s /bin/chmod -o /var/log/mysqld.log                          -j WRITE
/sbin/lidsconf -A -s /bin/chmod -o /var/lib/mysqld                              -j WRITE
/sbin/lidsconf -A -s /bin/rm -o /var/lib/mysql/mysql.sock                       -j WRITE

echo ""
echo "Sendmail y Procmail"
# Sendmail LIDS rules (using infinite inheritance for the sendmail
# children and delivery agents to work properly, but a lower inheritance
# like 2 or 3 would probably work as well.)

# Lock down /etc/mail if it's not already done elseware
/sbin/lidsconf -A -o /etc/mail                                                  -j READONLY
/sbin/lidsconf -A -o /usr/sbin/sendmail.sendmail                                -j READONLY
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/shadow                   -j READONLY
-i -1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/passwd                   -j READONLY
-i -1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/mail                     -j READONLY
-i -1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/mail/statistics          -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/aliases                  -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /etc/aliases.db               -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o CAP_SETUID                    -j GRANT -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o CAP_SETGID                    -j GRANT -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o CAP_SYS_ADMIN                 -j GRANT -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o CAP_NET_BIND_SERVICE 25-25    -j GRANT -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o CAP_KILL                      -j GRANT -i
-1
# Depending on how you have the log files secured
# (The maillog will normally get rotated out and this
# rule will stop working when that happens unless you
# stop the log rotation.)
```

```
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/log/maillog                    -j APPEND -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/lock/subsys                    -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/run                            -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/spool/mail                     -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/spool/mqueue                   -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/sbin/sendmail.sendmail -o /var/spool/clientmqueue             -j WRITE -i
-1
/sbin/lidsconf -A -s /bin/mail -o /var/spool/mqueue                                     -j WRITE -i
-1
/sbin/lidsconf -A -s /usr/bin/procmail -o /var/spool/mail                  -j WRITE -i -1

echo ""
echo "General commands"
/sbin/lidsconf            -A            -s            /bin/touch            -o            /var/lock
-j WRITE
/sbin/lidsconf            -A            -s            /bin/touch            -o            /var/run
-j WRITE
/sbin/lidsconf          -A          -s          /bin/chmod          -o          /var/lib/random-seed
-j WRITE
/sbin/lidsconf           -A           -s           /etc/rc.d/rc.sysinit           -o           /etc
-j WRITE
/sbin/lidsconf          -A          -s          /etc/rc.d/rc.sysinit          -o          /var/run
-j WRITE
/sbin/lidsconf          -A          -s          /etc/rc.d/rc.sysinit          -o          /var/lock
-j WRITE
/sbin/lidsconf         -A         -s         /etc/rc.d/rc.sysinit         -o         /var/lib/rpm
-j WRITE
/sbin/lidsconf             -A             -s             /bin/rm             -o             /var/run
-j WRITE
/sbin/lidsconf             -A             -s             /bin/rm             -o             /var/lock
-j WRITE
/sbin/lidsconf            -A            -s            /bin/rm            -o            /var/lib/rpm
-j WRITE
/sbin/lidsconf          -A          -s          /usr/sbin/logrotate          -o          /var/log
-j WRITE
/sbin/lidsconf         -A         -s         /usr/sbin/makewhatis         -o         /var/cache/man
-j WRITE
/sbin/lidsconf           -A           -s           /usr/sbin/tmpwatch           -o           /var
-j WRITE
/sbin/lidsconf      -A      -s      /etc/log.d/scripts/logwatch.pl      -o      /var/spool/mqueue
-j WRITE
/sbin/lidsconf        -A        -s        /etc/log.d/scripts/logwatch.pl        -o        /var/tmp
-j WRITE
/sbin/lidsconf       -A       -s       /etc/log.d/scripts/logwatch.pl       -o       /etc/cron.daily
-j WRITE
/sbin/lidsconf          -A          -s          /usr/lib/rpm/rpmq          -o          /var/lib/rpm
-j WRITE

echo ""
echo "Webmin"
/sbin/lidsconf       -A       -s       /usr/bin/perl       -o       CAP_NET_BIND_SERVICE       81-81
-j GRANT
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/miniserv.pl    -o    CAP_NET_BIND_SERVICE    81-81
-j GRANT
#         /sbin/lidsconf         -A         -s         /usr/sbin/httpd         -o         CAP_SETUID
-j GRANT
#         /sbin/lidsconf         -A         -s         /usr/sbin/httpd         -o         CAP_SETGID
-j GRANT
# Config files
/sbin/lidsconf                        -A                        -o                        /etc/webmin
-j DENY
/sbin/lidsconf               -A               -o               /usr/libexec/webmin/sysstats/graphs
-j WRITE
/sbin/lidsconf           -A           -s           /usr/bin/perl           -o           /etc/webmin
-j WRITE
/sbin/lidsconf       -A       -s       /usr/libexec/webmin/miniserv.pl       -o       /etc/webmin
```

```
-j WRITE
/sbin/lidsconf          -A          -s          /usr/bin/rrdtool          -o          /etc/webmin
-j WRITE
/sbin/lidsconf          -A          -s          /usr/bin/perl          -o          /var/webmin
-j WRITE
/sbin/lidsconf       -A       -s       /usr/libexec/webmin/miniserv.pl       -o       /var/webmin
-j WRITE
/sbin/lidsconf         -A         -s         /usr/bin/perl         -o         /usr/libexec/webmin
-j WRITE
/sbin/lidsconf      -A      -s      /usr/libexec/webmin/miniserv.pl      -o      /usr/libexec/webmin
-j WRITE
/sbin/lidsconf        -A        -s        /usr/bin/rrdtool        -o        /usr/libexec/webmin
-j WRITE
/sbin/lidsconf -A -s /usr/libexec/webmin/sysstats/modules/cpu-0.9.7/cpu.sh -o /usr/libexec/webmin
-j WRITE
/sbin/lidsconf -A -s /usr/libexec/webmin/sysstats/modules/cpu-0.9.7/cpu.pl -o /usr/libexec/webmin
-j WRITE
/sbin/lidsconf     -A     -s     /usr/libexec/webmin/sysstats/modules/cpu-0.9.7/cpu-lib.pl     -o
/usr/libexec/webmin                  -j WRITE
/sbin/lidsconf     -A     -s     /usr/libexec/webmin/sysstats/modules/disk-0.8.6/disk.sh     -o
/usr/libexec/webmin                  -j WRITE
/sbin/lidsconf     -A     -s     /usr/libexec/webmin/sysstats/modules/disk-0.8.6/disk-lib.pl     -o
/usr/libexec/webmin                  -j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modules/filesopen-0.4.1/filesopen.sh    -o
/usr/libexec/webmin          -j WRITE
/sbin/lidsconf  -A  -s  /usr/libexec/webmin/sysstats/modules/filesopen-0.4.1/filesopen-lib.pl  -o
/usr/libexec/webmin      -j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modules/internet-0.3.5/internet.sh    -o
/usr/libexec/webmin          -j WRITE
/sbin/lidsconf -A -s /usr/libexec/webmin/sysstats/modules/irq-0.8.6/irq.sh -o /usr/libexec/webmin
-j WRITE
/sbin/lidsconf -A -s /usr/libexec/webmin/sysstats/modules/load-0.2/load.sh -o /usr/libexec/webmin
-j WRITE
/sbin/lidsconf     -A     -s     /usr/libexec/webmin/sysstats/modules/mailq-0.5.5/mailq.sh     -o
/usr/libexec/webmin                  -j WRITE
/sbin/lidsconf -A -s /usr/libexec/webmin/sysstats/modules/mem-0.7.4/mem.sh -o /usr/libexec/webmin
-j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modules/network-0.8.6/network.sh    -o
/usr/libexec/webmin            -j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modules/network-0.8.6/network-lib.pl    -o
/usr/libexec/webmin          -j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modules/process-0.2.7/process.sh    -o
/usr/libexec/webmin            -j WRITE
/sbin/lidsconf     -A     -s     /usr/libexec/webmin/sysstats/modules/users-0.3.5/users.sh     -o
/usr/libexec/webmin                  -j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/clean_graph.sh    -o    /usr/libexec/webmin
-j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/modif_rrd.sh    -o    /usr/libexec/webmin
-j WRITE
/sbin/lidsconf    -A    -s    /usr/libexec/webmin/sysstats/index.cgi    -o    /usr/libexec/webmin
-j WRITE

echo ""
echo "Bind 9.x"
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_NET_BIND_SERVICE 53 -j GRANT
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_SETPCAP             -j GRANT
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_SYS_CHROOT          -j GRANT
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_SYS_RESOURCE        -j GRANT
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_SETUID              -j GRANT
/sbin/lidsconf -A -s /usr/sbin/named  -o CAP_SETGID              -j GRANT

echo ""
echo "ravantivirus"
/sbin/lidsconf -A -o /opt/rav                                    -j READONLY
/sbin/lidsconf -A -s /opt/rav/bin/ravmd -o /var/opt/rav          -j WRITE
/sbin/lidsconf -A -s /opt/rav/bin/RAVMilter -o /var/opt/rav      -j WRITE
```

Código 25 Script para establecer el comportamiento de LIDS.

PortSentry

Descripción

Es un detector de exploradores de puertos TCP (port scanner), el cual adopta una postura activa para cerrar el acceso a los atacantes, mientras notifica al administrador sobre la actividad de los exploradores. Cuenta con un proceso sencillo de configuración e inicialización. A los atacantes externos se les restringe el acceso al sistema mediante la eliminación de las rutas locales, el cambio en el filtrado dinámico de paquetes, o la inclusión en el sistema de "TCP wrappers" que niega el acceso al servidor desde las computadoras donde se está realizando el ataque. Todo esto sucede en tiempo real.

Algunas de sus características más importantes son:

- Es capaz de monitorear tanto ataques a puertos tipo TCP como UDP. Puede detectar los ataques que se realicen a varios puertos simultáneamente utilizando sólo una instancia en la ejecución del programa.

- Detecta ataques tipo stealth scan en cuatro distintos modos de operación, SYN/half-open, FIN, NULL, X-MÁS y oddball packet stealth.

- Reacciona automáticamente y en tiempo real a los ataques. Utilizando los mecanismos disponibles en el servidor donde se instala y las características de TCP/IP, bloquea el acceso al servidor desde los equipos donde se está realizando el ataque.

- PortSentry tiene una máquina de estados interna que le permite recordar qué equipos se habían conectado previamente; esto permite establecer en la configuración parámetros para identificar falsas alarmas y pruebas aleatorias de puertos.

- PortSentry emitirá reportes de todas las violaciones a la seguridad que detecte, a los sistemas de bitácoras, sean locales o remotos, indicando el nombre del equipo desde el que se realiza el reporte, la hora del ataque, la dirección IP del atacante y puertos TCP o UDS que fueron atacados. Cuando se utiliza junto con Logcheck, también emitirá correos electrónicos para avisar a los administradores.

- En su modo de operación normal, una vez que detecta un ataque, el servidor se convertirá en un hoyo negro para el atacante, haciendo que la mayoría de los ataques cesen en forma inmediata. Cuando se habla de la mayoría y no de todos, se está excluyendo aquellos ataques a los servicios que estén activos en el servidor y que por lo mismo no serán monitoreados por PortSentry.

- Gracias a su capacidad de monitorear puertos tipo UDP es posible detectar ataques a servicios tipo RPC, como TFTP, SNMP, etc.

Debido a que PortSentry cuenta con dos modalidades avanzadas de detección de ataques tipo stealth, la capacidad de PortSentry para detectar ataques se incrementa sustancialmente.

Actualmente, PortSentry trabaja bajo alguna de las siguientes modalidades de operación:

Clásica

En esta modalidad PortSentry va a escuchar un conjunto predefinido de puertos TCP y UDP y va a esperar a que se produzca un intento de conexión por ellos, en ese momento va a reaccionar bloqueando al equipo que intente conectarse a esos puertos.

Mejorada

Esta modalidad trabaja de forma muy similar a la clásica, con la única diferencia de que va a monitorear el conjunto de puertos identificando ataques tipo SYN/FIN etc. mediante una conexión directa a los puertos y no utilizando la función de sistema operativo *bind()*, la reacción es igual a la que se presenta en el modo clásico.

Avanzada

Esta modalidad se conoce como "conexión inversa a puertos". Lo que hace el programa es primero verificar qué puertos se encuentran en uso en el sistema y en seguida monitorear todos aquellos que no se encuentren en uso. Esta modalidad es muy poderosa y reacciona de forma extremadamente rápida a los ataques. Además es de muy bajo consumo de recursos del servidor. Adicionalmente tiene la característica de que verifica de forma permanente el estado de los puertos, de forma que, si posteriormente se activa un puerto que inicialmente no estaba activo, PortSentry va a eliminar el monitoreo de dicho puerto y dejar operar transparentemente al sistema que se haya conectado a dicho puerto. Con esto se evitan falsas alarmas, por ejemplo con protocolos como FTP que se conectan a sus clientes mediante un nuevo puerto una vez que se inicia una sesión. Una vez que los programas liberan los puertos, PortSentry retoma automáticamente el monitoreo, de forma que nunca se pierde la protección.

Configuración

```
# PortSentry Configuration
#
# $Id: portsentry.conf,v 1.13 1999/11/09 02:45:42 crowland Exp crowland $
#
# IMPORTANT NOTE: You CAN NOT put spaces between your port arguments.
#
# The default ports will catch a large number of common probes
#
# All entries must be in quotes.


########################
# Port Configurations #
########################
#
#
# Some example port configs for classic and basic Stealth modes
#
# I like to always keep some ports at the "low" end of the spectrum.
# This will detect a sequential port sweep really quickly and usually
# these ports are not in use (i.e. tcpmux port 1)
#
# ** X-Windows Users **: If you are running X on your box, you need to be sure
# you are not binding PortSentry to port 6000 (or port 2000 for OpenWindows users).
# Doing so will prevent the X-client from starting properly.
#
```

```
# These port bindings are *ignored* for Advanced Stealth Scan Detection Mode.
#

# Un-comment these if you are really anal:
TCP_PORTS="1,7,9,11,15,24,70,79,109,111,119,138,512,513,514,515,540,635,1080,1524,2000,2001,4000,
4001,5631,5742,6000,6001,6667,30303,32771,32772,32773,32774,31337,"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,32770,
32771,32772,32773,32774,31337,54321"
#
# Use these if you just want to be aware:
#TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,31337,32771
,32772,32773,32774,40421,49724,54320"
#UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,524,2000,12345,12346,20034,32771,32772,32773,32774,4
9724,54320"
UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321"

############################################
# Advanced Stealth Scan Detection Options #
############################################
#
# This is the number of ports you want PortSentry to monitor in Advanced mode.
# Any port *below* this number will be monitored. Right now it watches
# everything below 1023.
#
# On many Linux systems you cannot bind above port 61000. This is because
# these ports are used as part of IP masquerading. I don't recommend you
# bind over this number of ports. Realistically: I DON'T RECOMMEND YOU MONITOR
# OVER 1023 PORTS AS YOUR FALSE ALARM RATE WILL ALMOST CERTAINLY RISE. You've been
# warned! Don't write me if you have have a problem because I'll only tell
# you to RTFM and don't run above the first 1023 ports.
#
#
ADVANCED_PORTS_TCP="1023"
ADVANCED_PORTS_UDP="1023"
#
# This field tells PortSentry what ports (besides listening daemons) to
# ignore. This is helpful for services like ident that services such
# as FTP, SMTP, and wrappers look for but you may not run (and probably
# *shouldn't* IMHO).
#
# By specifying ports here PortSentry will simply not respond to
# incoming requests, in effect PortSentry treats them as if they are
# actual bound daemons. The default ports are ones reported as
# problematic false alarms and should probably be left alone for
# all but the most isolated systems/networks.
#
# Default TCP ident and NetBIOS service
ADVANCED_EXCLUDE_TCP="113,139"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
ADVANCED_EXCLUDE_UDP="520,138,137,67"


######################
# Configuration Files#
######################
#
# Hosts to ignore
IGNORE_FILE="/etc/portsentry/portsentry.ignore"
# Hosts that have been denied (running history)
HISTORY_FILE="/var/log/portsentry/portsentry.history"
# Hosts that have been denied this session only (temporary until next restart)
BLOCKED_FILE="/var/log/portsentry/portsentry.blocked"

###################
# Response Options#
###################
# Options to dispose of attacker. Each is an action that will
```

```
# be run if an attack is detected. If you don't want a particular
# option then comment it out and it will be skipped.
#
# The variable $TARGET$ will be substituted with the target attacking
# host when an attack is detected. The variable $PORT$ will be substituted
# with the port that was scanned.
#
###################
# Ignore Options #
###################
# These options allow you to enable automatic response
# options for UDP/TCP. This is useful if you just want
# warnings for connections, but don't want to react for
# a particular protocol (i.e. you want to block TCP, but
# not UDP). To prevent a possible Denial of service attack
# against UDP and stealth scan detection for TCP, you may
# want to disable blocking, but leave the warning enabled.
# I personally would wait for this to become a problem before
# doing though as most attackers really aren't doing this.
# The third option allows you to run just the external command
# in case of a scan to have a pager script or such execute
# but not drop the route. This may be useful for some admins
# who want to block TCP, but only want pager/e-mail warnings
# on UDP, etc.
#
#
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="0"
BLOCK_TCP="1"

####################
# Dropping Routes:#
####################
# This command is used to drop the route or add the host into
# a local filter table.
#
# The gateway (333.444.555.666) should ideally be a dead host on
# the *local* subnet. On some hosts you can also point this at
# localhost (127.0.0.1) and get the same effect. NOTE THAT
# 333.444.555.66 WILL *NOT* WORK. YOU NEED TO CHANGE IT!!
#
# All KILL ROUTE OPTIONS ARE COMMENTED OUT INITIALLY. Make sure you
# uncomment the correct line for your OS. If you OS is not listed
# here and you have a route drop command that works then please
# mail it to me so I can include it. ONLY ONE KILL_ROUTE OPTION
# CAN BE USED AT A TIME SO DON'T UNCOMMENT MULTIPLE LINES.
#
# NOTE: The route commands are the least optimal way of blocking
# and do not provide complete protection against UDP attacks and
# will still generate alarms for both UDP and stealth scans. I
# always recommend you use a packet filter because they are made
# for this purpose.
#

# Generic
#KILL_ROUTE="/sbin/route add $TARGET$ 333.444.555.666"

# Generic Linux
#KILL_ROUTE="/sbin/route add -host $TARGET$ gw 333.444.555.666"

# Newer versions of Linux support the reject flag now. This
# is cleaner than the above option.
#KILL_ROUTE="/sbin/route add -host $TARGET$ reject"

# Generic BSD (BSDI, OpenBSD, NetBSD, FreeBSD)
#KILL_ROUTE="/sbin/route add $TARGET$ 333.444.555.666"
```

```
# Generic Sun
#KILL_ROUTE="/usr/sbin/route add $TARGET$ 333.444.555.666 1"

# NEXTSTEP
#KILL_ROUTE="/usr/etc/route add $TARGET$ 127.0.0.1 1"

# FreeBSD (Not well tested.)
#KILL_ROUTE="route add -net $TARGET$ -netmask 255.255.255.255 127.0.0.1 -blackhole"

# Digital UNIX 4.0D (OSF/1 / Compaq Tru64 UNIX)
#KILL_ROUTE="/sbin/route add -host -blackhole $TARGET$ 127.0.0.1"

# Generic HP-UX
#KILL_ROUTE="/usr/sbin/route add net $TARGET$ netmask 255.255.255.0 127.0.0.1"

##
# Using a packet filter is the preferred method. The below lines
# work well on many OS's. Remember, you can only uncomment *one*
# KILL_ROUTE option.
##

# For those of you running Linux with ipfwadm installed you may like
# this better as it drops the host into the packet filter.
# You can only have one KILL_ROUTE turned on at a time though.
# This is the best method for Linux hosts.
#
#KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$ -o"
#
# This version does not log denied packets after activation
#KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$"
#
# New ipchain support for Linux kernel version 2.102+
KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l"
#
# For those of you running FreeBSD (and compatible) you can
# use their built in firewalling as well.
#
#KILL_ROUTE="/sbin/ipfw add 1 deny all from $TARGET$:255.255.255.255 to any"

################
# TCP Wrappers#
################
# This text will be dropped into the hosts.deny file for wrappers
# to use. There are two formats for TCP wrappers:
#
# Format One: Old Style - The default when extended host processing
# options are not enabled.
#
#KILL_HOSTS_DENY="ALL: $TARGET$"
#
# Format Two: New Style - The format used when extended option
# processing is enabled. You can drop in extended processing
# options, but be sure you escape all '%' symbols with a backslash
# to prevent problems writing out (i.e. \%c \%h )
#
#KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"

####################
# External Command#
####################
# This is a command that is run when a host connects, it can be whatever
# you want it to be (pager, etc.). This command is executed before the
# route is dropped. I NEVER RECOMMEND YOU PUT IN RETALIATORY ACTIONS
# AGAINST THE HOST SCANNING YOU. TCP/IP is an *unauthenticated protocol*
# and people can make scans appear out of thin air. The only time it
# is reasonably safe (and I *never* think it is reasonable) to run
# reverse probe scripts is when using the "classic" -tcp mode. This
# mode requires a full connect and is very hard to spoof.
#
#KILL_RUN_CMD="/some/path/here/script $TARGET$ $PORT$"
```

```
#####################
# Scan trigger value#
#####################
# Enter in the number of port connects you will allow before an
# alarm is given. The default is 0 which will react immediately.
# A value of 1 or 2 will reduce false alarms. Anything higher is
# probably not necessary. This value must always be specified, but
# generally can be left at 0.
#
# NOTE: If you are using the advanced detection option you need to
# be careful that you don't make a hair trigger situation. Because
# Advanced mode will react for *any* host connecting to a non-used
# below your specified range, you have the opportunity to really
# break things. (i.e someone innocently tries to connect to you via
# SSL [TCP port 443] and you immediately block them). Some of you
# may even want this though. Just be careful.
#

SCAN_TRIGGER="0"


# EOF
```

Código 26 Configuración de *portsentry*.

HostSentry

Descripción

HostSentry es una herramienta para la detección de intrusos para todo tipo de equipos o servidores tipo Unix. Esta herramienta ejecuta un proceso llamado LAD - "Login Anomaly Detection" (comportamiento anormal de sesión), el cual permite a los administradores que identifiquen un comportamiento extraño en el acceso al sistema (Login), responder rápidamente al comportamiento inusual e identificar las cuentas comprometidas. HostSentry incorpora una base de datos dinámica y aprende del comportamiento de las sesiones de los usuarios. Este comportamiento es entonces utilizado por distintos módulos detectores de *firmas*[xxi] para detectar acontecimientos inusuales.

LAD funciona a través del monitoreo de las sesiones interactivas con el servidor detectando comportamientos inusuales o actividades que indican que se tiene una violación a la seguridad del equipo o bien que hay un intruso. HostSentry hace el monitoreo y reporte de las actividades en tiempo real.

Una de las más grandes debilidades de seguridad de Unix no es un hoyo específico, sino el hecho de que le permite a quien lo solicite intentar establecer una sesión interactiva. Aun utilizando herramientas que permiten el cifrado de sesiones interactivas, como SSH, sigue siendo posible que un atacante intercepte y comprometa las claves de los usuarios a través de otros servicios donde la información no viaja cifrada. Es por esta razón que en el esquema de seguridad que se implementó en este proyecto se ha aplicado el concepto "un solo servicio por servidor", de manera que no hay claves de usuario que puedan ser comprometidas inadvertidamente cuando se utilizan distintos servicios. Esta técnica reduce significativamente el problema que acabamos de mencionar. Para mayor detalle, favor de revisar el diagrama (diagrama 17) de servidores que se encuentra en los resultados.

En general, los sistemas operativos tipo Unix proveen bitácoras de sistema y HostSentry utiliza esta información para identificar problemas, antes de que se conviertan en graves. Para ello se utilizan las técnicas que se describen a continuación.

¿Qué es lo que hace HostSentry?

HostSentry monitorea las bitácoras de inicio y fin de sesión (wtmp/utmp) identificando las acciones de los usuarios. En estas bitácoras es posible encontrar información como:

- Nombre del usuario que estableció o terminó una sesión
- Consola o Terminal a través de la cual se conectó.
- Hora en la que inicio/terminó su conexión.
- Equipo desde el que se originó la conexión.

Con toda esta información se crea una base de datos que sirve para el análisis de acciones que se presenten en el futuro. Alguna de esta información puede incluso servir para detectar problemas de forma inmediata. En algunos otros casos es necesario acumular suficiente información histórica para poder realizar análisis que revelen información sobre problemas. En cualquiera de los casos, esta información ya le permite a los distintos módulos de firmas del sistema contar con información para trabajar.

¿Qué es un módulo de firmas?

Un módulo de firmas de HostSentry es el conjunto de rutinas que realizan una o ambas de las siguientes acciones:

- Procesamiento al inicio de una sesión.
- Procesamiento al finalizar una sesión.

Al inicio de una sesión todos los módulos de firmas que realizan análisis de inicio de sesión son invocados, con el objeto de que detecten anomalías y tomen las acciones correspondientes.
Al finalizar una sesión todos los módulos de firmas que realizan análisis de fin de sesión son invocados, con el objeto de que detecten anomalías y tomen las acciones correspondientes.
Se puede decir que como parte de las acciones que toman ambos tipos de módulos de firmas está el reporte de cualquier anomalía detectada.

Los beneficios de este modo de operación dual son los siguientes:
Un usuario que es sospechoso es identificado inmediatamente al inicio de una sesión.
La actividad sospechosa que realizó un usuario durante su sesión se detecta inmediatamente al final de ésta. Dado que los módulos pueden trabajar tanto al inicio como al final de las sesiones, obtenemos una doble validación sobre las actividades de los usuarios.

Un ejemplo de un módulo que se activa sólo al inicio de la sesión es: moduleFirstLogin. Este módulo se ejecuta sólo al inicio de la sesión y su única función es verificar y reportar si ésta es la primera vez que un usuario establece una sesión interactiva.

Un ejemplo de un módulo que se activa sólo al fin de la sesión es moduleHistoryTruncated. Este módulo se encarga de verificar al final de la sesión del usuario que el archivo que almacena los comandos que el usuario ejecutó durante su sesión (history) no haya sido borrado, ligado a /dev/null o algún otro dispositivo y que sea de más de 0 bytes.

Un ejemplo de un módulo que se activa en ambos casos es: moduleHistoryTruncated que se encarga de grabar en las bitácoras el momento en que un usuario entra en sesión y el momento en que termina su sesión.

¿Qué es lo que hacen todos los módulos de firmas?

Los módulos de firmas realizan un conjunto muy variado de funciones. Dado que son modulares cada uno puede o no estar activo en el sistema; esto es decisión del administrador del sistema. La modularidad posibilita que se puedan programar y agregar módulos hechos a la medida. A continuación se presenta una lista de los módulos que vienen por omisión y una breve descripción de su función.

moduleLoginLogout[xxii]

Este módulo simplemente guarda en la bitácora un registro del momento en el que los usuarios inician o terminan su sesión. Éste es un módulo genérico cuya finalidad es ser complemento al registro de inicio y fin que tradicionalmente tienen los sistemas.

moduleFirstLogin

Dado que la mayoría de los usuarios de sistemas de cómputo no tienen ni necesidad ni conocimientos sobre cómo se utiliza una sesión interactiva con un servidor tipo Unix, la recomendación general es no darles acceso interactivo a los usuarios, aun cuando como usuarios de un cierto servidor reciban, utilicen o tengan derecho a algún otro tipo de servicios, por ejemplo correo electrónico. Sólo en los casos en que el usuario tenga un fin particular por el cual utilizar una sesión interactiva se le debe proporcionar una cuenta con capacidad para ello.

Por esta razón, el hecho de que un usuario que nunca había utilizado su capacidad de establecer sesiones interactivas con un servidor se decida a hacerlo constituye un evento importante que puede darnos pistas sobre una posible violación a la seguridad. El hecho de que el usuario haya establecido una sesión puede o no ser normal; el administrador es quien, una vez que ha sido notificado por la herramienta, debe decidir esto y tomar las medidas pertinentes, en caso necesario.

El único propósito de este módulo es el de alertar a los administradores de las *primeras veces* que los usuarios establecen sesiones interactivas con el servidor. Este módulo es especialmente útil para detectar casos en los que la clave de un usuario ha sido interceptada por algún medio y se empieza a utilizar para comprometer al sistema. Este módulo es muy útil cuando se tiene un gran número de usuarios en el servidor.

moduleForeignDomain

En muchos casos, los atacantes que intentan violar la seguridad de un servidor se conectan desde equipos que no tienen, al menos al menos de manera evidente, una relación con dicho servidor. Es por ello que es muy recomendable, cuando esto es posible sin negar servicios a usuarios legítimos, limitar el acceso a los servicios de nuestro servidor a aquellos usuarios que se conectan desde equipos que pertenecen a la misma empresa o que, de manera evidente, tienen alguna relación con nuestros servicios o con el servidor.

El objeto de este módulo es el de alertar al administrador cuando un usuario establece una sesión desde un equipo que pertenece a un dominio que no se encuentra entre aquellos que hemos listado en el archivo de configuración (moduleForeignDomain.allow). Cuando eso ocurre la sesión se clasifica como "extranjera" y el administrador recibe una alerta. Un ejemplo sería que si a nuestro servidor ubicado en México se conectara un usuario desde China y China no se encuentra dentro de nuestro archivo de configuración, entonces esta sesión sería una sesión "extranjera" y el administrador recibiría la alerta correspondiente.

moduleRhostCheck

Un usuario que hace modificaciones a su archive .rhosts que ponen en riesgo la seguridad de nuestro servidor puede estar haciendo esto, bien por ignorancia o bien porque no tiene buenas intenciones. Este módulo revisa el archivo .rhosts del usuario al final de su sesión y se asegura de que el contenido no sea tal que pueda comprometer el servidor. Al igual que en otros módulos descubrir una vulnerabilidad potencial genera un aviso al administrador.

En realidad, la mejor recomendación de seguridad que se puede hacer alrededor de los servicios remotos es simplemente no utilizarlos, ya que es muy difícil lograr una instalación correcta y que no permita grandes vulnerabilidades.

moduleHistoryTruncated

Este módulo se encarga de verificar al final de la sesión del usuario que el archivo que almacena los comandos que el usuario ejecutó durante su sesión (history) no haya sido borrado, ligado a /dev/null o a algún otro dispositivo y que sea de más de 0 bytes.

Esta verificación se realiza tomando en cuenta qué tipo de sistema interactivo de comandos esté utilizando el usuario (shell), revisando lo pertinente en la base de datos de usuarios del sistema, típicamente /etc/passwd.

Como en los demás casos, en el momento en que se identifica una anomalía, el administrador es notificado y se puede proceder a hacer una revisión exhaustiva.

Es importante señalar que todos estos módulos son útiles mientras que el atacante no logre el control total del sistema y deshabilite la herramienta misma.

moduleOddDirnames[xxiii]

En el caso en que el usuario cree un directorio con nombre *extraño*, por ejemplo nombres como ".. " ó "..." ó "etc", normalmente estaremos ante un caso en el que un usuario o atacante está intentando esconder información de una revisión casual o normal, no exhaustiva. Definitivamente el administrador debe recibir una alerta y revisar el directorio cuidadosamente para saber de qué se trata. Dado que el número de permutaciones y combinaciones de nombres de directorio de tipo *extraño* es enorme, este módulo no es infalible.

moduleMultipleLogins

Cuando un usuario establece varias sesiones desde más de un equipo remoto, probablemente estemos frente a un caso en el que la clave del usuario haya sido comprometida, o bien el usuario muy probablemente haya violado las normas de confidencialidad de las claves, compartiéndola con alguien de tal suerte que ésta otra persona se puede conectar también a nuestro servidor. En cualquiera de estos casos es necesario que el administrador sea notificado y proceda a revisar qué es lo que sucede. La configuración HostSentry (moduleMultipleLogins.allow) permite excepciones, de tal forma que usuarios que trabajan desde la oficina y, sin terminar dicha sesión, se conectan desde su casa y están autorizados para hacerlo, no generen una alerta innecesaria.

Dado que los módulos trabajan todo simultáneamente es posible detectar casos como **múltiples sesiones remotas** desde **equipos extranjeros**, lo que casi siempre significa una violación a la seguridad de nuestro servidor que ya se "extendió" o es del dominio público.

La segunda herramienta integrada al subsistema de seguridad es el Tripwire. Este producto es una herramienta que permite realizar verificaciones para determinar qué ha cambiado en el sistema. El programa se encarga de monitorear atributos claves de archivos que no pueden ser cambiados, incluyendo su firma binaria, su tamaño, cambio de tamaño esperado etc. La parte difícil de este proceso es hacerlo en la forma correcta, con seguridad, y con facilidades para el mantenimiento y preservando la totalidad de la funcionalidad y operabilidad del sistema.

Configuración

```
# HostSentry Máster Config File
# Author: Craig H. Rowland <crowland@psionic.com>
# Created: 10-6-98
#
# Send all changes/modifications/bugfixes to the above address.
#
# This software is Copyright(c) 1997-98 Craig H. Rowland
#
# Disclaimer:
#
# All software distributed by Craig H. Rowland ("the author") and
# Psionic Systems is distributed AS IS and carries NO WARRANTY or
# GUARANTEE OF ANY KIND. End users of the software acknowledge that
# they will not hold the author, Psionic Systems, and any employer of
# the author liable for failure or non-function of a software
# product. YOU ARE USING THIS PRODUCT AT YOUR OWN RISK
#
# Licensing restrictions apply. See the license that came with this
# file for more information or visit http://www.psionic.com for more
# information.
```

```
#
# This software is NOT GPL NOR PUBLIC DOMAIN so please read the license
# before modifying or distributing. Contact the above address if you have
# any questions.
#
# $Id: hostsentry.conf,v 1.3 1999/03/25 22:05:44 crowland Exp crowland $


IGNORE_FILE = "/etc/hostsentry/hostsentry.ignore"
ACTION_FILE = "/etc/hostsentry/hostsentry.action"
MODULE_FILE = "/etc/hostsentry/hostsentry.modules"
MODULE_PATH = "/usr/lib/hostsentry/modules"
WTMP_FILE = "/var/log/wtmp"
DB_FILE = "/var/hostsentry/hostsentry.db"
DB_TTY_FILE = "/var/hostsentry/hostsentry.tty.db"


# WTMP formats vary between Unices. As a result you need to let HostSentry
# know what format your wtmp is. Luckily I made this fairly straight
# forward if you know how to read your systems utmp.h or utmpx.h file.
#
# The basic things needed are:
#
# a) Size of utmp record (sizeof(struct utmp)) for your host.
# b) Offset to tty field from beginning of record.
# c) Length of tty field.
# d) Offset to username field from beginning of record.
# e) Length of username field.
# f) Offset to hostname field from beginning of record.
# g) Length of hostname field.
#
# The format is formed like this:
#
# utmpRecordLength/ttyOffset:ttyLen/usernameOffset:usernameLen/hostnameOffset:hostnameLen
#
# For example on RedHat:
#
# utmp record size is: 384 bytes
# tty entry offset is: 8 bytes
# tty entry size from offset is: 32 bytes
# username entry offet is: 44 bytes
# username entry size from offset is: 32 bytes
# hostname entry offset is: 76 bytes
# hostname entry size from offset: 256 bytes
#
# This would be formed as "384/8:32/44:32/76:256"
#
# NOTE: All of this garbage will hopefully go away on a future update when
# I wrap native getutent() functions for Python.
#
# RedHat
WTMP_FORMAT = "384/8:32/44:32/76:256"
# Slackware
#WTMP_FORMAT = "56/8:12/28:8/36:16"
# BSD variants
#WTMP_FORMAT = "36/0:8/8:8/16:16"
```

Código 27 Configuración de *hostsentry*.

Tripwire

Descripción

Tripwire es una herramienta que verifica qué es lo que ha cambiado en un sistema. Esto lo hace a través de un monitoreo de los atributos clave de los archivos, tales como su firma[xxiv], tamaño, permisos, etc. (diagrama 15) Lo complicado es hacer esto manteniendo un balance adecuado en cuanto a seguridad, mantenimiento y funcionalidad, sin embargo, si no pretendemos detectar los cambios en el preciso momento en que suceden, Tripwire hace muy bien el trabajo. Dado que para la protección más elemental de la información más crítica para nuestro sistema se está utilizando LIDS, que impide en todo momento el acceso a los archivos de contenido a todos los usuarios distintos de aquel que ejecuta el proceso del servidor de páginas, el hecho de que la detección de los cambios se realice sólo una vez al día no es de un impacto crítico o grave y dado que la cobertura de esta herramienta es mayor que la cobertura de LIDS, entendiendo cobertura como el número de archivos que supervisan uno y otro, su uso se vuelve de interés y utilidad.

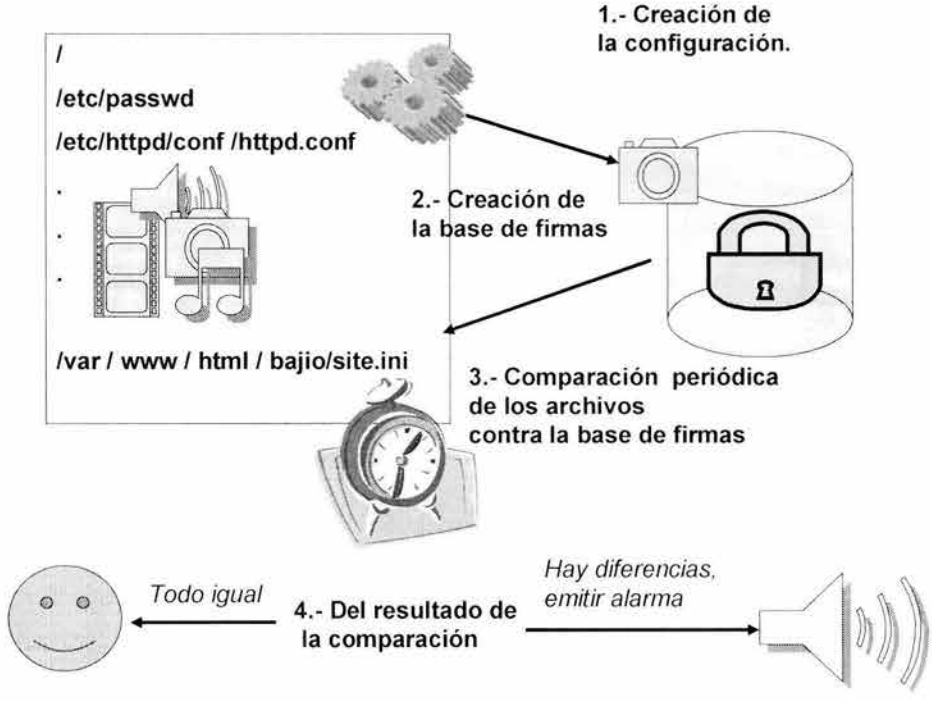


Diagrama 15 Funcionamiento de Tripwire.

Configuración

```
##############################################################################
#                                                                           ##
##############################################################################  #
#                                                                           #  #
#                     Policy file for Red Hat Linux                         #  #
#                              V1.2.0rh                                     #  #
#                           August 9, 2001                                  #  #
#                                                                           ##
##############################################################################


##############################################################################
#                                                                           ##
##############################################################################  #
#                                                                           #  #
# TRIPWIRE CONFIGURATION FILE                                               #  #
```

```
#                                                                              # #
#  If you have comment/questions/suggestions about this script, please         # #
#  drop me a line at:                                                          # #
#                                                                              # #
#                                                                              # #
#  sebas@iac.com.mx                                                            # #
#                                                                              # #
#  I welcome suggestions! .                                                    # #
# semi-colon delimited.                                                        # #
#                                                                              ##
################################################################################

  ##############################################################################
 #                                                                             ##
################################################################################ #
#                                                                              # #
# Global Variable Definitions                                                  # #
#                                                                              # #
# These are defined at install time by the installation script.  You may       # #
# Manually edit these if you are using this file directly and not from the     # #
# installation script itself.                                                  # #
#                                                                              ##
################################################################################

@@section GLOBAL
TWROOT=/usr/sbin;
TWBIN=/usr/sbin;
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME=localhost;

@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;  # Critical files that cannot change
SEC_SUID      = $(IgnoreNone)-SHa ;  # Binaries with the SUID or SGID flags set
SEC_BIN       = $(ReadOnly) ;        # Binaries that should not change
SEC_CONFIG     = $(Dynamic) ;          # Config files that are changed infrequently but accessed
often
SEC_LOG       = $(Growing) ;         # Files that grow, but that should never change ownership
SEC_INVARIANT = +tpug ;                   # Directories that should never change permission or
ownership
SIG_LOW       = 33 ;                 # Non-critical files that are of minimal security impact
SIG_MED       = 66 ;                 # Non-critical files that are of significant security impact
SIG_HI          = 100 ;                        # Critical files that are significant points of
vulnerability

# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen                     -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                   -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                    -> $(SEC_BIN) ;
  $(TWBIN)/twprint                    -> $(SEC_BIN) ;
}

# Tripwire Data Files - Configuration Files, Policy Files, Keys, Reports, Databases
(
  rulename = "Tripwire Data Files",
  severity = $(SIG_HI)
)
{
  # NOTE: We remove the inode attribute because when Tripwire creates a backup,
  # it does so by renaming the old file and creating a new one (which will
  # have a new inode number).  Inode is left turned on for keys, which shouldn't
  # ever change.
```

```
  # NOTE: The first integrity check triggers this rule and each integrity check
  # afterward triggers this rule until a database update is run, since the
  # database file does not exist before that point.

  $(TWDB)                                -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol                        -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg                        -> $(SEC_BIN) -i ;
  $(TWLKEY)/$(HOSTNAME)-local.key        -> $(SEC_BIN) ;
  $(TWSKEY)/site.key                     -> $(SEC_BIN) ;

  #don't scan the individual reports
  $(TWREPORT)                            -> $(SEC_CONFIG) (recurse=0) ;
}

# Commonly accessed directories that should remain static with regards to owner and group
(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)
{
  /                                      -> $(SEC_INVARIANT) (recurse = 0) ;
  /home                                  -> $(SEC_INVARIANT) (recurse = 0) ;
  /etc                                   -> $(SEC_INVARIANT) (recurse = 0) ;
}
  ################################################
 #                                              ##
################################################ #
#                                              # #
# File System and Disk Administration Programs # #
#                                              ##
################################################

(
  rulename = "File System and Disk Administraton Programs",
  severity = $(SIG_HI)
)
{
  /sbin/accton                           -> $(SEC_CRIT) ;
  /sbin/badblocks                        -> $(SEC_CRIT) ;
  /sbin/busybox                          -> $(SEC_CRIT) ;
  /sbin/busybox.anaconda                 -> $(SEC_CRIT) ;
  /sbin/convertquota                     -> $(SEC_CRIT) ;
  /sbin/dosfsck                          -> $(SEC_CRIT) ;
  /sbin/debugfs                          -> $(SEC_CRIT) ;
  /sbin/debugreiserfs                    -> $(SEC_CRIT) ;
  /sbin/dumpe2fs                         -> $(SEC_CRIT) ;
  /sbin/dump                             -> $(SEC_CRIT) ;
  /sbin/dump.static                      -> $(SEC_CRIT) ;
  # /sbin/e2fsadm                          -> $(SEC_CRIT) ; tune2fs?
  /sbin/e2fsck                           -> $(SEC_CRIT) ;
  /sbin/e2label                          -> $(SEC_CRIT) ;
  /sbin/fdisk                            -> $(SEC_CRIT) ;
  /sbin/fsck                             -> $(SEC_CRIT) ;
  /sbin/fsck.ext2                        -> $(SEC_CRIT) ;
  /sbin/fsck.ext3                        -> $(SEC_CRIT) ;
  /sbin/fsck.minix                       -> $(SEC_CRIT) ;
  /sbin/fsck.msdos                       -> $(SEC_CRIT) ;
  /sbin/fsck.vfat                        -> $(SEC_CRIT) ;
  /sbin/ftl_check                        -> $(SEC_CRIT) ;
  /sbin/ftl_format                       -> $(SEC_CRIT) ;
  /sbin/hdparm                           -> $(SEC_CRIT) ;
  #/sbin/lvchange                         -> $(SEC_CRIT) ;
  #/sbin/lvcreate                         -> $(SEC_CRIT) ;
  #/sbin/lvdisplay                        -> $(SEC_CRIT) ;
  #/sbin/lvextend                         -> $(SEC_CRIT) ;
  #/sbin/lvmchange                        -> $(SEC_CRIT) ;
  #/sbin/lvmcreate_initrd                 -> $(SEC_CRIT) ;
  #/sbin/lvmdiskscan                      -> $(SEC_CRIT) ;
  #/sbin/lvmsadc                          -> $(SEC_CRIT) ;
```

```
#/sbin/lvmsar                    -> $(SEC_CRIT) ;
#/sbin/lvreduce                  -> $(SEC_CRIT) ;
#/sbin/lvremove                  -> $(SEC_CRIT) ;
#/sbin/lvrename                  -> $(SEC_CRIT) ;
#/sbin/lvscan                    -> $(SEC_CRIT) ;
/sbin/mkbootdisk                 -> $(SEC_CRIT) ;
/sbin/mkdosfs                    -> $(SEC_CRIT) ;
/sbin/mke2fs                     -> $(SEC_CRIT) ;
/sbin/mkfs                       -> $(SEC_CRIT) ;
/sbin/mkfs.bfs                   -> $(SEC_CRIT) ;
/sbin/mkfs.ext2                  -> $(SEC_CRIT) ;
/sbin/mkfs.minix                 -> $(SEC_CRIT) ;
/sbin/mkfs.msdos                 -> $(SEC_CRIT) ;
/sbin/mkfs.vfat                  -> $(SEC_CRIT) ;
/sbin/mkinitrd                   -> $(SEC_CRIT) ;
/sbin/mkpv                       -> $(SEC_CRIT) ;
/sbin/mkraid                     -> $(SEC_CRIT) ;
/sbin/mkreiserfs                 -> $(SEC_CRIT) ;
/sbin/mkswap                     -> $(SEC_CRIT) ;
#/sbin/mtx                       -> $(SEC_CRIT) ;
/sbin/pam_console_apply          -> $(SEC_CRIT) ;
/sbin/parted                     -> $(SEC_CRIT) ;
/sbin/pcinitrd                   -> $(SEC_CRIT) ;
#/sbin/pvchange                  -> $(SEC_CRIT) ;
#/sbin/pvcreate                  -> $(SEC_CRIT) ;
#/sbin/pvdata                    -> $(SEC_CRIT) ;
#/sbin/pvdisplay                 -> $(SEC_CRIT) ;
#/sbin/pvmove                    -> $(SEC_CRIT) ;
#/sbin/pvscan                    -> $(SEC_CRIT) ;
/sbin/quotacheck                 -> $(SEC_CRIT) ;
/sbin/quotaon                    -> $(SEC_CRIT) ;
/sbin/raidstart                  -> $(SEC_CRIT) ;
/sbin/reiserfsck                 -> $(SEC_CRIT) ;
/sbin/resize2fs                  -> $(SEC_CRIT) ;
/sbin/resize_reiserfs            -> $(SEC_CRIT) ;
/sbin/restore                    -> $(SEC_CRIT) ;
/sbin/restore.static             -> $(SEC_CRIT) ;
/sbin/scsi_info                  -> $(SEC_CRIT) ;
/sbin/sfdisk                     -> $(SEC_CRIT) ;
/sbin/stinit                     -> $(SEC_CRIT) ;
#/sbin/tapeinfo                  -> $(SEC_CRIT) ;
/sbin/tune2fs                    -> $(SEC_CRIT) ;
/sbin/unpack                     -> $(SEC_CRIT) ;
/sbin/update                     -> $(SEC_CRIT) ;
#/sbin/vgcfgbackup               -> $(SEC_CRIT) ;
#/sbin/vgcfgrestore              -> $(SEC_CRIT) ;
#/sbin/vgchange                  -> $(SEC_CRIT) ;
#/sbin/vgck                      -> $(SEC_CRIT) ;
#/sbin/vgcreate                  -> $(SEC_CRIT) ;
#/sbin/vgdisplay                 -> $(SEC_CRIT) ;
#/sbin/vgexport                  -> $(SEC_CRIT) ;
#/sbin/vgextend                  -> $(SEC_CRIT) ;
#/sbin/vgimport                  -> $(SEC_CRIT) ;
#/sbin/vgmerge                   -> $(SEC_CRIT) ;
#/sbin/vgmknodes                 -> $(SEC_CRIT) ;
#/sbin/vgreduce                  -> $(SEC_CRIT) ;
#/sbin/vgremove                  -> $(SEC_CRIT) ;
#/sbin/vgrename                  -> $(SEC_CRIT) ;
#/sbin/vgscan                    -> $(SEC_CRIT) ;
#/sbin/vgsplit                   -> $(SEC_CRIT) ;
/bin/chgrp                       -> $(SEC_CRIT) ;
/bin/chmod                       -> $(SEC_CRIT) ;
/bin/chown                       -> $(SEC_CRIT) ;
/bin/cp                          -> $(SEC_CRIT) ;
/bin/cpio                        -> $(SEC_CRIT) ;
/bin/mount                       -> $(SEC_CRIT) ;
/bin/umount                      -> $(SEC_CRIT) ;
/bin/mkdir                       -> $(SEC_CRIT) ;
/bin/mknod                       -> $(SEC_CRIT) ;
/bin/mktemp                      -> $(SEC_CRIT) ;
```

```
  /bin/rm                                -> $(SEC_CRIT) ;
  /bin/rmdir                             -> $(SEC_CRIT) ;
  /bin/touch                             -> $(SEC_CRIT) ;
)

  ###################################
 #                                  ##
################################### #
#                                  # #
# Kernel Administration Programs # #
#                                  ##
###################################

(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/adjtimex                         -> $(SEC_CRIT) ;
  /sbin/ctrlaltdel                       -> $(SEC_CRIT) ;
  /sbin/depmod                           -> $(SEC_CRIT) ;
  /sbin/insmod                           -> $(SEC_CRIT) ;
  /sbin/insmod.static                    -> $(SEC_CRIT) ;
  /sbin/insmod_ksymoops_clean            -> $(SEC_CRIT) ;
  /sbin/klogd                            -> $(SEC_CRIT) ;
  /sbin/ldconfig                         -> $(SEC_CRIT) ;
  /sbin/minilogd                         -> $(SEC_CRIT) ;
  /sbin/modinfo                          -> $(SEC_CRIT) ;
  /sbin/nuactlun                         -> $(SEC_CRIT) ;
  /sbin/nuscsitcpd                       -> $(SEC_CRIT) ;
  /sbin/pivot_root                       -> $(SEC_CRIT) ;
  /sbin/sndconfig                        -> $(SEC_CRIT) ;
  /sbin/sysctl                           -> $(SEC_CRIT) ;
)

  ########################
 #                      ##
######################## #
#                      # #
# Networking Programs  # #
#                      ##
########################

(
  rulename = "Networking Programs",
  severity = $(SIG_HI)
)
{
  /etc/sysconfig/network-scripts/ifdown                  -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-cipcb            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ippp             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ipv6             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-isdn             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-post             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ppp              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-sit              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-sl               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup                    -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-aliases            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-cipcb              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ippp               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ipv6               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-isdn               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-plip               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-plusb              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-post               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ppp                -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-routes             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-sit                -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-sl                 -> $(SEC_CRIT) ;
```

```
  /etc/sysconfig/network-scripts/ifup-wireless          -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/network-functions      -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/network-functions-ipv6 -> $(SEC_CRIT) ;
  /bin/ping                             -> $(SEC_CRIT) ;
  /sbin/agetty                          -> $(SEC_CRIT) ;
  /sbin/arp                             -> $(SEC_CRIT) ;
  /sbin/arping                          -> $(SEC_CRIT) ;
  /sbin/dhcpcd                          -> $(SEC_CRIT) ;
  /sbin/ether-wake                      -> $(SEC_CRIT) ;
  #/sbin/getty                           -> $(SEC_CRIT) ;
  /sbin/ifcfg                           -> $(SEC_CRIT) ;
  /sbin/ifconfig                        -> $(SEC_CRIT) ;
  /sbin/ifdown                          -> $(SEC_CRIT) ;
  /sbin/ifenslave                       -> $(SEC_CRIT) ;
  /sbin/ifport                          -> $(SEC_CRIT) ;
  /sbin/ifup                            -> $(SEC_CRIT) ;
  /sbin/ifuser                          -> $(SEC_CRIT) ;
  /sbin/ip                              -> $(SEC_CRIT) ;
  /sbin/ip6tables                       -> $(SEC_CRIT) ;
  /sbin/ipchains                        -> $(SEC_CRIT) ;
  /sbin/ipchains-restore                -> $(SEC_CRIT) ;
  /sbin/ipchains-save                   -> $(SEC_CRIT) ;
  /sbin/ipfwadm                         -> $(SEC_CRIT) ;
  /sbin/ipmaddr                         -> $(SEC_CRIT) ;
  /sbin/iptables                        -> $(SEC_CRIT) ;
  /sbin/iptables-restore                -> $(SEC_CRIT) ;
  /sbin/iptables-save                   -> $(SEC_CRIT) ;
  /sbin/iptunnel                        -> $(SEC_CRIT) ;
  /sbin/ipvsadm                         -> $(SEC_CRIT) ;
  /sbin/ipvsadm-restore                 -> $(SEC_CRIT) ;
  /sbin/ipvsadm-save                    -> $(SEC_CRIT) ;
  /sbin/ipx_configure                   -> $(SEC_CRIT) ;
  /sbin/ipx_interface                   -> $(SEC_CRIT) ;
  /sbin/ipx_internal_net                -> $(SEC_CRIT) ;
  /sbin/iwconfig                        -> $(SEC_CRIT) ;
  /sbin/iwgetid                         -> $(SEC_CRIT) ;
  /sbin/iwlist                          -> $(SEC_CRIT) ;
  /sbin/iwpriv                          -> $(SEC_CRIT) ;
  /sbin/iwspy                           -> $(SEC_CRIT) ;
  /sbin/mgetty                          -> $(SEC_CRIT) ;
  /sbin/mingetty                        -> $(SEC_CRIT) ;
  /sbin/nameif                          -> $(SEC_CRIT) ;
  /sbin/netreport                       -> $(SEC_CRIT) ;
  /sbin/plipconfig                      -> $(SEC_CRIT) ;
  /sbin/portmap                         -> $(SEC_CRIT) ;
  /sbin/ppp-watch                       -> $(SEC_CRIT) ;
  #/sbin/rarp                            -> $(SEC_CRIT) ;
  /sbin/route                           -> $(SEC_CRIT) ;
  /sbin/slattach                        -> $(SEC_CRIT) ;
  /sbin/tc                              -> $(SEC_CRIT) ;
  #/sbin/uugetty                         -> $(SEC_CRIT) ;
  /sbin/vgetty                          -> $(SEC_CRIT) ;
  /sbin/ypbind                          -> $(SEC_CRIT) ;
}

  ###################################
 #                                 ##
################################### #
#                                 # #
# System Administration Programs # #
#                                 ##
###################################

(
  rulename = "System Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/chkconfig                       -> $(SEC_CRIT) ;
  /sbin/fuser                           -> $(SEC_CRIT) ;
```

```
  /sbin/halt                              -> $(SEC_CRIT) ;
  /sbin/init                              -> $(SEC_CRIT) ;
  /sbin/initlog                           -> $(SEC_CRIT) ;
  /sbin/install-info                      -> $(SEC_CRIT) ;
  /sbin/killall5                          -> $(SEC_CRIT) ;
  /sbin/linuxconf                         -> $(SEC_CRIT) ;
  /sbin/linuxconf-auth                    -> $(SEC_CRIT) ;
  /sbin/pam_tally                         -> $(SEC_CRIT) ;
  /sbin/pwdb_chkpwd                       -> $(SEC_CRIT) ;
  /sbin/remadmin                          -> $(SEC_CRIT) ;
  /sbin/rescuept                          -> $(SEC_CRIT) ;
  /sbin/rmt                               -> $(SEC_CRIT) ;
  /sbin/rpc.lockd                         -> $(SEC_CRIT) ;
  /sbin/rpc.statd                         -> $(SEC_CRIT) ;
  /sbin/rpcdebug                          -> $(SEC_CRIT) ;
  /sbin/service                           -> $(SEC_CRIT) ;
  /sbin/setsysfont                        -> $(SEC_CRIT) ;
  /sbin/shutdown                          -> $(SEC_CRIT) ;
  /sbin/sulogin                           -> $(SEC_CRIT) ;
  /sbin/swapon                            -> $(SEC_CRIT) ;
  /sbin/syslogd                           -> $(SEC_CRIT) ;
  /sbin/unix_chkpwd                       -> $(SEC_CRIT) ;
  /bin/pwd                                -> $(SEC_CRIT) ;
  /bin/uname                              -> $(SEC_CRIT) ;
}

  ########################################
 #                                      ##
######################################## #
#                                      # #
# Hardware and Device Control Programs # #
#                                      ##
########################################
(
  rulename = "Hardware and Device Control Programs",
  severity = $(SIG_HI)
)
{
  /bin/setserial                          -> $(SEC_CRIT) ;
  /bin/sfxload                            -> $(SEC_CRIT) ;
  /sbin/blockdev                          -> $(SEC_CRIT) ;
  /sbin/cardctl                           -> $(SEC_CRIT) ;
  /sbin/cardmgr                           -> $(SEC_CRIT) ;
  /sbin/cbq                               -> $(SEC_CRIT) ;
  /sbin/dump_cis                          -> $(SEC_CRIT) ;
  /sbin/elvtune                           -> $(SEC_CRIT) ;
  /sbin/hotplug                           -> $(SEC_CRIT) ;
  /sbin/hwclock                           -> $(SEC_CRIT) ;
  /sbin/ide_info                          -> $(SEC_CRIT) ;
  /sbin/isapnp                            -> $(SEC_CRIT) ;
  /sbin/kbdrate                           -> $(SEC_CRIT) ;
  /sbin/losetup                           -> $(SEC_CRIT) ;
  /sbin/lspci                             -> $(SEC_CRIT) ;
  /sbin/lspnp                             -> $(SEC_CRIT) ;
  /sbin/mii-tool                          -> $(SEC_CRIT) ;
  /sbin/pack_cis                          -> $(SEC_CRIT) ;
  /sbin/pnpdump                           -> $(SEC_CRIT) ;
  /sbin/probe                             -> $(SEC_CRIT) ;
  /sbin/pump                              -> $(SEC_CRIT) ;
  /sbin/setpci                            -> $(SEC_CRIT) ;
  /sbin/shapecfg                          -> $(SEC_CRIT) ;
}

  ################################
 #                              ##
################################ #
#                              # #
# System Information Programs  # #
#                              ##
################################
```

```
(
  rulename = "System Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/consoletype                    -> $(SEC_CRIT) ;
  /sbin/kernelversion                  -> $(SEC_CRIT) ;
  /sbin/runlevel                       -> $(SEC_CRIT) ;
}

  ###################################
 #                                  ##
################################### #
#                                  # #
# Application Information Programs # #
#                                  ##
###################################

(
  rulename = "Application Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/genksyms                       -> $(SEC_CRIT) ;
  /sbin/genksyms.old                   -> $(SEC_CRIT) ;
  /sbin/rtmon                          -> $(SEC_CRIT) ;
}

  ##########################
 #                        ##
########################## #
#                        # #
# Shell Related Programs # #
#                        ##
##########################
(
  rulename = "Shell Related Programs",
  severity = $(SIG_HI)
)
{
  /sbin/getkey                         -> $(SEC_CRIT) ;
  /sbin/nash                           -> $(SEC_CRIT) ;
  /sbin/sash                           -> $(SEC_CRIT) ;
}


  ################
 #              ##
################ #
#              # #
# OS Utilities # #
#              ##
################
(
  rulename = "Operating System Utilities",
  severity = $(SIG_HI)
)
{
  /bin/arch                            -> $(SEC_CRIT) ;
  /bin/ash                             -> $(SEC_CRIT) ;
  /bin/ash.static                      -> $(SEC_CRIT) ;
  /bin/aumix-minimal                   -> $(SEC_CRIT) ;
  /bin/basename                        -> $(SEC_CRIT) ;
  /bin/cat                             -> $(SEC_CRIT) ;
  /bin/consolechars                    -> $(SEC_CRIT) ;
  /bin/cut                             -> $(SEC_CRIT) ;
  /bin/date                            -> $(SEC_CRIT) ;
  /bin/dd                              -> $(SEC_CRIT) ;
  /bin/df                              -> $(SEC_CRIT) ;
  /bin/dmesg                           -> $(SEC_CRIT) ;
```

```
  /bin/doexec                          -> $(SEC_CRIT) ;
  /bin/echo                            -> $(SEC_CRIT) ;
  /bin/ed                              -> $(SEC_CRIT) ;
  /bin/egrep                           -> $(SEC_CRIT) ;
  /bin/false                           -> $(SEC_CRIT) ;
  /bin/fgrep                           -> $(SEC_CRIT) ;
  /bin/gawk                            -> $(SEC_CRIT) ;
  /bin/gawk-3.1.0                      -> $(SEC_CRIT) ;
  /bin/gettext                         -> $(SEC_CRIT) ;
  /bin/grep                            -> $(SEC_CRIT) ;
  /bin/gunzip                          -> $(SEC_CRIT) ;
  /bin/gzip                            -> $(SEC_CRIT) ;
  /bin/hostname                        -> $(SEC_CRIT) ;
  /bin/igawk                           -> $(SEC_CRIT) ;
  /bin/ipcalc                          -> $(SEC_CRIT) ;
  /bin/kill                            -> $(SEC_CRIT) ;
  /bin/ln                              -> $(SEC_CRIT) ;
  /bin/loadkeys                        -> $(SEC_CRIT) ;
  /bin/login                           -> $(SEC_CRIT) ;
  /bin/ls                              -> $(SEC_CRIT) ;
  /bin/mail                            -> $(SEC_CRIT) ;
  /bin/more                            -> $(SEC_CRIT) ;
  /bin/mt                              -> $(SEC_CRIT) ;
  /bin/mv                              -> $(SEC_CRIT) ;
  /bin/netstat                         -> $(SEC_CRIT) ;
  /bin/nice                            -> $(SEC_CRIT) ;
  /bin/pgawk                           -> $(SEC_CRIT) ;
  /bin/ps                              -> $(SEC_CRIT) ;
  /bin/rpm                             -> $(SEC_CRIT) ;
  /bin/sed                             -> $(SEC_CRIT) ;
  /bin/sleep                           -> $(SEC_CRIT) ;
  /bin/sort                            -> $(SEC_CRIT) ;
  /bin/stty                            -> $(SEC_CRIT) ;
  /bin/su                              -> $(SEC_CRIT) ;
  /bin/sync                            -> $(SEC_CRIT) ;
  /bin/tar                             -> $(SEC_CRIT) ;
  /bin/true                            -> $(SEC_CRIT) ;
  /bin/usleep                          -> $(SEC_CRIT) ;
  /bin/vi                              -> $(SEC_CRIT) ;
  /bin/zcat                            -> $(SEC_CRIT) ;
  /bin/zsh                             -> $(SEC_CRIT) ;
  /bin/zsh-4.0.2                       -> $(SEC_CRIT) ;
  /sbin/sln                            -> $(SEC_CRIT) ;
  /usr/bin/vimtutor                    -> $(SEC_CRIT) ;
}

  ##############################
 #                            ##
############################## #
#                            # #
# Critical Utility Sym-Links # #
#                            ##
##############################
(
  rulename = "Critical Utility Sym-Links",
  severity = $(SIG_HI)
)
{
  /sbin/askrunlevel                    -> $(SEC_CRIT) ;
  /sbin/clock                          -> $(SEC_CRIT) ;
  /sbin/fixperm                        -> $(SEC_CRIT) ;
  /sbin/fsck.reiserfs                  -> $(SEC_CRIT) ;
  /sbin/fsconf                         -> $(SEC_CRIT) ;
  /sbin/ipfwadm-wrapper                -> $(SEC_CRIT) ;
  /sbin/kallsyms                       -> $(SEC_CRIT) ;
  /sbin/ksyms                          -> $(SEC_CRIT) ;
  /sbin/lsmod                          -> $(SEC_CRIT) ;
  /sbin/mailconf                       -> $(SEC_CRIT) ;
  /sbin/mkfs.reiserfs                  -> $(SEC_CRIT) ;
  /sbin/modemconf                      -> $(SEC_CRIT) ;
```

```
  /sbin/modprobe                          -> $(SEC_CRIT) ;
  /sbin/mount.ncp                         -> $(SEC_CRIT) ;
  /sbin/mount.ncpfs                       -> $(SEC_CRIT) ;
  /sbin/mount.smb                         -> $(SEC_CRIT) ;
  /sbin/mount.smbfs                       -> $(SEC_CRIT) ;
  /sbin/netconf                           -> $(SEC_CRIT) ;
  /sbin/pidof                             -> $(SEC_CRIT) ;
  /sbin/poweroff                          -> $(SEC_CRIT) ;
  /sbin/quotaoff                          -> $(SEC_CRIT) ;
  /sbin/raid0run                          -> $(SEC_CRIT) ;
  /sbin/raidhotadd                        -> $(SEC_CRIT) ;
  /sbin/raidhotgenerateerror              -> $(SEC_CRIT) ;
  /sbin/raidhotremove                     -> $(SEC_CRIT) ;
  /sbin/raidstop                          -> $(SEC_CRIT) ;
  /sbin/rdump                             -> $(SEC_CRIT) ;
  /sbin/rdump.static                      -> $(SEC_CRIT) ;
  /sbin/reboot                            -> $(SEC_CRIT) ;
  /sbin/rmmod                             -> $(SEC_CRIT) ;
  /sbin/rrestore                          -> $(SEC_CRIT) ;
  /sbin/rrestore.static                   -> $(SEC_CRIT) ;
  /sbin/swapoff                           -> $(SEC_CRIT) ;
  /sbin/telinit                           -> $(SEC_CRIT) ;
  /sbin/userconf                          -> $(SEC_CRIT) ;
  /sbin/uucpconf                          -> $(SEC_CRIT) ;
  /sbin/vregistry                         -> $(SEC_CRIT) ;
  /bin/awk                                -> $(SEC_CRIT) ;
  /bin/bash2                              -> $(SEC_CRIT) ;
  /bin/bsh                                -> $(SEC_CRIT) ;
  /bin/csh                                -> $(SEC_CRIT) ;
  /bin/dnsdomainname                      -> $(SEC_CRIT) ;
  /bin/domainname                         -> $(SEC_CRIT) ;
  /bin/ex                                 -> $(SEC_CRIT) ;
  /bin/gtar                               -> $(SEC_CRIT) ;
  /bin/nisdomainname                      -> $(SEC_CRIT) ;
  /bin/red                                -> $(SEC_CRIT) ;
  /bin/rvi                                -> $(SEC_CRIT) ;
  /bin/rview                              -> $(SEC_CRIT) ;
  /bin/view                               -> $(SEC_CRIT) ;
  /bin/ypdomainname                       -> $(SEC_CRIT) ;
}


  #########################
 #                       ##
########################## #
#                       # #
# Temporary directories # #
#                       ##
#########################
(
  rulename = "Temporary directories",
  recurse = false,
  severity = $(SIG_LOW)
)
{
  /usr/tmp                                -> $(SEC_INVARIANT) ;
  /var/tmp                                -> $(SEC_INVARIANT) ;
  /tmp                                    -> $(SEC_INVARIANT) ;
}

  ###############
 #             ##
############### #
#             # #
# Local files # #
#             ##
###############
(
  rulename = "User binaries",
  severity = $(SIG_MED)
```

```
)
{
  /sbin                                -> $(SEC_BIN) (recurse = 1) ;
  /usr/bin                             -> $(SEC_BIN) (recurse = 1) ;
  /usr/sbin                            -> $(SEC_BIN) (recurse = 1) ;
  /usr/local/bin                       -> $(SEC_BIN) (recurse = 1) ;
}

(
  rulename = "Shell Binaries",
  severity = $(SIG_HI)
)
{
  /bin/bash                            -> $(SEC_BIN) ;
  /bin/ksh                             -> $(SEC_BIN) ;
  # /bin/psh                             -> $(SEC_BIN) ; # No longer used?
  # /bin/Rsh                             -> $(SEC_BIN) ; # No longer used?
  /bin/sh                              -> $(SEC_BIN) ;
  # /bin/shell                           -> $(SEC_SUID) ; # No longer used?
  # /bin/tsh                             -> $(SEC_BIN) ; # No longer used?
  /bin/tcsh                            -> $(SEC_BIN) ;
  /sbin/nologin                        -> $(SEC_BIN) ;
}

(
  rulename = "Security Control",
  severity = $(SIG_HI)
)
{
  /etc/group                           -> $(SEC_CRIT) ;
  /etc/security                        -> $(SEC_CRIT) ;
  #/var/spool/cron/crontabs             -> $(SEC_CRIT) ; # Uncomment when this file exists
}

#(
#  rulename = "Boot Scripts",
#  severity = $(SIG_HI)
#)
#{
#  /etc/rc                              -> $(SEC_CONFIG) ;
#  /etc/rc.bsdnet                       -> $(SEC_CONFIG) ;
#  /etc/rc.dt                           -> $(SEC_CONFIG) ;
#  /etc/rc.net                          -> $(SEC_CONFIG) ;
#  /etc/rc.net.serial                   -> $(SEC_CONFIG) ;
#  /etc/rc.nfs                          -> $(SEC_CONFIG) ;
#  /etc/rc.powerfail                    -> $(SEC_CONFIG) ;
#  /etc/rc.tcpip                        -> $(SEC_CONFIG) ;
#  /etc/trcfmt.Z                        -> $(SEC_CONFIG) ;
#}

(
  rulename = "Login Scripts",
  severity = $(SIG_HI)
)
{
  /etc/bashrc                          -> $(SEC_CONFIG) ;
  /etc/csh.cshrc                       -> $(SEC_CONFIG) ;
  /etc/csh.login                       -> $(SEC_CONFIG) ;
  /etc/inputrc                         -> $(SEC_CONFIG) ;
  # /etc/tsh_profile                     -> $(SEC_CONFIG) ; #Uncomment when this file exists
  /etc/profile                         -> $(SEC_CONFIG) ;
}

# Libraries
(
  rulename = "Libraries",
  severity = $(SIG_MED)
)
{
  /usr/lib                             -> $(SEC_BIN) ;
```

```
  /usr/local/lib                          -> $(SEC_BIN) ;
}


  ########################################################
 #                                                       ##
##########################################################  #
#                                                       #  #
# Critical System Boot Files                            #  #
# These files are critical to a correct system boot.    #  #
#                                                       ##
##########################################################

(
  rulename = "Critical system boot files",
  severity = $(SIG_HI)
)
{
     /boot                                -> $(SEC_CRIT) ;
     #/sbin/devfsd                        -> $(SEC_CRIT) ;
     /sbin/grub                           -> $(SEC_CRIT) ;
     /sbin/grub-install                   -> $(SEC_CRIT) ;
     /sbin/grub-md5-crypt                 -> $(SEC_CRIT) ;
     /sbin/installkernel                  -> $(SEC_CRIT) ;
     /sbin/lilo                           -> $(SEC_CRIT) ;
     /sbin/mkkerneldoth                   -> $(SEC_CRIT) ;
     !/boot/System.map ;
     !/boot/module-info ;
     /usr/share/grub/i386-redhat/e2fs_stage1_5       -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/fat_stage1_5        -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/ffs_stage1_5        -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/minix_stage1_5      -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/reiserfs_stage1_5   -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/stage1              -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/stage2              -> $(SEC_CRIT) ;
     /usr/share/grub/i386-redhat/vstafs_stage1_5     -> $(SEC_CRIT) ;
     # other boot files may exist.  Look for:
     #/ufsboot                             -> $(SEC_CRIT) ;
}
   ####################################################
  ####################################################
  # These files change every time the system boots ##
  ####################################################
(
  rulename = "System boot changes",
  severity = $(SIG_HI)
)
{
     !/var/run/ftp.pids-all ; # Comes and goes on reboot.
     !/root/.enlightenment ;
     /dev/log                             -> $(SEC_CONFIG) ;
     /dev/cua0                            -> $(SEC_CONFIG) ;
     # /dev/printer                           -> $(SEC_CONFIG) ; # Uncomment if you have a printer
device
     /dev/console                          -> $(SEC_CONFIG) -u ; # User ID may change on console
login/logout.
     /dev/tty1                            -> $(SEC_CONFIG) ; # tty devices
     /dev/tty2                            -> $(SEC_CONFIG) ; # tty devices
     /dev/tty3                            -> $(SEC_CONFIG) ; # are extremely
     /dev/tty4                            -> $(SEC_CONFIG) ; # variable
     /dev/tty5                            -> $(SEC_CONFIG) ;
     /dev/tty6                            -> $(SEC_CONFIG) ;
     /dev/urandom                         -> $(SEC_CONFIG) ;
     /dev/initctl                         -> $(SEC_CONFIG) ;
     /var/lock/subsys                     -> $(SEC_CONFIG) ;
     /var/lock/subsys/amd                 -> $(SEC_CONFIG) ;
     /var/lock/subsys/anacron             -> $(SEC_CONFIG) ;
     /var/lock/subsys/apmd                -> $(SEC_CONFIG) ;
     /var/lock/subsys/arpwatch            -> $(SEC_CONFIG) ;
     /var/lock/subsys/atd                 -> $(SEC_CONFIG) ;
```

```
/var/lock/subsys/autofs          -> $(SEC_CONFIG) ;
/var/lock/subsys/bcm5820         -> $(SEC_CONFIG) ;
/var/lock/subsys/bgpd            -> $(SEC_CONFIG) ;
/var/lock/subsys/bootparamd      -> $(SEC_CONFIG) ;
/var/lock/subsys/canna           -> $(SEC_CONFIG) ;
/var/lock/subsys/crond           -> $(SEC_CONFIG) ;
/var/lock/subsys/cWnn            -> $(SEC_CONFIG) ;
/var/lock/subsys/dhcpd           -> $(SEC_CONFIG) ;
/var/lock/subsys/firewall        -> $(SEC_CONFIG) ;
/var/lock/subsys/freeWnn         -> $(SEC_CONFIG) ;
/var/lock/subsys/gated           -> $(SEC_CONFIG) ;
/var/lock/subsys/gpm             -> $(SEC_CONFIG) ;
/var/lock/subsys/httpd           -> $(SEC_CONFIG) ;
/var/lock/subsys/identd          -> $(SEC_CONFIG) ;
/var/lock/subsys/innd            -> $(SEC_CONFIG) ;
/var/lock/subsys/ipchains        -> $(SEC_CONFIG) ;
/var/lock/subsys/iptables        -> $(SEC_CONFIG) ;
/var/lock/subsys/ipvsadm         -> $(SEC_CONFIG) ;
/var/lock/subsys/irda            -> $(SEC_CONFIG) ;
/var/lock/subsys/iscsi           -> $(SEC_CONFIG) ;
/var/lock/subsys/isdn            -> $(SEC_CONFIG) ;
/var/lock/subsys/junkbuster      -> $(SEC_CONFIG) ;
/var/lock/subsys/kadmin          -> $(SEC_CONFIG) ;
/var/lock/subsys/keytable        -> $(SEC_CONFIG) ;
/var/lock/subsys/kprop           -> $(SEC_CONFIG) ;
/var/lock/subsys/krb524          -> $(SEC_CONFIG) ;
/var/lock/subsys/krb5kdc         -> $(SEC_CONFIG) ;
/var/lock/subsys/kudzu           -> $(SEC_CONFIG) ;
/var/lock/subsys/kWnn            -> $(SEC_CONFIG) ;
/var/lock/subsys/ldap            -> $(SEC_CONFIG) ;
/var/lock/subsys/linuxconf       -> $(SEC_CONFIG) ;
/var/lock/subsys/lpd             -> $(SEC_CONFIG) ;
/var/lock/subsys/mars_nwe        -> $(SEC_CONFIG) ;
/var/lock/subsys/mcserv          -> $(SEC_CONFIG) ;
/var/lock/subsys/mysqld          -> $(SEC_CONFIG) ;
/var/lock/subsys/named           -> $(SEC_CONFIG) ;
/var/lock/subsys/netfs           -> $(SEC_CONFIG) ;
/var/lock/subsys/network         -> $(SEC_CONFIG) ;
/var/lock/subsys/nfs             -> $(SEC_CONFIG) ;
/var/lock/subsys/nfslock         -> $(SEC_CONFIG) ;
/var/lock/subsys/nscd            -> $(SEC_CONFIG) ;
/var/lock/subsys/ntpd            -> $(SEC_CONFIG) ;
/var/lock/subsys/ospf6d          -> $(SEC_CONFIG) ;
/var/lock/subsys/ospfd           -> $(SEC_CONFIG) ;
/var/lock/subsys/pcmcia          -> $(SEC_CONFIG) ;
/var/lock/subsys/portmap         -> $(SEC_CONFIG) ;
/var/lock/subsys/postgresql      -> $(SEC_CONFIG) ;
/var/lock/subsys/pxe             -> $(SEC_CONFIG) ;
/var/lock/subsys/radvd           -> $(SEC_CONFIG) ;
/var/lock/subsys/random          -> $(SEC_CONFIG) ;
/var/lock/subsys/rarpd           -> $(SEC_CONFIG) ;
/var/lock/subsys/reconfig        -> $(SEC_CONFIG) ;
/var/lock/subsys/rhnsd           -> $(SEC_CONFIG) ;
/var/lock/subsys/ripd            -> $(SEC_CONFIG) ;
/var/lock/subsys/ripngd          -> $(SEC_CONFIG) ;
/var/lock/subsys/routed          -> $(SEC_CONFIG) ;
/var/lock/subsys/rstatd          -> $(SEC_CONFIG) ;
/var/lock/subsys/rusersd         -> $(SEC_CONFIG) ;
/var/lock/subsys/rwalld          -> $(SEC_CONFIG) ;
/var/lock/subsys/rwhod           -> $(SEC_CONFIG) ;
/var/lock/subsys/sendmail        -> $(SEC_CONFIG) ;
/var/lock/subsys/smb             -> $(SEC_CONFIG) ;
/var/lock/subsys/snmpd           -> $(SEC_CONFIG) ;
/var/lock/subsys/squid           -> $(SEC_CONFIG) ;
/var/lock/subsys/sshd            -> $(SEC_CONFIG) ;
/var/lock/subsys/syslog          -> $(SEC_CONFIG) ;
/var/lock/subsys/tux             -> $(SEC_CONFIG) ;
/var/lock/subsys/tWnn            -> $(SEC_CONFIG) ;
/var/lock/subsys/ups             -> $(SEC_CONFIG) ;
/var/lock/subsys/vncserver       -> $(SEC_CONFIG) ;
```

```
     /var/lock/subsys/wine              -> $(SEC_CONFIG) ;
     /var/lock/subsys/xfs               -> $(SEC_CONFIG) ;
     /var/lock/subsys/xinetd            -> $(SEC_CONFIG) ;
     /var/lock/subsys/ypbind            -> $(SEC_CONFIG) ;
     /var/lock/subsys/yppasswdd         -> $(SEC_CONFIG) ;
     /var/lock/subsys/ypserv            -> $(SEC_CONFIG) ;
     /var/lock/subsys/ypxfrd            -> $(SEC_CONFIG) ;
     /var/lock/subsys/zebra             -> $(SEC_CONFIG) ;
     /var/run                           -> $(SEC_CONFIG) ;
     /var/log                           -> $(SEC_CONFIG) ;
     /etc/ioctl.save                    -> $(SEC_CONFIG) ;
     /etc/issue.net                     -> $(SEC_CONFIG) -i ; # Inode number changes
     /etc/issue                         -> $(SEC_CONFIG) ;
     /etc/mtab                               -> $(SEC_CONFIG) -i ; # Inode number changes on any
mount/unmount
     /lib/modules                       -> $(SEC_CONFIG) ;
     /etc/.pwd.lock                     -> $(SEC_CONFIG) ;
     # /lib/modules/preferred             -> $(SEC_CONFIG) ; #Uncomment when this file exists
}

# These files change the behavior of the root account
(
  rulename = "Root config files",
  severity = 100
)
{
     /root                              -> $(SEC_CRIT) ; # Catch all additions to /root
     /root/.Xresources                  -> $(SEC_CONFIG) ;
     /root/.bashrc                      -> $(SEC_CONFIG) ;
     /root/.bash_profile                -> $(SEC_CONFIG) ;
     /root/.bash_logout                 -> $(SEC_CONFIG) ;
     /root/.cshrc                       -> $(SEC_CONFIG) ;
     /root/.tcshrc                      -> $(SEC_CONFIG) ;
     /root/Mail                         -> $(SEC_CONFIG) ;
     /root/mail                         -> $(SEC_CONFIG) ;
     /root/.amandahosts                 -> $(SEC_CONFIG) ;
     /root/.addressbook.lu              -> $(SEC_CONFIG) ;
     /root/.addressbook                 -> $(SEC_CONFIG) ;
     /root/.bash_history                -> $(SEC_CONFIG) ;
     /root/.elm                         -> $(SEC_CONFIG) ;
     /root/.esd_auth                    -> $(SEC_CONFIG) ;
     /root/.gnome_private               -> $(SEC_CONFIG) ;
     /root/.gnome-desktop               -> $(SEC_CONFIG) ;
     /root/.gnome                       -> $(SEC_CONFIG) ;
     /root/.ICEauthority                -> $(SEC_CONFIG) ;
     /root/.mc                          -> $(SEC_CONFIG) ;
     /root/.pinerc                      -> $(SEC_CONFIG) ;
     /root/.sawfish                     -> $(SEC_CONFIG) ;
     /root/.Xauthority                  -> $(SEC_CONFIG) -i ; # Changes Inode number on login
     /root/.xauth                       -> $(SEC_CONFIG) ;
     /root/.xsession-errors             -> $(SEC_CONFIG) ;
}

  ################################
 #                              ##
################################ #
#                              # #
# Critical configuration files # #
#                              ##
################################
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI)
)
{
     /etc/conf.linuxconf                -> $(SEC_BIN) ;
     /etc/crontab                       -> $(SEC_BIN) ;
     /etc/cron.hourly                   -> $(SEC_BIN) ;
     /etc/cron.daily                    -> $(SEC_BIN) ;
     /etc/cron.weekly                   -> $(SEC_BIN) ;
```

```
    /etc/cron.monthly                -> $(SEC_BIN) ;
    /etc/default                     -> $(SEC_BIN) ;
    /etc/fstab                       -> $(SEC_BIN) ;
    /etc/exports                     -> $(SEC_BIN) ;
    /etc/group-                      -> $(SEC_BIN) ;  # changes should be infrequent
    /etc/host.conf                   -> $(SEC_BIN) ;
    /etc/hosts.allow                 -> $(SEC_BIN) ;
    /etc/hosts.deny                  -> $(SEC_BIN) ;
    /etc/httpd/conf                  -> $(SEC_BIN) ;  # changes should be infrequent
    /etc/protocols                   -> $(SEC_BIN) ;
    /etc/services                    -> $(SEC_BIN) ;
    /etc/rc.d/init.d                 -> $(SEC_BIN) ;
    /etc/rc.d                        -> $(SEC_BIN) ;
    /etc/mail.rc                     -> $(SEC_BIN) ;
    /etc/modules.conf                -> $(SEC_BIN) ;
    /etc/motd                        -> $(SEC_BIN) ;
    /etc/named.conf                  -> $(SEC_BIN) ;
    /etc/passwd                      -> $(SEC_CONFIG) ;
    /etc/passwd-                     -> $(SEC_CONFIG) ;
    /etc/profile.d                   -> $(SEC_BIN) ;
    /var/lib/nfs/rmtab               -> $(SEC_BIN) ;
    /usr/sbin/fixrmtab               -> $(SEC_BIN) ;
    /etc/rpc                         -> $(SEC_BIN) ;
    /etc/sysconfig                   -> $(SEC_BIN) ;
    /etc/samba/smb.conf              -> $(SEC_CONFIG) ;
    #/etc/gettydefs                   -> $(SEC_BIN) ;
    /etc/nsswitch.conf               -> $(SEC_BIN) ;
    /etc/yp.conf                     -> $(SEC_BIN) ;
    /etc/hosts                       -> $(SEC_CONFIG) ;
    /etc/xinetd.conf                 -> $(SEC_CONFIG) ;
    /etc/inittab                     -> $(SEC_CONFIG) ;
    /etc/resolv.conf                 -> $(SEC_CONFIG) ;
    /etc/syslog.conf                 -> $(SEC_CONFIG) ;
)

  ####################
 #                    ##
#################### #
#                   # #
# Critical devices  # #
#                   ##
####################
(
  rulename = "Critical devices",
  severity = ${SIG_HI},
  recurse = false
)
{
    /dev/kmem                        -> $(Device) ;
    /dev/mem                         -> $(Device) ;
    /dev/null                        -> $(Device) ;
    /dev/zero                        -> $(Device) ;
    /proc/devices                    -> $(Device) ;
    /proc/net                        -> $(Device) ;
    /proc/sys                        -> $(Device) ;
    /proc/cpuinfo                    -> $(Device) ;
    /proc/modules                    -> $(Device) ;
    /proc/mounts                     -> $(Device) ;
    /proc/dma                        -> $(Device) ;
    /proc/filesystems                -> $(Device) ;
    /proc/pci                        -> $(Device) ;
    /proc/interrupts                 -> $(Device) ;
    /proc/driver/rtc                 -> $(Device) ;
    /proc/ioports                    -> $(Device) ;
    /proc/scsi                       -> $(Device) ;
    /proc/kcore                      -> $(Device) ;
    /proc/self                       -> $(Device) ;
    /proc/kmsg                       -> $(Device) ;
    /proc/stat                       -> $(Device) ;
    /proc/ksyms                      -> $(Device) ;
```

```
    /proc/loadavg                   -> $(Device) ;
    /proc/uptime                    -> $(Device) ;
    /proc/locks                     -> $(Device) ;
    /proc/version                   -> $(Device) ;
    /proc/mdstat                    -> $(Device) ;
    /proc/meminfo                   -> $(Device) ;
    /proc/cmdline                   -> $(Device) ;
    /proc/misc                      -> $(Device) ;
}

# Rest of critical system binaries
(
  rulename = "OS executables and libraries",
  severity = $(SIG_HI)
)
{
    /bin                            -> $(SEC_BIN) ;
    /lib                            -> $(SEC_BIN) ;
}

#===============================================================================
#
# Copyright 2000 Tripwire, Inc. Tripwire is a registered trademark of Tripwire,
# Inc. in the United States and other countries. All rights reserved.
#
# Linux is a registered trademark of Linus Torvalds.
#
# UNIX is a registered trademark of The Open Group.
#
#===============================================================================
#
# Permission is granted to make and distribute verbatim copies of this document
# provided the copyright notice and this permission notice are preserved on all
# copies.
#
# Permission is granted to copy and distribute modified versions of this
# document under the conditions for verbatim copying, provided that the entire
# resulting derived work is distributed under the terms of a permission notice
# identical to this one.
#
# Permission is granted to copy and distribute translations of this document
# into another language, under the above conditions for modified versions,
# except that this permission notice may be stated in a translation approved by
# Tripwire, Inc.
#
# DCM
```

Código 28 Archivo de políticas de Tripwire.

Logcheck

Descripción

Son programas que se encargan de implementar un esquema formal de auditoría de sistemas. Adicionalmente, se encargan de monitorear automática y periódicamente las bitácoras del sistema y de detectar y avisar sobre las violaciones de seguridad que detectan (código 29, 30, 31, y 32).

Configuración

```
"wiz"
"WIZ"
"debug"
"DEBUG"
ATTACK
nested
```

```
VRFY bbs
VRFY decode
VRFY uudecode
VRFY lp
VRFY demo
VRFY guest
VRFY root
VRFY uucp
VRFY oracle
VRFY sybase
VRFY games
vrfy bbs
vrfy decode
vrfy uudecode
vrfy lp
vrfy demo
vrfy guest
vrfy root
vrfy uucp
vrfy oracle
vrfy sybase
vrfy games
expn decode
expn uudecode
expn wheel
expn root
EXPN decode
EXPN uudecode
EXPN wheel
EXPN root
LOGIN root REFUSED
rlogind.*: Connection from .* on illegal port
rshd.*: Connection from .* on illegal port
sendmail.*: user .* attempted to run daemon
uucico.*: refused connect from .*
tftpd.*: refused connect from .*
login.*: .*LOGIN FAILURE.* FROM .*root
login.*: .*LOGIN FAILURE.* FROM .*guest
login.*: .*LOGIN FAILURE.* FROM .*bin
login.*: .*LOGIN FAILURE.* FROM .*uucp
login.*: .*LOGIN FAILURE.* FROM .*adm
login.*: .*LOGIN FAILURE.* FROM .*bbs
login.*: .*LOGIN FAILURE.* FROM .*games
login.*: .*LOGIN FAILURE.* FROM .*sync
login.*: .*LOGIN FAILURE.* FROM .*oracle
login.*: .*LOGIN FAILURE.* FROM .*sybase
kernel: Oversized packet received from
attackalert
```

Código 29 Configuración de *logcheck*, hacking.

```
authsrv.*AUTHENTICATE
cron.*CMD
cron.*RELOAD
cron.*STARTUP
ftp-gw.*: exit host
ftp-gw.*: permit host
ftpd.*ANONYMOUS FTP LOGIN
ftpd.*FTP LOGIN FROM
ftpd.*retrieved
ftpd.*stored
http-gw.*: exit host
http-gw.*: permit host
mail.local
named.*Lame delegation
named.*Response from
named.*answer queries
```

```
named.*points to a CNAME
named.*reloading
named.*starting
netacl.*: exit host
netacl.*: permit host
popper.*Unable
popper: -ERR POP server at
popper: -ERR Unknown command: "uidl".
qmail.*new msg
qmail.*info msg
qmail.*starting delivery
qmail.*delivery
qmail.*end msg
rlogin-gw.*: exit host
rlogin-gw.*: permit host
sendmail.*User Unknown
sendmail.*User Unknown
sendmail.*alias database.*rebuilt
sendmail.*aliases.*longest
sendmail.*from=
sendmail.*lost input channel
sendmail.*message-id=
sendmail.*putoutmsg
sendmail.*return to sender
sendmail.*return to sender
sendmail.*stat=
sendmail.*timeout waiting
smap.*host=
smapd.*daemon running
smapd.*daemon running
smapd.*delivered
smapd.*delivered
telnetd.*ttloop:  peer died
tn-gw.*: exit host
tn-gw.*: permit host
x-gw.*: exit host
x-gw.*: permit host
xntpd.*Previous time adjustment didn't complete
xntpd.*time reset
root 1
```

Código 30 Configuración de *logcheck*, ignore.

```
!=
-ERR Password
ATTACK
BAD
CWD etc
DEBUG
EXPN
FAILURE
ILLEGAL
LOGIN FAILURE
LOGIN REFUSED
PERMITTED
REFUSED
RETR group
RETR passwd
RETR pwd.db
ROOT LOGIN
SITE EXEC
VRFY
"WIZ"
admin
alias database
debug
denied
```

```
deny
deny host
expn
failed
illegal
kernel: Oversized packet received from
nested
permitted
reject
rexec
rshd
securityalert
setsender
shutdown
smrsh
su root
su:
sucked
unapproved
vrfy
attackalert
```

Código 31 Configuración de *logcheck*, violations.

```
stat=Deferred
```

Código 32 Configuración de *logcheck*, violations ignore.

ssh

Descripción

Secure Shell (ssh) es un servicio que permite establecer una sesión interactiva remota con un servidor asegurándose de que la información que viaja entre ambos puntos lo hace de manera cifrada, evitando así que se puedan interceptar clave o información. Sobre este mismo protocolo se tienen otros servicios como la copia remota de archivos o la ejecución remota de comandos.

Como parte del esquema de seguridad y como una funcionalidad para mover archivos en forma cifrada al interior de la red de servidores se ha instalado y configurado (código 33) el servicio de sshd. Como una medida adicional nos aseguramos de que sólo se hacen conexiones utilizando el protocolo ssh2, ya que a la versión 1 se le conocen algunas debilidades que lo pueden hacer vulnerable.

Configuración

```
#       $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
```

```
Protocol 2
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
#PermitRootLogin yes
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile    .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
```

```
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
#Banner /some/path
#VerifyReverseMapping no

# override default of no subsystems
Subsystem      sftp    /usr/libexec/openssh/sftp-server
```

Código 33 Configuración de *sshd*.

GRUB

Descripción

GRUB es la herramienta encargada del arranque del sistema, más específicamente es la herramienta encargada de la carga inicial del sistema operativo. Tiene la capacidad de administrar equipos en los que se encuentren instalados varios sistemas operativos simultáneamente, además puede permitir varias configuraciones para un mismo sistema operativo.

Debido a que es posible tanto iniciar el sistema en modo de mantenimiento, donde no nos requerirá de una clave para darnos acceso a la cuenta del administrador, como deshabilitar LIDS, a través del paso de parámetros al momento de la carga inicial del sistema operativo, se vuelve indispensable proteger con una clave la configuración y el paso de parámetros. Para ello utilizaremos una configuración (código 34) de grub que requiera de una clave para realizar cambios y que tenga por omisión una configuración que levanta el equipo con LIDS activado.

Configuración

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
password $1$U$JK7xFegdxWH6VuppCUSIb. /boot/grub/menu-admin.lst
title Red Hat Linux (2.4.7-10)
        root (hd0,0)
        kernel /vmlinuz-2.4.7-10 ro root=/dev/hda2
        initrd /initrd-2.4.7-10.img
        lock
title Red Hat Linux (2.4.16)
        root (hd0,0)
        kernel /vmlinuz-2.4.16 ro root=/dev/hda2
```

Código 34 Archivo *grub.conf* encargado del control del sistema de carga del sistema operativo.

Aplicaciones

Libsafe

Descripción

El siguiente componente dentro de nuestro sistema de seguridad es libsafe.

libsafe es una herramienta para contener los ataques que se basan en la explotación de dos debilidades conocidas de los programas como *buffer overflow* y *format string*[xxv], ambas afectan las pilas de los procesos, ambas son también muy comunes en los ataque que se han producido recientemente.

Lo que hace libsafe es implementar un nuevo método de detección y manejo de dichos ataques. En contraste con los métodos disponibles anteriormente con este método no se necesita tener acceso o modificar el código fuente de los programas que queremos proteger, esta ventaja le da la posibilidad de proteger servidores completos y no sólo aquellos programas que han sido modificados para estar protegidos. Otras ventajas son el que el no requiere modificaciones al sistema operativo, sino que se integra a él sin necesidades especiales, ni tampoco requiere el procesamiento especial o fuera de línea de los binarios del servidor o la recompilación de ellos. La solución es un sistema tipo middleware que intercepta todas las llamadas de función hechas a las distintas bibliotecas. En el proceso de intercepción se substituyen todas aquellas funciones de las que se sabe que son vulnerables por versiones de las mismas que han sido programadas de tal forma que no presentan ya dicha vulnerabilidad. Esto impide que un atacante utilice las técnicas conocidas de ataque. Además, el componente contiene dichos intentos impidiendo que se reescriba la pila de los procesos o que se redefinan dinámicamente los puntos de retorno de las funciones.

Con este mecanismo no sólo se previenen los ataques que ya se conocen, sino también aquéllos que aún no han sido descubiertos, puesto que lo que estamos haciendo es substituir las rutinas defectuosas en las bibliotecas, que pueden utilizar muchas aplicaciones distintas, por rutinas que han sido programadas eliminado las vulnerabilidades. Todo esto sin que el hecho de hacer pasar todas las llamadas a sistema por libsafe afecte de forma perceptible el desempeño del sistema. Todo esto es posible gracias al alto grado de estandarización que existe en las bibliotecas de los sistemas operativos tipo Unix.

Como es sabido, la mejor manera de corregir una vulnerabilidad tipo *buffer overflow* y *format string* es modificando el código de la aplicación que tiene el problema. Sin embargo, para poder arreglar un programa es necesario saber que tiene un problema de este tipo. Esto hace de libsafe una solución generalizada que tiene muy buenos resultados aun cuando se desconozca qué programas tienen el problema. Otra ventaja de libsafe es que su instalación es muy simple, y rápida y no requiere un mantenimiento o una actualización permanente. Es muy importante señalar que libsafe está enfocado a proteger sistemas que utilizan glibc.

Configuración

Con libsafe más que una configuración (código 35) lo que tenemos es una instalación.

```
En el  archivo
/etc/ld.so.preload

Agregar la linea
/lib/libsafe.so.2
```

Código 35 Configuración de *libsafe*.

Como nuestros sistemas de administración de contenido y de transacciones bancarias estarán ambos escritos en PHP, y PHP es normalmente un lenguaje interpretado, resulta que el código fuente está siempre disponible cuando la aplicación corre. Dado que tener el código fuente disponible y a la vista de cualquiera que pudiera lograr una intrusión resulta peligroso, se decidió recurrir a las herramientas de Zend para lograr la compilación código fuente de la aplicación.

Y en términos de programación, aparte de haber auditado el código por parte de las herramientas de Zend y de todos los miembros del equipo de BB, se implementó la caducidad de sesión, para que se minimice el riesgo de que una sesión donde un usuario ya se haya autenticado sea secuestrada[xxvi] o se quede inadvertidamente disponible.

Cabe resaltar que los programas (código 36) que forman parte de eZ Publish así como los desarrollados para el IVA fueron compilados y codificados (código 37) utilizando Zend Encoder.

```
<?php
//
// $Id: datasupplier.php,v 1.3 2001/07/19 12:48:35 jakobn Exp $
//
// Created on: <23-Oct-2000 17:53:46 bf>
//
// This source file is part of IVA.
//
// Copyright (C) 1997-2004 Internet de Alta Calidad, S.A. de C.V.  All rights reserved.
//
// Programó: Sebastián Mantilla Beniers
//
// This program is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation; either version 2
// of the License, or (at your option) any later version.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with this program; if not, write to the Free Software
// Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, US
//

switch ( $url_array[2] )
{
    case "catálogo":
    {
        include( "eztasas/admin/catálogo.php" );
    }
```

```
    break;

    case "vigencia":
    {
        include( "eztasas/admin/vigencia.php" );
    }
    break;

    default :
    {
        // go to default module page or show an error message
        print( "Error: your page request was not found" );
    }
}
?>
```

Código 36 Código antes de compilar (datasupplier eZTasas).


```
 2002062301▮▮1▮▮356▮▮887▮xù
▮2▮▮W½NÃ0▮6[¥ }▮#ö6©▮'eç%X▮Õ▮▮®±#'▮▮▮▮▮Wá)▮▮Q▮▮SÀñolD▮▮ë³Ow>ß}ßMÎÿº
9¾¢▮ÑpA¦▮9ªÐTöE8J÷»8Ã»dúGx▮`±▮R▮ä}]▮k'ç\ó:P
gR▮▮¼,Ô▮ö?öÏaõion▮$]ÃOFbÊþ▮▮]ù2Ã▮ÀA¤ùEJ& e▮[S▮£3k#▮ozR2´▮▮â±#-i7$¯+º1¶ÖÎ]³P[õ▮▮M<r▮ñâ▮¹▮uh▮µHÞø▮ç÷
UYÐCEö¶-Àó)MÎÈÀ?®▮cië▮¤ ▮ZÜ▮I▮
bä▮Î^£ç^%I|pö▮Z▮:ç▮_Å▮õ▮6¤ ´Ã Qvõ▮ ▮²▮Þ²▮«s+▮ÜKq▮ ▮_ ¼KlÜi
w3ôS£óZ¶à ^úmMÃ®RÆ{K ª2▮Ê▮tuC8'Ã2N▮¼▮0▮mùEà▮áDw«
```


Código 37 Código compilado (datasupplier eZTasas).

Datos

En el sistema integral de banca por Internet tenemos dos tipos de datos: aquéllos concernientes a las transacciones financieras que se están realizando y aquéllos relativos a la información de productos y servicios del Banco. Por su naturaleza y por perseguir objetivos de protección distintos, requieren tratamientos distintos.

Veamos primero los datos de productos y servicios del banco. Nuestro objetivo aquí es evitar que sean modificados. Obviamente, a ningún banco le gustaría ver su página afectada por el vandalismo de algún intruso.

Como la información de productos y servicios del banco está almacenada en la base de datos del sistema de administración de contenido, lo que tenemos que hacer es restringir el acceso a la base de datos de forma que su modificación no sea viable.

Sabemos que la base de datos, MySQL, nos ofrece la capacidad de definir permisos de acceso a nivel base, tabla y equipo. Definiremos entonces que sólo usuarios con clave y conectados desde el mismo equipo podrán tener acceso al servidor de bases de datos. Adicionalmente diremos que sólo un usuario con una clave definida para cumplir con los más altos estándares de seguridad[xxvii] puede tener acceso a la base de datos del sistema. Configuraremos también al motor de bases de datos para que guarde la información de las claves de los usuarios utilizando el algoritmo md5, así, si alguna llegara a ser comprometida, no será posible obtener la clave sino sólo la versión cifrada de la clave.

Adicionalmente a la información sobre productos y servicios que tenemos en la base de datos, están todos los elementos gráficos. Tanto los que dan forma al sitio, sitedesign/xxx/, como aquéllos que ilustran los artículos, ezimagecataloge/files/. Es por esta razón que, apoyándonos en LIDS, ocultaremos cuando menos esos dos directorios, para que no sean visibles. Adicionalmente, a través de los permisos para los archivos que establece el sistema operativo, éstos estarán restringidos para que no sean modificables.

Para la protección de los datos de las transacciones financieras, debido a que éstos residen en el backend bancario y podríamos decir que sólo son responsabilidad nuestra mientras los entregamos a los clientes, bastará, para no comprometerlos, que cifremos toda comunicación que haya entre nosotros y los clientes de BB.

Para ello nos apoyaremos en la capacidad de apache de incorporar capacidades para cifrar las comunicaciones http, utilizando el protocolo SSL.

Cubiertos así los requisitos de seguridad que necesitamos resolver a nivel del diseño pasemos a ver la construcción del sistema integral de banca por Internet.

Se construyó un pequeño archivo de procesamiento por lotes (código 38) para activar la seguridad como ya se había definido. Es muy útil para hacerlo siempre igual.

```
#!/bin/bash
echo "Activando y desactivando servicios"
/sbin/chkconfig --level 345 httpd on
/sbin/chkconfig --level 345 anacron on
/sbin/chkconfig --level 345 atd on
/sbin/chkconfig --level 345 crond on
/sbin/chkconfig --level 345 keytable on
/sbin/chkconfig --level 345 kudzu on
/sbin/chkconfig --level 345 mysqld on
/sbin/chkconfig --level 345 network on
/sbin/chkconfig --level 345 random on
/sbin/chkconfig --level 345 sendmail on
/sbin/chkconfig --level 345 sshd on
/sbin/chkconfig --level 345 syslog on
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 apmd off
/sbin/chkconfig --level 345 gpm off
/sbin/chkconfig --level 345 ipchains off
/sbin/chkconfig --level 345 iptables off
/sbin/chkconfig --level 345 netfs off
/sbin/chkconfig --level 345 portmap off
/sbin/chkconfig --level 345 rawdevices off
echo "Activando libsafe"
/usr/share/doc/libsafe-2.0/tools/libsafe-install.sh -i
echo "Activando LIDS"
rm -rf /etc/mtab
ln -s /proc/mounts /etc/mtab
echo "Estableciendo una clave para LIDS"
echo "Por favor tecle una clave a continuacion. Asegurese de no olvidarla"
/sbin/lidsconf -P
echo "Corriendo el script de inicializacion de la base de datos de LIDS"
/root/lids.sh
echo "Listo, la seguridad ha sido activada"
echo "Para tener una terminal de una sesion teclee:"
echo "lidsadm -S -- -LIDS"
echo "y proporcione la clave que acaba de utilizar."
echo "Por favor reinicie el equipo"
```

Código 38 Configuración y activación de los distintos elementos de seguridad.

Apache

Apache contribuye a la protección de los datos, desde la perspectiva de la entrega de información al cliente, sin que ésta sea vista o modificada por nadie más que el cliente.

Para ello le hemos agregado a Apache el módulo mod_ssl que implementa SSL (diagrama 16).

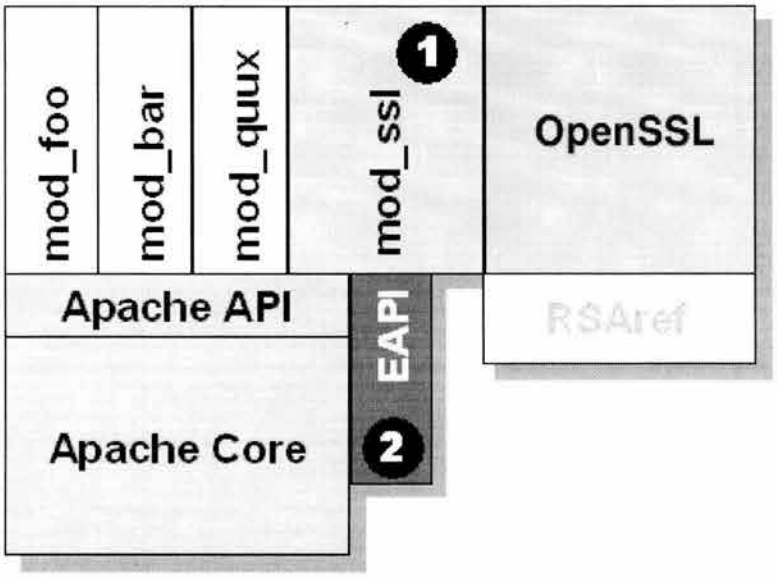


Diagrama 16 Integración de mod_ssl en Apache.

Gracias a que el gobierno de los Estados Unidos de Norteamérica ya liberalizó sus restricciones en cuanto a la exportación de software de criptografía y sus derivados, hoy en día en México ya podemos utilizar cifrado de 128 bits, cosa que estamos haciendo. Y no sólo eso, sino que lo estamos haciendo de manera flexible; es decir, si el cliente que se conecta al servidor soporta cifrado a 128 bits, se utiliza, pero si no, se hace una degradación automática e imperceptible a 40 bits.

Esto lo logramos utilizando lo que se conoce como un supercertificado, que viene siendo la credencial de elector con fotografía para el servidor, que ha sido construido utilizando unaparte de la especificación que da la oportunidad de presentar una llave privada de 128 o de 40 bits dependiendo del navegador.

Bitácoras

No podemos terminar el aspecto de seguridad sin mencionar lo importante, importantísimo, que es revisar las bitácoras, ya sea porque alguna herramienta como logwatch nos las envíe periódicamente por correo, ya sea porque nosotros entramos periódicamente al servidor a hacer

una revisión manual. En cualquier caso hacerlo, es de extrema importancia para asegurarnos del correcto funcionamiento del servidor y de sus servicios.

```
Active System Attack Alerts
-=-=-=-=-=-=-=-=-=-=-=-=-=-
Mar 14 05:15:50 rackspace portsentry[843]: attackalert: SYN/Normal scan from host: OL155-
70.fibertel.com.ar/24.232.70.155 to TCP port: 1080
Mar 14 05:15:50 rackspace portsentry[843]: attackalert: Host: OL155-
70.fibertel.com.ar/24.232.70.155 is already blocked Ignoring
Mar 14 11:59:20 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:20 rackspace portsentry[843]: attackalert: Host 68.49.81.66 has been blocked via
dropped route using command: "/sbin/ipchains -I input -s 68.49.81.66 -j DENY -l"
Mar 14 11:59:22 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:22 rackspace portsentry[843]: attackalert: Host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 is already blocked Ignoring
Mar 14 11:59:23 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:23 rackspace portsentry[843]: attackalert: Host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 is already blocked Ignoring
Mar 14 13:17:13 rackspace portsentry[847]: attackalert: Connect from host:
impala.sat.rackspace.com/64.39.1.231 to UDP port: 161
Mar 14 13:17:13 rackspace portsentry[847]: attackalert: Host: 64.39.1.231 is already blocked.
Ignoring

Security Violations
-=-=-=-=-=-=-=-=-=-=
Mar 14 05:15:50 rackspace portsentry[843]: attackalert: SYN/Normal scan from host: OL155-
70.fibertel.com.ar/24.232.70.155 to TCP port: 1080
Mar 14 05:15:50 rackspace portsentry[843]: attackalert: Host: OL155-
70.fibertel.com.ar/24.232.70.155 is already blocked Ignoring
Mar 14 11:59:20 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:20 rackspace portsentry[843]: attackalert: Host 68.49.81.66 has been blocked via
dropped route using command: "/sbin/ipchains -I input -s 68.49.81.66 -j DENY -l"
Mar 14 11:59:22 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:22 rackspace portsentry[843]: attackalert: Host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 is already blocked Ignoring
Mar 14 11:59:23 rackspace portsentry[843]: attackalert: SYN/Normal scan from host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 to TCP port: 4000
Mar 14 11:59:23 rackspace portsentry[843]: attackalert: Host:
pcp04636489pcs.gambrl01.md.comcast.net/68.49.81.66 is already blocked Ignoring
Mar 14 13:17:13 rackspace portsentry[847]: attackalert: Connect from host:
impala.sat.rackspace.com/64.39.1.231 to UDP port: 161
Mar 14 13:17:13 rackspace portsentry[847]: attackalert: Host: 64.39.1.231 is already blocked.
Ignoring
Mar 15 03:56:31 rackspace named[11912]: client 200.66.107.109#3180: updating zone 'benzu.com/IN':
update failed: 'RRset exists (value dependent)' prerequisite not satisfied (NXRRSET)
Mar 15 03:56:31 rackspace named[11912]: client 200.66.107.109#3183: update 'benzu.com/IN' denied
Mar 15 04:56:31 rackspace named[11912]: client 200.66.107.109#3559: updating zone 'benzu.com/IN':
update failed: 'RRset exists (value dependent)' prerequisite not satisfied (NXRRSET)
Mar 15 04:56:32 rackspace named[11912]: client 200.66.107.109#3562: update 'benzu.com/IN' denied
Mar 14 23:45:03 rackspace portsentry[3048]: securityalert: Psionic PortSentry is shutting down
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: LOGIN User: root TTY: pts/1 Host: dsl-
200-95-60-212.prod-infinitum.com.mx
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: First time login for user: root
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Action being taken for user: root
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Module requesting action is:
moduleFirstLogin
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Action complete for module:
moduleFirstLogin
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Foreign domain login detected for
user: root from: dsl-200-95-60-212.prod-infinitum.com.mx
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Action being taken for user: root
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Module requesting action is:
moduleForeignDomain
```

```
Mar 14 23:49:42 rackspace hostSentry[3261]: securityalert: Action complete for module:
moduleForeignDomain
Mar 15 05:56:33 rackspace named[11912]: client 200.66.107.109#3937: updating zone 'benzu.com/IN':
update failed: 'RRset exists (value dependent)' prerequisite not satisfied (NXRRSET)
Mar 15 05:56:33 rackspace named[11912]: client 200.66.107.109#3940: update 'benzu.com/IN' denied
Mar 14 04:05:45 rackspace sendmail[24101]: i2EA5jPY024101: rackspace.iac.com.mx [209.61.189.108]
did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA

Unusual System Events
=-=-=-=-=-=-=-=-=-=-=-=-=
Mar 14 04:03:44 rackspace syslogd 1.3-3: restart.
Mar 14 04:03:44 rackspace syslogd 1.3-3: restart.
Mar 14 04:03:44 rackspace syslogd 1.3-3: restart.
Mar 14 04:03:44 rackspace syslogd 1.3-3: restart.
Mar 14 04:04:00 rackspace CROND[24021]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:05:00 rackspace CROND[24073]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:05:00 rackspace CROND[24075]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:06:01 rackspace CROND[24107]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:07:00 rackspace CROND[24130]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:08:00 rackspace CROND[24149]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:09:00 rackspace CROND[24166]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:10:00 rackspace CROND[24187]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:10:00 rackspace CROND[24189]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:10:01 rackspace CROND[24191]: (apache) CMD (/usr/local/Zend/sbin/cache_clean
/usr/local/Zend/etc/php.ini)
Mar 14 10:10:06 rackspace named[11912]: lame server resolving '212.230.111.161.in-addr.arpa' (in
'230.111.161.in-addr.arpa'?): 130.206.1.2#53
Mar 14 04:10:48 rackspace bsmon: status for rackspace.msgs changed from 1 to 3
Mar 14 04:10:49 rackspace bsmon: clearing alarm: rackspace.msgs mail error, messages looks fine
Mar 14 04:10:49 rackspace bsmon: sending page for rackspace.msgs with severity 50 by
/usr/lib/sendmail to alarm: messages looks fine|>syslog looks fine
Mar 14 04:11:00 rackspace CROND[24229]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:12:00 rackspace CROND[24305]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:13:00 rackspace CROND[24329]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:14:00 rackspace CROND[24346]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:15:00 rackspace CROND[24371]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:15:00 rackspace CROND[24373]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:16:00 rackspace CROND[24402]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:17:00 rackspace CROND[24427]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:18:00 rackspace CROND[24447]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:19:00 rackspace CROND[24480]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:19:31 rackspace ntpd[421]: time reset 1.970133 s
Mar 14 04:19:31 rackspace ntpd[421]: synchronisation lost
Mar 14 04:20:02 rackspace CROND[24505]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:20:02 rackspace CROND[24507]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:20:02 rackspace CROND[24509]: (apache) CMD (/usr/local/Zend/sbin/cache_clean
/usr/local/Zend/etc/php.ini)
Mar 14 04:21:00 rackspace CROND[24538]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:22:00 rackspace CROND[24561]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:22:00 rackspace CROND[24559]: (root) CMD (run-parts /etc/cron.weekly)
Mar 14 04:23:00 rackspace CROND[27599]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:24:01 rackspace CROND[30110]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:25:00 rackspace CROND[429]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:25:00 rackspace CROND[427]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:26:00 rackspace CROND[509]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:27:00 rackspace CROND[529]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:28:01 rackspace CROND[559]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:29:00 rackspace CROND[576]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:30:00 rackspace CROND[596]: (root) CMD (/etc/webmin/sysstats/sysstats.pl)
Mar 14 04:30:00 rackspace CROND[598]: (mailman) CMD (/usr/bin/python -S
/var/mailman/cron/gate_news)
Mar 14 04:30:00 rackspace CROND[600]: (apache) CMD (/usr/local/Zend/sbin/cache_clean
/usr/local/Zend/etc/php.ini)
```

Código 39 Ejemplo de un reporte preparado por logcheck (fragemento).

Si olvidamos revisar periódicamente las bitácoras (código 39), arriesgamos que el sistema sea comprometido en algún momento, sin que tengamos noticias de tal cosa. Véase la parte marcada del reporte, para que se identifique el riesgo y la gravedad de no atenderlo.

Capítulo 5 Operación

Los procedimientos son guías breves que apoyan a los operadores en sus funciones cotidianas.

Procedimientos de Operación

Alta del servidor o los servicios

La situación inicial, que se considera existe para las instrucciones que a continuación se detallan, es que el equipo ha sido instalado utilizando un disco compacto de instalación construido especialmente para BB y del que ya se dieron sus generalidades. Se considera, además, que el equipo se encuentra apagado. Existen dos tipos de *servidores*[xxviii], que pueden estar en dos equipos o un mismo equipo para cubrir ambas funciones.

Si el equipo se instaló utilizando el disco compacto especial para BB entonces lo primero es encender el equipo y eso deberá automáticamente levantar los servicios necesarios. En ambos casos debemos observar los mensajes que el servidor envía a la consola. Si estamos levantando un servidor transaccional, entonces en el proceso de inicialización del servidor nos pedirá la frase clave de la llave privada del certificado que sirve para establecer conexiones seguras mediante SSL. Si el proceso de inicialización terminó sin problemas, entonces debemos corroborar que los servicios están operando correctamente y que hay conectividad tanto del servidor hacia Internet, como de Internet hacia el servidor y del servidor hacia el backend bancario.

Para decir que hemos dado de alta el servidor tenemos que asegurarnos de que hay dos servicios en activo:

- el servidor de páginas (apache),
- el servidor de bases de datos (mysql),

y, además, que la conectividad del servidor con sus contrapartes funciona.

Para corroborar que el servidor de bases de datos se encuentra disponible escribimos:

```
root@rackspace /etc/httpd/conf/conf.d# service mysqld status
mysqld (pid 27852) is running...
```

Si, como en este caso, la respuesta es que el servicio se encuentra corriendo entonces probaremos conectarnos al motor y hacer una consulta sobre alguna de las tablas de la base de datos del SAC.

```
root@rackspace ~# mysql bajionet
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 114555 to server version: 3.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select ID from eZArticle_Article where ID=10;
+----+
| ID |
+----+
| 10 |
+----+
1 row in set (0.02 sec)

mysql> \q
Bye
root@rackspace ~#
```

Dado que la consulta también fue exitosa, podemos asegurar que el servidor de base de datos se encuentra disponible.

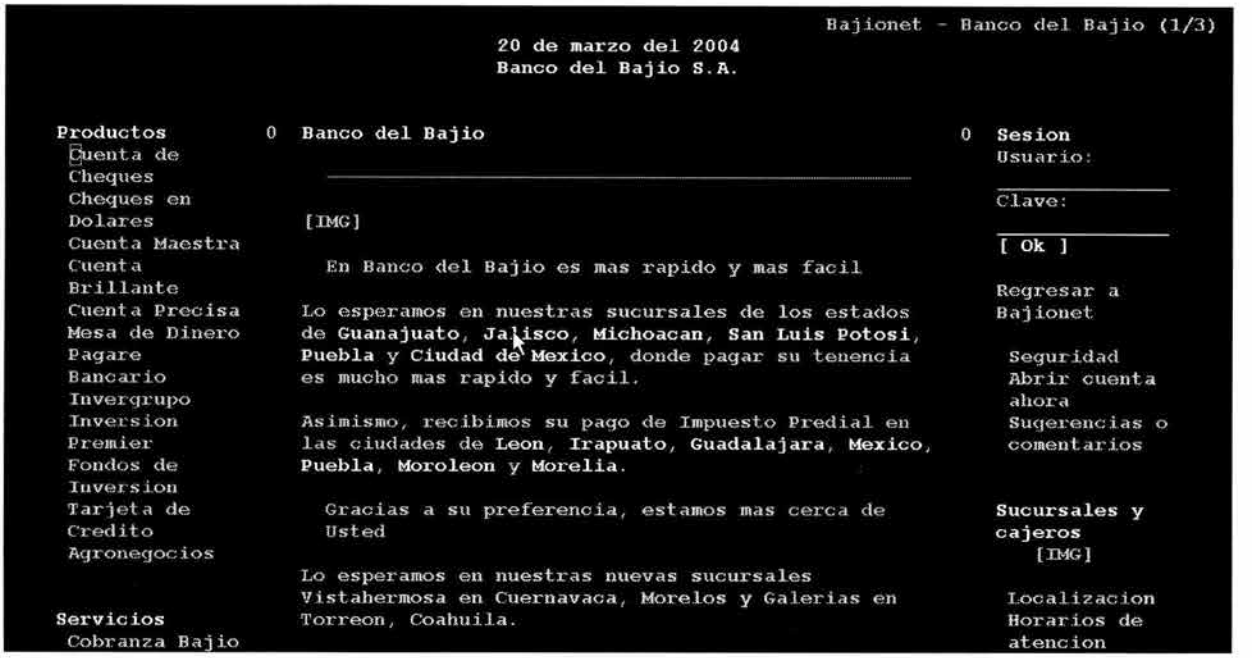
Veamos ahora que el servidor de páginas también se encuentre disponible. Lo primero es verificar el estado del proceso.

```
root@rackspace ~# service httpd status
httpd (pid 20413 20412 20411 20267 20266 20265 20039 19751 19750 19731 19726 19725 19724 19723 19722
 19721 19720 19719 19716) is running...
```

Dado que el reporte es positivo, veremos si está contestando peticiones.

```
root@rackspace ~# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
Escape character is '^]'.
GET /
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
```

Como el servidor sí está contestando peticiones, probaremos si lo que contesta es lo que debería contestar. Esto es más fácil saberlo cuando utilizamos un navegador. Como estamos trabajando en la consola, utilizaremos un navegador modo texto.



Como lo que el servidor está enviando es lo que esperábamos recibir, podemos afirmar que los servicios están activos y funcionando correctamente.

La siguiente prueba es de conectividad entre este servidor y el servidor del backend bancario. Para ello primero obtendremos el servidor del backend bancario que está configurado para esta instalación de la aplicación y posteriormente haremos un ping.

```
root@rackspace ~# grep -i backend /var/www/html/www.bajio.com.mx/site.ini
Backend=209.61.189.106
root@rackspace ~# ping 209.61.189.106
PING 209.61.189.106 (209.61.189.106) 56(84) bytes of data.
64 bytes from 209.61.189.106: icmp_seq=0 ttl=255 time=0.574 ms
64 bytes from 209.61.189.106: icmp_seq=1 ttl=255 time=0.513 ms
64 bytes from 209.61.189.106: icmp_seq=2 ttl=255 time=0.508 ms

--- 209.61.189.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.508/0.531/0.574/0.040 ms, pipe 2
root@rackspace ~#
```

Con esto corroboramos la conectividad interna. Ahora probemos la externa. Un ping a yahoo.com bastará.

```
root@rackspace ~# ping www.yahoo.com
PING www.yahoo.akadns.net (216.109.117.205) 56(84) bytes of data.
64 bytes from p18.www.dcn.yahoo.com (216.109.117.205): icmp_seq=0 ttl=50 time=48.3 ms
64 bytes from p18.www.dcn.yahoo.com (216.109.117.205): icmp_seq=1 ttl=50 time=48.2 ms

--- www.yahoo.akadns.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 48.217/48.275/48.333/0.058 ms, pipe 2
root@rackspace ~#
```

Gracias a que, afortunadamente, obtenemos respuestas, entonces hay conectividad, al menos del servidor hacia Internet.

Podemos entonces pasar a verificar si los servicios están disponibles desde equipos remotos. Dado que existen al menos dos firewalls entre este servidor y los clientes de los servicios que este servidor proporciona probaremos primero en otro equipo de la misma red y posteriormente desde un equipo conectado a Internet.

Desde el equipo en la misma red obtenemos que

```
root@shark ~# telnet 200.76.36.70 80
Trying 200.76.36.70...
Connected to 200.76.36.70.
Escape character is '^]'.
GET /
```

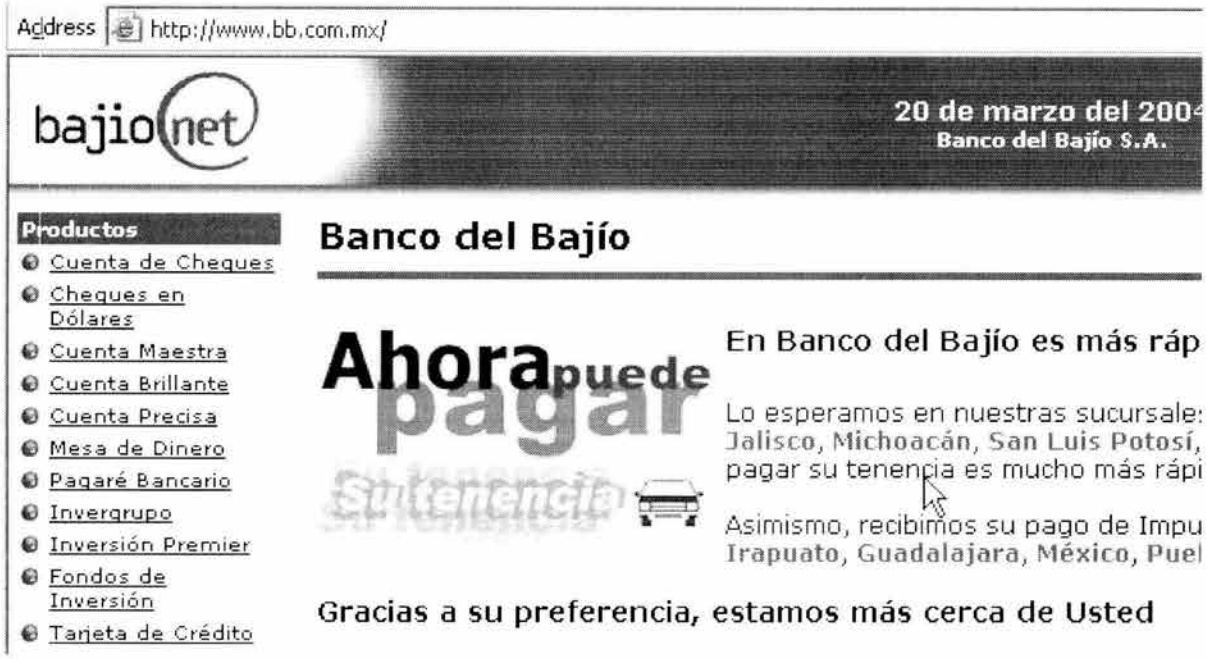
El servidor contesta sin problemas, es decir, el firewall que está instalado en dicho servidor funciona conforme a lo que esperamos y además el servidor y los servicios también.

Ahora hagamos la prueba pero utilizando nombres en lugar de direcciones IP.

```
root@shark ~# telnet www.bb.com.mx 80
Trying 66.98.180.48...
Connected to www.bb.com.mx.
Escape character is '^]'.
GET /
<html>
```

Como también contesta por nombre, hemos comprobado dos cosas: la primera, que el servidor de nombres está operando y lo hace de manera correcta y segunda, que el servidor contesta las peticiones que se hacen a dicho sitio. Con esto también comprobamos que la configuración de apache está operando correctamente.

Finalmente, probemos desde un equipo conectado a Internet y sin relación alguna con las redes del Banco.



Dado que esta prueba es también satisfactoria, podemos concluir que el servidor ha sido levantado satisfactoriamente.

Veamos entonces una variante que corresponde a cuando el equipo se encuentra encendido y deseamos corroborar que los servicios están operando y, si no lo están, proceder a levantarlos.

Con el fin de ofrecer nuevas formas de detección sobre la disponibilidad de un servicio cambiaremos un poco el esquema utilizado con anterioridad.

Primero veremos qué procesos se encuentran corriendo.

```
root@rackspace ~# ps fax
  PID TTY      STAT   TIME COMMAND
    1 ?        S      0:51 init [3]
    2 ?        SW     0:11 [keventd]
    3 ?        SW     0:40 [kapmd]
    4 ?        SWN    0:00 [ksoftirqd/0]
    7 ?        SW     0:00 [bdflush]
    5 ?        SW     6:22 [kswapd]
    6 ?        SW     1:43 [kscand]
    8 ?        SW     0:21 [kupdated]
    9 ?        SW     0:00 [mdrecoveryd]
   95 ?        SW     0:02 [kjournald]
   96 ?        SW    23:09 [kjournald]
  357 ?        S     11:10 syslogd -m 0
  361 ?        S      0:01 klogd
```

Como utilizamos un comando que nos muestra todos los procesos que están corriendo en el servidor y su jerarquía padre-hijo, el listado es excesivo. Analicemos entonces un fragmento de dicho listado que contiene la información que nos interesa.

```
  446 ?        S      5:13 xinetd -stayalive -pidfile /var/run/xinetd.pid
  632 ?        S      0:18 crond
  649 ?        S      0:00 /usr/sbin/atd
  843 ?        S     49:38 portsentry -stcp
  847 ?        S      0:00 portsentry -udp
  875 tty1     S      0:00 /sbin/mingetty tty1
  876 tty2     S      0:00 /sbin/mingetty tty2
  877 tty3     S      0:00 /sbin/mingetty tty3
  878 tty4     S      0:00 /sbin/mingetty tty4
  879 tty5     S      0:00 /sbin/mingetty tty5
  880 tty6     S      0:00 /sbin/mingetty tty6
 1018 ?        S      4:41 /usr/local/Zend/sbin/cache_clean /usr/local/Zend/etc/php.ini
27825 ?        S      0:00 /bin/sh /usr/bin/safe_mysqld --defaults-file=/etc/my.cnf
27852 ?        S   3083:32  \_ /usr/libexec/mysqld --defaults-file=/etc/my.cnf --basedir=/usr --dat
 3261 ?        S      0:03 python hostsentry.py
19716 ?        S      0:01 /usr/sbin/httpd
29119 ?        S      0:37  \_ /usr/sbin/httpd
29751 ?        S      0:28  \_ /usr/sbin/httpd
29752 ?        S      0:30  \_ /usr/sbin/httpd
29753 ?        S      0:28  \_ /usr/sbin/httpd
30063 ?        S      0:20  \_ /usr/sbin/httpd
30566 ?        S      0:16  \_ /usr/sbin/httpd
30567 ?        S      0:14  \_ /usr/sbin/httpd
30568 ?        S      0:14  \_ /usr/sbin/httpd
30694 ?        S      0:12  \_ /usr/sbin/httpd
31208 ?        S      0:03  \_ /usr/sbin/httpd
31210 ?        S      0:03  \_ /usr/sbin/httpd
31211 ?        S      0:04  \_ /usr/sbin/httpd
31289 ?        S      0:01  \_ /usr/sbin/httpd
root@rackspace ~#
```

Aquí tenemos que el servidor de base de datos está corriendo, tal como podemos ver en los procesos 27825 y 27852.

Lo mismo el servidor de páginas está corriendo, como podemos ver en el proceso 19716 y sus hijos.

En el caso de que el servidor de base de datos no estuviera corriendo, para levantarlo haremos lo siguiente.

```
root@rackspace ~# service mysqld start
Starting MySQL:                                            [  OK  ]
root@rackspace ~# service mysqld status
mysqld (pid 32280) is running...
```

Ahora bien, si el servicio que no estuviera disponible fuera el servidor de páginas, lo que haríamos sería:

```
root@rackspace ~# service httpd start
Starting httpd:                                            [  OK  ]
root@rackspace ~# service httpd status
httpd (pid 32365 32364 32362 32360 32359 32358 32357 32356 32355 32354 32353 32350) is running...
```

Finalmente, analicemos una última situación. Pensemos en que hemos modificado la configuración del servidor de páginas que atiende la aplicación transaccional y deseamos que dichas modificaciones sean tomadas en cuenta. Para ello debemos reiniciar el servidor y proporcionar la frase clave correspondiente. El proceso sería similar al siguiente:

```
root@shark ~# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd: Apache/2.0.47 mod_ssl/2.0.47 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.

Server shark.internetdealtacalidad.com:443 (RSA)
Enter pass phrase:

Ok: Pass Phrase Dialog successful.
                                                           [  OK  ]
```

Si proporcionamos la frase clave correcta, se podrá utilizar la llave privada del certificado para el sitio seguro y con ellos tendremos un servidor capaz de realizar transacciones financieras.

Baja del servidor

Para dar de baja el servidor basta un solo comando. Además en los equipos modernos este mismo comando puede apagar físicamente el equipo.

```
root@rackspace ~# halt
```

Si hacemos esto estando en la consola, veremos el listado de todos los pasos que sigue el servidor para darse de baja. Sí lo hacemos de manera remota el servidor nos dará un aviso de que se está dando de baja, y tan pronto como desactive el servicio de conexión a una sesión remota segura, perderemos la conexión con él.

Procedimiento Monitoreo

El monitoreo es una técnica que nos permite aumentar la disponibilidad del servicio respondiendo de forma rápida a las eventualidades que se pudieran presentar. La mejor manera de realizarlo es automatizándolo y configurando las herramientas que utilicemos para la automatización para que las alertas que emitan nos lleguen por varias vías. Por ejemplo correo electrónico, beeper, mensajes de texto a celular, etc. La idea es detectar situaciones eventuales que se pudieran convertir en problemas por ejemplo la sobrecarga del servidor aplicativo, y problemas para darles la más rápida solución posible.

Aún cuando hay varias alternativas, por ejemplo contratar alguno de los sitios que ofrecen realizar dicho servicio o hacerlo manualmente, programar nosotros un conjunto de herramientas, etc., nuestra recomendación es utilizar BigSister para esta tarea.

BigSister

BigSister es una herramienta que sirve para

- Monitorea sistemas que están en red.
- Proporciona una visión sencilla del estado de la red y de sus componentes.

- Avisa al administrador cuando algún sistema entra en un estado crítico y cuando lo abandona.
- Crea una historia de los cambios de estado por sistema o servicio monitoreado.
- Almacena y muestra varios datos sobre el desempeño del equipo o los sistemas monitoreados.

Esta herramienta es capaz de hacer monitoreo local-local, es decir se puede instalar la herramienta en el mismo sistema que se va a monitorear, local-remoto, se puede instalar la herramienta para monitorear un equipo distinto a aquél donde se instaló y, finalmente, remoto-remoto, es decir instalar el sistema en dos equipos distintos donde uno de ellos hace el monitoreo, otro es el monitoreado y el tercero sólo muestra los resultados del monitoreo.

A continuación presentamos la configuración para realizar un monitoreo local-local para los servicios de http, ssh, pop3 y smtp, entre otros:

Configuración ejemplo

```
# Set the default SNMP community to "public", the
# default frequency is 1/5min anyway
DEFAULT         community=public frequency=5 ALL

# Set the default version and protocol for rpc checks to "1" and "udp"
DEFAULT         version=1 proto=udp rpc

rackspace.iac.com.mx    load diskload memory http ssh pop3 smtp \
                fs=all(6%-10%),all-ufs(6%-10%),all-ext2(6%-10%) diskfree \
                syslog dumpdates \
                procs=init(1-1),sendmail(1-20) procs eventlog cpuload \
                network

# iac.com.mx(iac)       http ssh pop3 smtp

# EDIT THIS, replace localhost by the name of your BigSister server
rackspace.iac.com.mx    bsdisplay

# uncomment this and replace localhost by a suitable BigSister server
# if you want to enable performance data trend charts
rackspace.iac.com.mx    frequency=10 perfdata=etc/perf options=perf bsdisplay
rackspace.iac.com.mx    frequency=30 perfdata=etc/perfslow options=perf bsdisplay

# include file for specific hosts, do not name it uxmon-net.* as a new
# process is started for every file matching that pattern

include include_checks.$HOST
```

Código 40 Archivo de configuración de BigSister utilizado para realizar un monitoreo local-local.

En la línea 3 de este archivo (código 40) se define la comunidad que se debe utilizar para hacer monitoreo a través de SNMP, en nuestro caso no estamos monitoreando ningún servicio, equipo o dispositivo a través de este protocolo. Sin embargo, debemos definir un valor por omisión.

Algo similar pasa con la línea 6, donde debemos definir una versión y un protocolo para monitorear la disponibilidad de servicios tipo rpc. Sin embargo, ni estamos utilizando ni estamos monitoreando servicios tipo rpc.

Las líneas 8 a 12 son las verdaderamente importantes para nosotros. Aquí estamos definiendo que equipo se va a monitorear así como que se le va a monitorear.

En este caso el equipo a monitorear es rackspace.iac.com.mx y vamos a monitorear distintas cosas. Entre las más importantes está la disponibilidad del servidor de páginas (http), del servicio de sesiones remotas seguras (ssh), los servicios de correo tanto entrante como saliente (pop3 y smtp), la carga del servidor (load) los discos duros y los rangos en los que hay que mandar avisos por situación crítica y la disponibilidad de red (network).

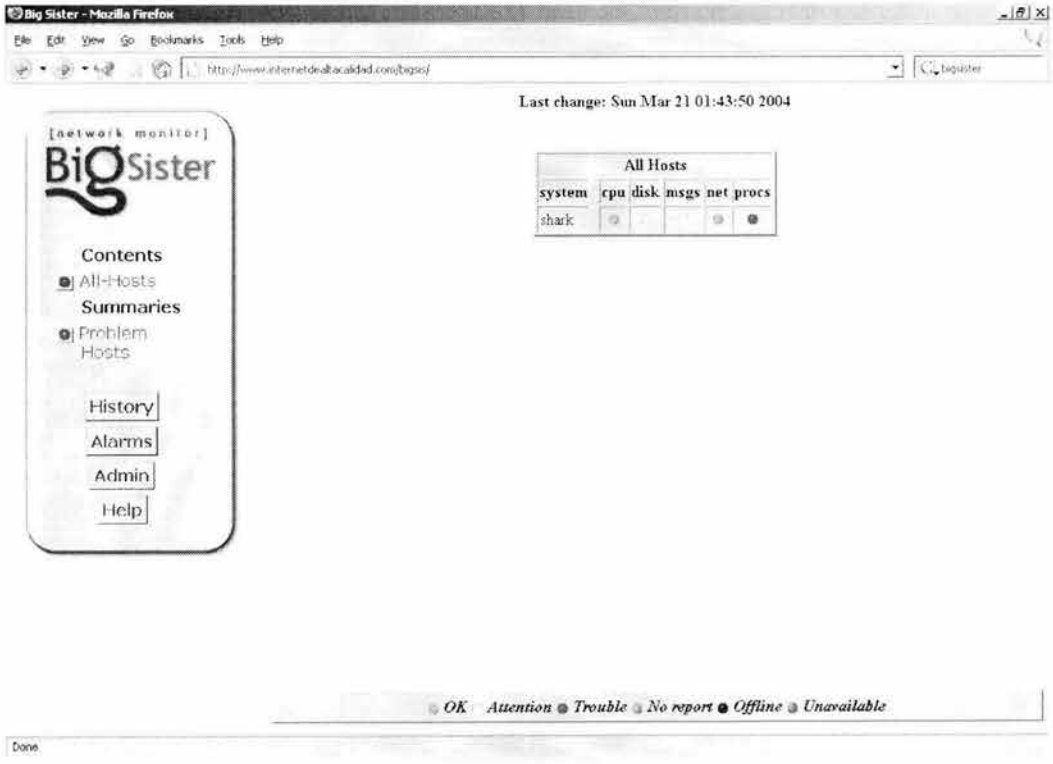
Debido a la capacidad de la herramienta de desplegar la información recabada en el monitoreo local o remota o debemos definir cuál es el servidor donde se presentará. En este caso es el mismo, puesto que estamos haciendo un monitoreo local-local.

Aprovecharemos las capacidades de monitoreo de la herramienta para en las líneas 21 y 22 definirle que queremos que se monitoree y con qué frecuencia.

Pantallas de muestra del resultado del monitoreo

Una de las ventajas más interesantes de BigSister es que, automáticamente, prepara una página con la información más reciente que ha recabado en los monitoreos, y desde ahí es posible acceder a la historia de todos y cada uno de los servidores que se estén monitoreando.

Esta primera pantalla (pantalla 19) nos muestra la página principal de BigSister en un servidor de despliegue.

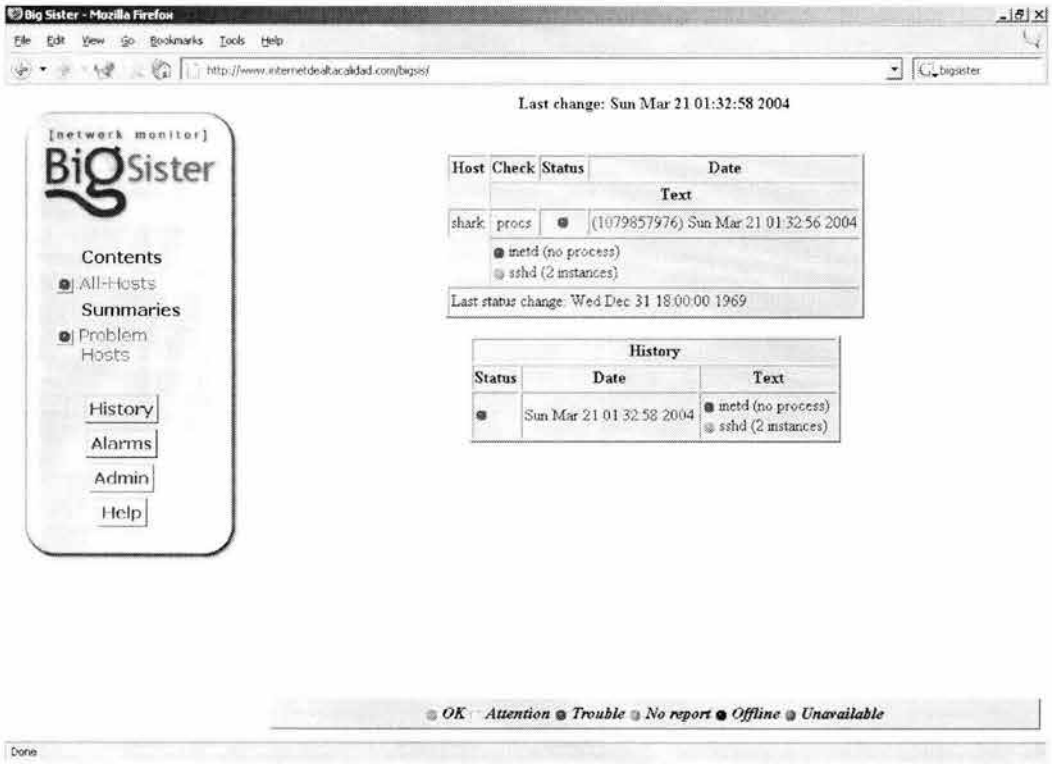


Pantalla 19 Página principal de un servidor de despliegue de BigSister.

En esta página se presenta el resultado del monitoreo de un sitio local y nada más.

Resulta que este servidor tiene dos aspectos trabajando normalmente: el procesador y la red. Dos aspectos en un estado que requiere atención: los discos duros y la bitácora. Y, finalmente, uno en estado crítico: los procesos.

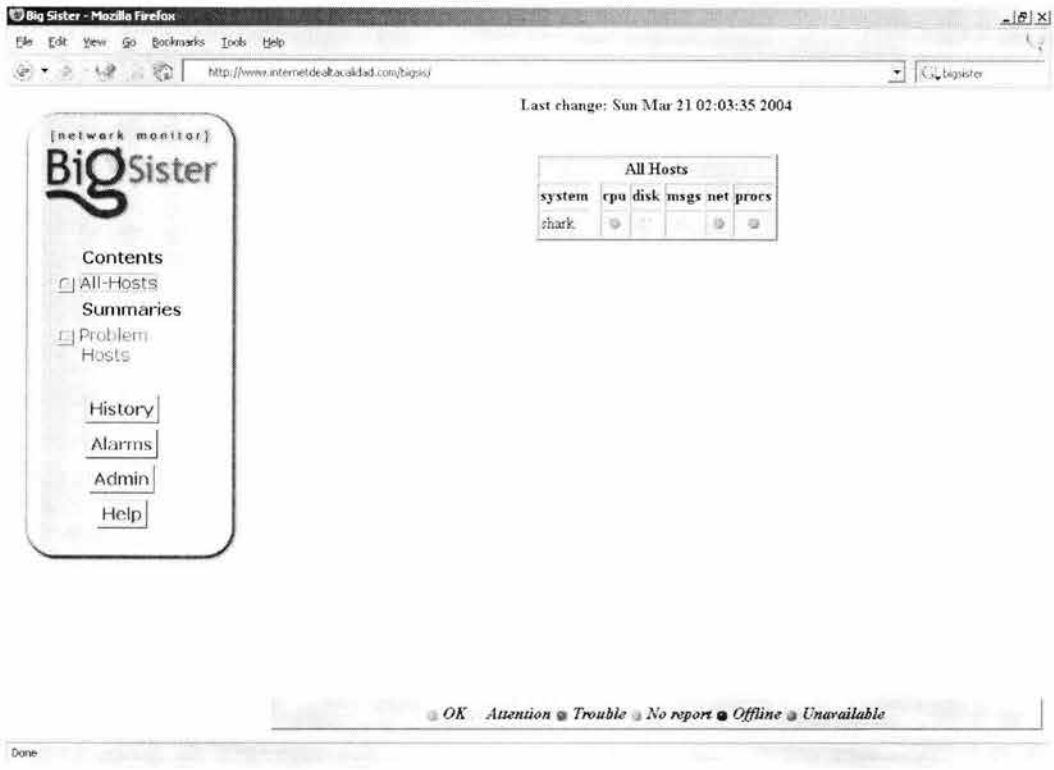
Si hacemos click sobre cada uno de los indicadores obtendremos información de detalle. Así, pues, veamos (pantalla 20) qué nos puede decir del porqué se señala como en estado crítico a los procesos.



Pantalla 20 Página de detalle sobre el estado de un servicio.

El detalle nos está revelando que el monitoreo detectó que inetd no está corriendo, situación que normalmente es conflictiva, puesto que a través de este servicio suelen atenderse peticiones de recuperación de correo electrónico, de sesión remota, de ftp, etc. Sin embargo, por la configuración del servidor que estamos usando de muestra nosotros sabemos que esto no es problemático, que en este caso, lo que se debe hacer es corregir la configuración del monitor para que no considere esta situación como problemática.

Una vez corregida la configuración (pantalla 21), el monitoreo se ve como sigue.



Pantalla 21 Página principal con la configuración corregida.

Se utilizó el ejemplo de una configuración errónea para hacer notar que antes de poder confiar en nuestra herramienta de monitoreo, tenemos que asegurarnos de que la hemos configurado adecuadamente. Sobre todo en función de los servicios que ofrece cada servidor y de aquéllos que queremos que se monitoreen. También vale la pena hacer notar aquí que cada vez que se nos reporte una situación de excepción en algún servidor, antes de alarmarnos, debemos hacer un análisis que nos permita identificar la posible fuente del problema.

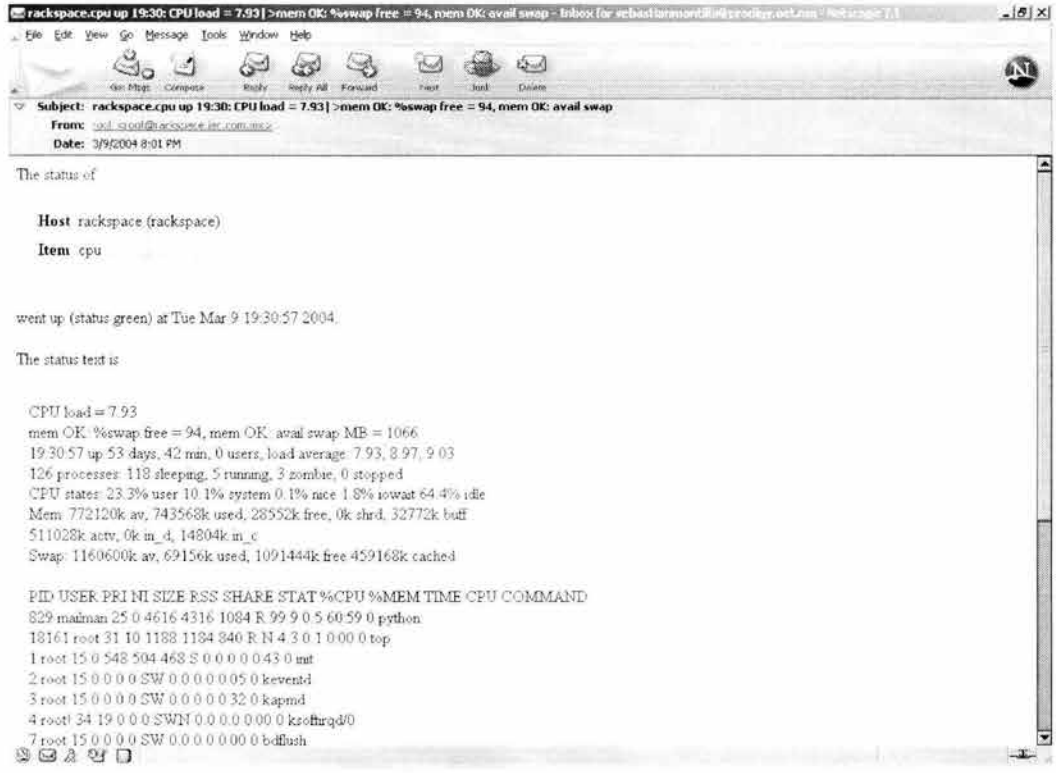
Correos electrónicos: muestra de los resultados de monitoreo.

Dado que los avisos se pueden enviar por varias vías pero la que es más sencilla de mostrar aquí es el correo electrónico, veremos aquí a continuación algunos ejemplos de ellos.

Como habíamos mencionado, BigSister, avisa tanto cuando el sistema entra en estado crítico, como cuando sale de él, a continuación veremos un caso de una alerta de que el sistema salió de su condición problemática.

El cambio de estado de un servidor o servicio puede ser producto de las acciones correctivas que se tomaron, o bien de que, en este caso particular, el sistema tiene menos demanda y por ello ha pasado a un estado no crítico. Este tipo de situaciones se producen cuando un servidor ofrece servicios que están vinculados con horarios y hay un momento en el que la demanda supera la capacidad normal de atención y eso provoca que se tenga una carga excesiva.

Cuando se ofrecen servicios donde el tiempo de respuesta al usuario es determinante, se deben tomar medidas correctivas inmediatas, puesto que si bien un servidor con más carga de la normal no implica que se esté dejando de dar el servicio, sí implica que los tiempos de respuesta se han degradado. Dependiendo de las necesidades y compromisos que se tengan, se puede tener que llegar a diseñar el sistema en su conjunto para que cumpla con un conjunto de parámetros en los momentos en los que se encuentra en sus picos superiores de demanda. Esto generalmente lleva a configuraciones[xxix] donde en la mayor parte del tiempo se tiene un excedente de recursos, mismos que son los justos para cumplir con los parámetros de diseño en los momentos de mayor demanda.



Pantalla 22 Correo con aviso de BigSister notificando que la carga disminuyó y por ello el servidor salió del estado crítico en el que se encontraba.

Vale la pena resaltar de este correo (pantalla 22) que tanto en el aviso de entrada como en el de salida, la información que contiene es bastante amplia, por ejemplo, la carga, la memoria y su distribución en disponible, ocupada y swap, el tiempo que el servidor tiene activo, el número de procesos, el número de procesos activos, en ejecución, zombies, durmientes, parados, el listado de los proceso activos en ese momento y las características de cada uno de ellos.

Toda esta información es útil, porque permite contar con una fotografía del equipo cuando ingresa al estado crítico y determinar que recurso puede ser el más demandado sí procesador, memoria o disco duro y quien puede ser quien más lo esté demandando. Analizando esa información se puede proceder a diseñar una estrategia que corrija las situaciones problemáticas.

El siguiente (pantalla 23) es un ejemplo de cuando un servidor entra en estado crítico. Nótese como se habla de un (status red) en señal de que el estado del servidor es problemático.

Pantalla 23 Correo con aviso de BigSister notificando que el servicio de correo dejo de contestar y por ello el servidor se encuentra en estado crítico (status red).

Con esto terminamos la descripción del procedimiento de monitoreo puesto que ya vimos las fases de configuración, monitoreo, aviso y atención del aviso.

Capítulo 6 Resultados y conclusiones

Resultados

Para evaluar los resultados utilizaremos como guía los objetivos. Junto a cada uno de ellos pondremos si se alcanzó o no.

Resultado general

Construir un sistema integral de banca por Internet que ofrezca una disponibilidad de servicios de 7 x 24 x 365, que pueda crecer y satisfacer una demanda creciente, sin comprometer ninguno de sus parámetros y que permita a los clientes encontrar toda la información relevante sobre los productos y servicios del banco, así como efectuar desde Internet toda clase de operaciones bancarias en tiempo real y con el mayor grado de seguridad y confiabilidad, con lo que se aumente la capacidad de atención y la calidad de los servicios.

Alcanzado. Se construyó el sistema y opera desde hace 3 años sin problemas. De hecho ha sido tal el crecimiento de su demanda que ha puesto fuertemente a prueba su capacidad de crecer.

Resultados particulares

Sistema de administración de contenido

A continuación se presenta un listado de los requerimientos que se han planteado para el sistema de administración de contenido:

- Permitir el acceso directo de los clientes
  - a un buzón de sugerencias,
  - a la descripción del 100% de los productos y servicios del banco,
  - a los detalles del 100% de sucursales y cajeros automáticos,
  - a las preguntas más frecuentes de nuestros clientes y a la liga a las respuestas y
  - a la información sobre seguridad pertinente para los servicios de banca por Internet en el momento en que el portal esté al aire.

Alcanzado. El sistema cumple con todo lo que se planteó.

- Permitir el cambio del tipo de letra, imagen de fondo y formato de fechas sin tener que modificar todos y cada uno de los documentos que formen parte del sitio.

Alcanzado. El sistema cumple, basta modificar frame.php del diseño del portal.

- Contar con la capacidad de incluir imágenes en la información que se incorpore al portal.

Alcanzado. El sistema cumple, eZArticle permite incorporar imágenes y archivos a toda la información que se da de alta en el módulo de administración de contenido.

- Impartir capacitación del sistema de administración de contenido y operación.

Alcanzado. Se dio la capacitación necesaria y hoy en día personal de tres áreas distintas del banco lo modifica, lo administra y lo opera.

- Impartir capacitación sobre el desarrollo de temas y plantillas.

Alcanzado. El área de sistemas recibió dicha capacitación y es capaz de hacer las modificaciones que requiera.

- Contar con la capacidad de ofrecer a los clientes un comparativo de las tasas de interés que ofrece el banco contra las que ofrecen otros bancos.

Alcanzado. De hecho se desarrollaron ex profeso dos módulos eZTasas y eZBancos para dar cumplimiento con esta necesidad.

- Contar con la capacidad de delegar la administración del contenido al área de mercadotecnia.

Alcanzado. El sistema de administración de contenido lo maneja el área de mercadotecnia del banco.

- Reflejar una imagen moderna y de servicios financieros de alto nivel con noticias financieras y de negocios, así como un recuadro con los principales indicadores financieros.

Alcanzado. La página de BB tiene un diseño gráfico profesional, atractivo, serio y que demuestra modernidad.

- Desarrollar un encabezado y un pie de página que serán comunes a todas las páginas del sitio.

Alcanzado. El sitio tiene un encabezado y un pie de página común. Esto se logró incorporando ambos elementos a frame.php en el directorio correspondiente, dentro de sitedesign.

- Control de acceso a los distintos módulos del sistema de acuerdo a usuarios, claves y privilegios asignados.

Alcanzado. Gracias a eZ Publish todos los módulos tienen un control de acceso como el que se necesitaba.

- Construir el sistema asegurando que será de fácil manejo.

Alcanzado. El sistema es de tan fácil manejo que personal sin preparación en computación lo opera cotidianamente sin problemas.

- Desarrollar el sistema para que todos los cambios al contenido se reflejen inmediatamente.

Alcanzado. En eZ Publish o eZ Publish desktop edition, siempre que después de editar un contenido independientemente de que use o no la función de previsualización del mismo, en cuanto se publica está disponible, no necesitamos hacer nada más. El contenido se modifica en tiempo real.

- Desarrollar el sistema para que administre todo el contenido del portal, es decir para que tenga carácter integral.

Alcanzado. El sistema cumple ya que el contenido que pudiera haber sido especial, la comparación de las tasas, fue integrado al mismo sistema gracias al desarrollo de dos módulos nuevos.

- Debe generar automáticamente un mapa del sitio, con el contenido que ha sido publicado.

Alcanzado. El sistema se apoya en las categorías que se hayan definido y hace un árbol o mapa del sitio.

- Construir un motor de búsqueda integrado al sistema.

Alcanzado. Lo incluye eZ Publish. Desafortunadamente una decisión posterior llevó a desactivarlo del sitio.

- Debe ofrecer la facilidad de mostrar una presentación de la información previa a su publicación.

Alcanzado. Lo incluye eZ Publish en su módulo de eZArticle.

- Que desde la página principal se acceda directamente a BajíoNet, la parte del sitio donde se puede realizar operaciones bancarias.

Alcanzado. En el menú del lado derecho se puso una forma que da acceso directo y seguro al sistema transaccional.

- Debe ser rápido, utilizando como métrica de referencia las evaluaciones que proporcionan sitios especializados en la medición del desempeño de sitios en Internet.

Alcanzado. Las evaluaciones que se han hecho con herramientas de medición de respuesta de los sitios lo ubican en la media.

- El manejo y la presentación del sistema debe ser uniforme.

Alcanzado. Gracias a las plantillas todo el contenido se presenta uniformemente.

Sistema aplicativo o transaccional

A continuación se presenta un listado de los requerimientos que se han planteado para el sistema aplicativo.

Permitir el acceso directo de los clientes a las siguientes transacciones:

- Cambio de clave de acceso.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Clave mancomunada (Empresas).

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Consulta de movimientos.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Consulta de saldos en cuentas de vista, créditos e inversiones (que se despliegue automáticamente al entrar).

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Consultas de estado de cuenta.

Alcanzado. Existe la transacción y hay acceso directo a ella. Aquí cabe hacer la anotación de que, debido a que Microsoft Internet Explorer tiene problemas con la transferencia de archivos en modo seguro https, se tuvo que recurrir a una doble implementación para IE y para todos los demás. Esto se hizo posteriormente.

- Generación de órdenes de pago interbancario (SPEUA, IDEA, EDI) con cargo a una cuenta de vista.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Inversiones (Plazos, bajío premier).

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Inversión a plazo fijo con cargo a una cuenta de vista.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Operaciones con cheques.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Operaciones con tarjetas de débito.

Alcanzado. Existen las transacciones y hay acceso directo a ellas.

- Pago de impuestos con cargo a una cuenta de vista.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Pago de servicios (luz, teléfono, colegiaturas, agua, etc. con cargo a una cuenta de vista).

Alcanzado. Existen las transacciones y hay acceso directo a ellas.

- Pagos a terceros con cargo a una cuenta de vista, ejemplo: pago a proveedores.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Proceso y dispersión de nómina electrónica con cargo a una cuenta de vista.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Reporte de robo o extravío de cheques y tarjetas de débito.

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Reposiciones de tarjeta, reexpedición de NNIIPP.

Alcanzado. Existen las transacciones y hay acceso directo a ellas.

- Tesorería Empresarial (concentración y dispersión de fondos).

Alcanzado. Existen las transacciones y hay acceso directo a ellas.

- Transferencias de fondos (propias, terceros, ligas a cuentas de terceros, SPEUA, Pago Interbancario, verificación de cuentas).

Alcanzado. Existe la transacción y hay acceso directo a ella.

- Tasas y tipo de cambio

Alcanzado. Existe la transacción y hay acceso directo a ella.

- en el momento en que el portal esté al aire.

Alcanzado. Las transacciones estuvieron disponibles desde el mismo momento que estuvo disponible el sitio.

- Construir el sistema asegurando que será de fácil manejo.

Alcanzado. Gracias a su presentación y uniformidad el sistema es de muy fácil manejo.

- Construir el sistema con la modularidad suficiente para asegurar que será a través de él que los clientes realizarán todas las operaciones que los clientes puedan realizar utilizando Internet (integral).

Alcanzado. Se han agregado operaciones después del lanzamiento y se han hecho transacciones con nuevos backends sin problemas, siempre bajo el mismo esquema.

- Construir el sistema utilizando técnicas de programación de orientación a objetos.

Alcanzado. Tanto eZ Publish como los nuevos módulos están programados utilizando orientación a objetos.

- Construir el sistema garantizando que no presentará fallas[xxx]. Lograr robustez.

Alcanzado. Gracias a las pruebas unitarias, integrales y con el usuario una vez que se han lanzado las transacciones al portal, no han presentado fallas.

- Construir el sistema para que los tiempos de respuesta a las peticiones de los clientes sea el menor posible (rápido).

Alcanzado. Estamos operando con menores tiempos de respuesta que la media.

Seguridad

La seguridad debe abarcar todos los aspectos de la solución, es decir debe incluir protección desde el sistema operativo hasta la aplicación en sí, pasando por todas las herramientas intermedias que intervienen.

Es por ello que el objetivo es que nunca el sistema sea comprometido, ni a nivel de sistema operativo o herramientas ni a nivel de aplicación. Estamos hablando de que nunca sufra una intrusión.

Alcanzado. ***Desde su lanzamiento el sistema jamás ha sufrido una intrusión. Se han vivido problemas con ataques tipo DOS[cxxxi], pero nunca han sido graves y se ha reaccionado a tiempo para combatirlos. Una parte muy importante de los ataques de este tipo se ha debido a virus y no a grupos o individuos que intenten una penetración.***

El objetivo con respecto a la seguridad del contenido es muy simple: nunca deberá ser modificado por alguien que no cuente con la autorización respectiva para hacerlo.

Alcanzado. ***El contenido jamás ha sido modificado por alguien que no tuviera permisos para hacerlo.***

Por lo que respecta a las transacciones bancarias, el parámetro es que nunca se debe permitir realizar una transacción a alguien que no se haya autenticado como el legítimo cliente.

Alcanzado. ***Hasta el momento en ninguna de las auditorías contables realizadas a Bajionet se ha encontrado una irregularidad.***

En cuanto a la información de los clientes y su información financiera ésta nunca debe ser vista por alguien distinto del cliente mismo.

Alcanzado. ***Gracias a SSL jamás hemos recibido un reporte de que alguien haya interceptado información que no sea la suya o de que a alguien le hayan interceptado su información.***

Conclusiones

A lo largo de este trabajo hemos puesto de manifiesto nuestros conocimientos sobre:

- Sistemas operativos.
- Seguridad informática.
- Compiladores.
- Redes de computadoras.
- Bases de datos.
- Programación de sistemas.
- Ingeniería de software.

Y hemos demostrado capacidad para resolver con éxito problemas de Ingeniería en Computación, así como de poner por escrito tales hechos.

El sistema en su conjunto

Hoy en día el sistema en su conjunto es la siguiente (diagrama 17) granja de servidores:

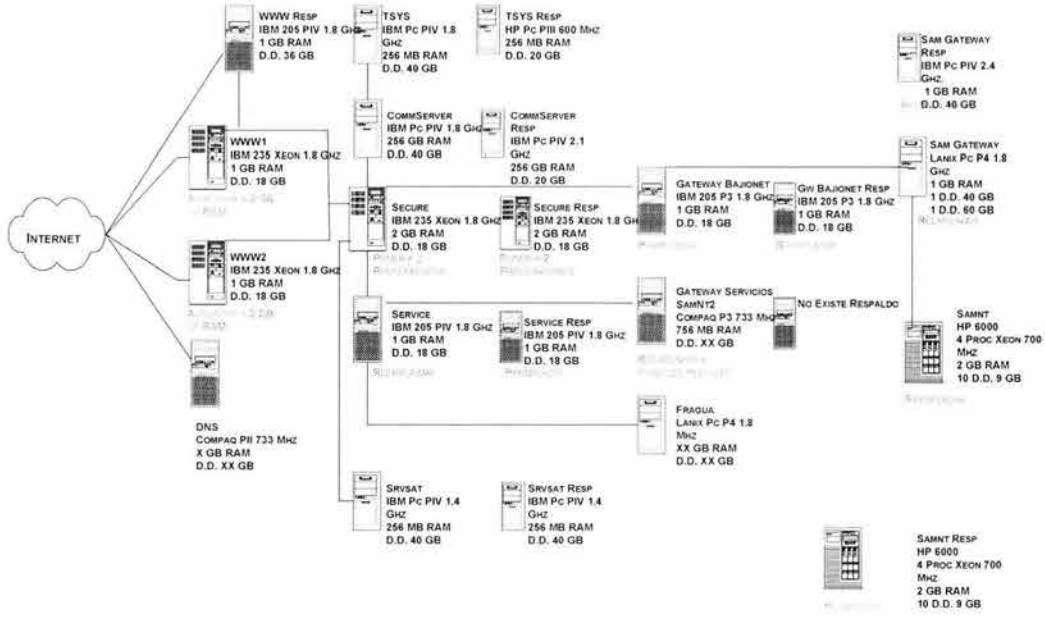


Diagrama 17 Granja de servidores que atiende hoy en día Bajionet.

El hecho de que haya hoy en día una inversión tan importante por parte de BB en su infraestructura, es sin duda reflejo de la satisfacción y la confianza que el Banco le tiene a esta solución.

Cuando un cliente le apuesta a una solución como lo ha hecho BB, no hay la menor duda de que se han obtenido resultados muy positivos con ella.

Nosotros creemos que el éxito no ha sido gratuito. La ventaja de que se haya hecho una conceptualización global adecuada y que se haya alcanzado el 100% de los objetivos planteados, demuestra que, cuando se hacen bien las cosas, se obtienen buenos resultados.

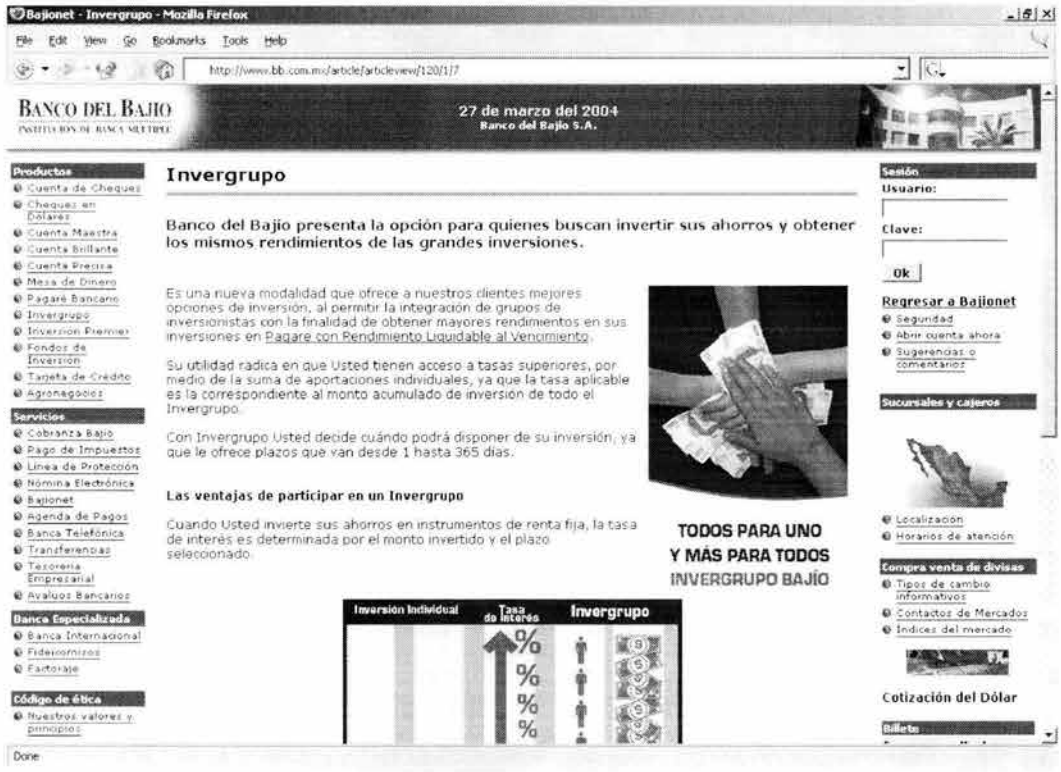
El éxito ha sido tal que Banco del Bajío le vendió, tanto en términos de convencimiento como en términos económicos, su solución a American Express Bank México.

El sistema de administración de contenido

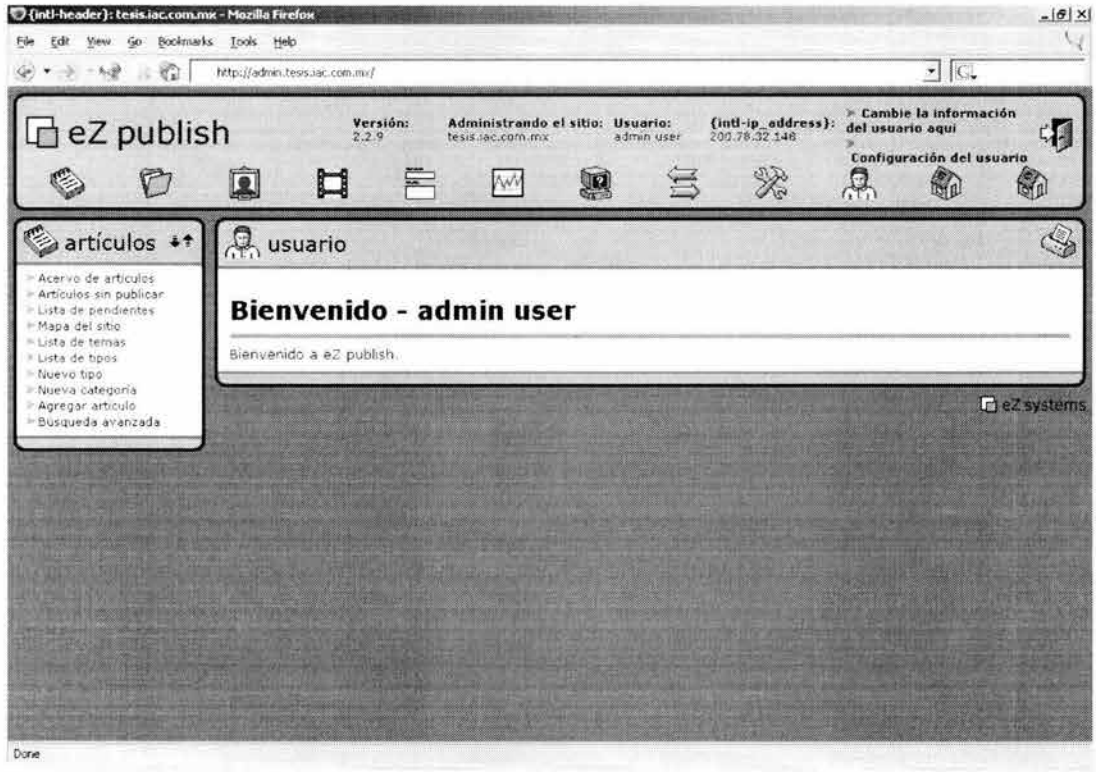
Gracias al diseño moderno (pantalla 24), al sistema de administración de contenido (pantalla 25) y a los usuarios satisfechos estuvimos entre los mejores 10 de un iBest[xxxii] en el año 2002.

El área de mercadotecnia opera cotidianamente y sin problemas el sistema de administración (pantalla 26) de contenido, desde su escritorio, gracias a eZ Publish Desktop Edition. Siendo ésta un área donde no suele haber conocimientos técnicos esto es un logro indiscutible.

Pantalla 24 Página principal.



Pantalla 25 Páginas de información.



Pantalla 26 Páginas del administrador.

El SAC se usó para el sitio y para la ayuda del mismo, demostrando con esto una gran flexibilidad y capacidad de separación del contenido en secciones y usos.

Como dato interesante adicional podríamos mencionar que el desarrollo involucró:

- 21453 Líneas nuevas de código PHP.
- 11880 Líneas nuevas de plantillas.
- 5718 Líneas nuevas de archivos de internacionalización.

El sistema aplicativo o transaccional

Su concepción y su construcción flexible, gracias al apego a estándares y sistemas abiertos, le ha permitido y le permitirá crecer y adaptarse a las necesidades que tenga el banco. No hay duda de que tiene un futuro brillante.

Su flexibilidad es más evidente cuando vemos la gama de transacciones que maneja:

- Integración de SNA tarjetas de crédito.
- Integración de applet nuevo pago de impuestos.
- Integración de domiciliación.
- Integración de pago de servicios y nómina electrónica.
- Integración de procesos que requieren de transferencia de archivos.

La seguridad

Nunca ha habido una intrusión ni cambio de contenido. ¿Qué más puede pedirse con respecto a la seguridad?

A futuro

Si somos creativos y nos gustan los retos, siempre hay espacio para crecer, para hacer más, mejorar e innovar. Así pues presentamos a continuación tres ideas simples sobre qué se puede hacer en el futuro con el sistema.

Administrador de transacciones

Debido a que utilizamos patrones, tenemos la facilidad de llevarnos el modelo que tenemos implementado a una versión más abstracta que sirva para generar nuevas transacciones sin necesidad de programas. Es decir podemos construir la parte del lado del administrador del módulo de transacciones que de manera que sirva tanto para darle mantenimiento a las que ya existen, como para crear nuevas transacciones, sin necesidad de programar, desde una interfase web.

Portal

Otra oportunidad de mejorar, esta vez en beneficio directo del cliente, sería darle un carácter más informativo al sitio. Tener en él noticias, tanto económicas como financieras, nacionales, internacionales, políticas, etc. y presentar todo convenientemente integrado con los servicios y productos de BB. Y aprovechando que eZ Publish tiene el soporte para hacerlo, debería publicarse la información de BB, para que otros la puedan incorporar a su contenido (RSS). Esto le conferiría el carácter de portal y no únicamente de sitio.

Personalización

Permitir que los usuarios seleccionen la organización del menú, el idioma del sistema, los nombres de sus cuentas, etc; todo ello forma las bases para dar un toque personal, para recibir y tener una atención más cálida, más a la medida y al gusto del cliente. Todo ello hecho por el cliente mismo. Agregar la funcionalidad necesaria para lograr esto es un interesante reto.

Glosario

A

acumulador: registro de la unidad aritmética lógica que se determina para operaciones aritméticas y para cargar y almacenar datos entre la CPU y la memoria principal.

acceso directo: es un ícono que permite abrir con más facilidad y rapidez un archivo o programa.

Address: señala la posición que ocupa una palabra en la memoria

ADA: lenguaje de programación que se originó para los sistemas de programación en tiempo real

AI: Artificial Intelligence: Inteligencia Artificial.

Algol: lenguaje de programación de alto nivel. Fue creado en 1958 para la investigación de las altas matemáticas.

Alfanumérico: algo compuesto de cifras y números.

algoritmo: es la especificación paso a paso del planteamiento para la resolución de un problema. El método algorítmico consiste en descomponer un problema en infinidad de secuencias o partes, para llegar al resultado final.. El método algorítmico es lo contrario del heurístico, cuyo objetivo es averiguar la verdad por medio de las hipótesis.

AMIBIOS: una de las marcas de BIOS más usadas.

ancho de banda: indica la cantidad de datos que pueden ser transmitidos en determinado lapso. En las redes se expresa en bps.

ANSI: siglas de American National Standard Institute o Instituto Americano de Normás Nacionales.

antivirus: programa que busca y elimina los virus informáticos.

AOL: America Online: proveedor de servicios de Internet de los Estados Unidos.

applet: pequeño programa en lenguaje de programación Java integrado en una página web.

árbol (tree): estructura de datos en la cual los registros son almacenados de manera jerárquica.

append: anexar. Acto de añadir algo al fin de una cosa.

ARPA: Advanced Research Proyects Agency: Agencia del Departamento de Defensa de los Estados Unidos que creó ARPAnet, red que dio origen a Internet.

ARPANet: Advanced Research Proyects Agency Network: Red de comunicación desarrollada por ARPA a fines de la década de los 60. Se la considera el origen de la Internet.

arquitectura: conjunto de las características, disposiciones e interconexiones de los principales componentes de un sistema operativo.

artificial intelligence (Inteligencia artificial): bajo este concepto se agrupan todas las tecnologías que estudian y desarrollan los problemas del conocimiento y la creación de máquinas con capacidad de razonamiento independiente y autoaprendizaje.

ASCII: acrónimo del American Standard Code of Information Interchange: Código normalizado para el intercambio de la información. Código que permite definir caracteres alfanuméricos; se lo usa para lograr compatibilidad entre diversos equipos de procesamiento y comunicación de datos.

AutoCad: programa de dibujo técnico muy utilizado especialmente por los arquitectos.

avatar: en ciertos chats de la World Wide Web, un avatar es una imagen que representa al usuario, con la misma función de un login name.

B

backup: duplicado o salvaguarda. Copia de seguridad en una memoria auxiliar. Se hace para prevenir una posible pérdida de información.

banner: gráfico, generalmente rectangular, que se inserta en una página web. Generalmente se utiliza para publicitar.

base de datos: conjunto de datos organizados que se puede editar y gestionar para buscar información o trabajar con ella.

BASIC: Beginner's All-Purpose Symbolic Instruction Code: Código de Instrucción Simbólica Multipropósito para Principiantes. Lenguaje de programación muy popular y simple creado en 1963.

Batch (lote): es un modo de tratamiento tal que un programa es introducido en la computadora y el resultado se obtiene luego y por lotes.

Baudio: unidad utilizada en transmisiones telefónicas o telegráficas que representa la velocidad de modulación de una señal.

BBS: (Bulletin Board System): sistema de servicios que opera automáticamente, por programas, al que se accede por módem y ofrece servicio de mensajería, juegos y descarga de archivos.

benchmark: programa especialmente diseñado para realizar pruebas o ensayos comparativos sobre distintos hardware para ver sus características.

Bidireccional: hilo conductor por el que los datos pueden transitar en un sentido o en otro.

Binario: sistema de numeración cuya base es 2 y es el utilizado por las computadoras

BIOS: Basic Input/Output System: Sistema básico de ingreso/salida de datos. Conjunto de procedimientos que controla el flujo de datos entre el sistema operativo y dispositivos tales como el disco rígido, la placa de video, el teclado, el mouse y la impresora.

bit: contracción de la palabra inglésa Binary Digit.. Abreviatura de binary digit (dígito binario). El bit es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora.

Board: (placa): soporte donde se colocan los circuitos integrados y los componentes electrónicos de la computadora.

Bookmarck: anotación o marca de una dirección de Internet que se hace con el navegador a fin de entrar a ella más ágilmente en posterioridad.

Boot (bootear): iniciar la puesta en marcha de una computadora

BPS: bits por segundo.

browser: navegador.

buffer: memoria intermedia. Area de la memoria que se utiliza para almacenar datos temporariamente. Cumple la función de cuaderno de notas para guardar información hasta que algún otro sistema esté dispuesto a recibirla.

bug: polilla, bicho, insecto. Término que expresa error de programación.

Bus: término electrónico procedente de la abreviación de ómnibus y que describe el conjunto de líneas que transportan las señales de funciones analógicas. Cualquier microprocesador tiene tres buses: el bus de datos, el de dirección y el de mando.

buscador, motor de búsqueda: search engine. Programa, ubicado en un sitio de Internet, que recibe un pedido de búsqueda, lo compara con las entradas de su base de datos y devuelve el resultado. Algunos de los más conocidos: Yahoo, Altavista, Lycos, Infoseek.

Aparte están los metabuscadores que buscan en los motores de búsqueda.

byte: unidad de información utilizada por las computadoras. Cada byte está compuesto por ocho bits. Y representa un carácter.

C

cache memory: memoria de alta velocidad utilizada como intermedia entre la CPU y la memoria principal para almacenar secuencias de instrucciones.

cable coaxial: cable coaxil.

cable coaxil : cable de conexión eléctrica que comprende a la vez un conductor interior y otro exterior. Es utilizado por muchas compañías de televisión por cable y para suministrar conexión a Internet mediante cablemódem.

cable-módem: módem que conecta una computadora con Internet a alta velocidad. Permite conexiones permanentes.

caché: en un navegador, el caché guarda copias de documentos de acceso frecuente, para que en el futuro aparezcan más rápidamente.

CAD: Computer Aided Design: Diseño Asistido por Computadora. Software que permite crear dibujos de precisión, bidimensionales y tridimensionales. Lo usan principalmente arquitectos e ingenieros.

call: llamada. Instrucción que se utiliza para desviar la secuencia de ejecución de un programa hacia un subprograma.

cassette: cinta magnética utilizada para registros de audio e informáticos.

carácter: número, letra o símbolo en la computadora, formado por un byte.

CD-ROM: Compact Disk - Read Only Memory. Disco óptico ROM. Tiene una capacidad de almacenamiento de por lo menos 650 megabytes.

Celeron: microprocesador de la familia Intel, de menor costo que el Pentium II.

chat: charla. Servicio de Internet que permite a dos o más usuarios conversar en línea y en tiempo real utilizando el teclado.

chip: abreviatura de "microchip". Circuito muy pequeño, compuesto por miles a millones de transistores impresos sobre una oblea de silicio.

cibercafé: bar donde, además de beber y comer, los clientes pueden usar computadoras para acceder a Internet.

clipboard: portapapeles.

cluster: grupo; racimo; agrupamiento. En la tecnología de las computadoras, un cluster es la unidad de almacenamiento en el disco rígido. Un archivo está compuesto por varios clusters, que pueden estar almacenados en diversos lugares del disco.

command: comando o instrucción que un usuario imparte al sistema operativo para que realice una acción determinada.

compilador: intérprete. Programa traductor que convierte las instrucciones de un lenguaje avanzado en secuencias de instrucciones binarias llamadas código objeto para poder ejecutarlas.

computadora: dispositivo electrónico para realizar operaciones aritméticas y lógicas de alta velocidad. Consta de cinco componentes básicos: la unidad aritmética lógica (ALU), la unidad de control, dispositivos de entrada y salidad de datos y memoria.

computer system: sistema informático.

Concentrador: procesador programado para combinar datos transmitidos por varios dispositivos de baja velocidad y luego transmitirlos a una velocidad mucho mayor, generalmente a una computadora remota.

comprimir: reducir el tamaño de un archivo. Se hace para ahorrar espacio o para transmitirlo a mayor velocidad. Uno de los programas de compresión más populares de Windows es WinZip.

Controlador: unidad que controla la ejecución de las instrucciones de la computadora y su secuencia de operaciones.

Control Unit: elemento de la CPU que recibe instrucciones de un programa, lo decodifica y envía señales a las unidades correspondientes de la computadora para ejecutar la instrucción.

cookie: pequeño archivo de texto que un sitio web coloca en el disco rígido de una computadora que lo visita. Agiliza la navegación en el sitio. Su uso es controvertido, porque pone en riesgo la privacidad de los usuarios ya que toma información sobre el mismo.
CPU: Central Processing Unit. Unidad central de procesamiento.
CPS: siglas que indican caracteres por segundo.
CRT: Cathode Ray Tube. Tubo de rayos catódicos de un monitor.
cursor: forma luminosa que se desplaza por el monitor, generalmente centelleante o en forma de flecha y señala la posición activa.

D

data: dato. Información que se facilita a la computadora
database: base de datos. Organización sistemática de archivos de datos para facilitar el acceso, búsqueda y actualización.
Data entry: proceso de ingresar datos a una computadora para su procesamiento.
debugger: depuración, corrección de errores o bugs.
Decoder: decodificador o descifrador.
default: por defecto. Por omisión.
delete: borrar; eliminar; anular.
Desktop publishing. Autoedición. Se trata de un sistema que permite la creación de publicidades mediante el uso de la computadora y otros elementos.
Digit: cifra. Carácter numérico comprendido entre el cero y el nueve.
diodo: componente electrónico que permite el paso de la corriente eléctrica en un solo sentido.
Density: densidad.. Cantidad de caracteres que se pueden registrar en una determinada longitud de superficie de grabación y que es expresada en bits o bytes por pulgada.
Digitalizar: traducir datos analógicos a digitales.
directorio (directory): catálogo o biblioteca. Es una lista de archivos relacionados entre sí que se guardan bajo un nombre. Un directorio puede contener a su vez otros directorios llamados subdirectorios.
Disable: desactivar.
disco rígido: unidad de almacenamiento magnética en forma de placa circular. Los datos se graban en pistas concéntricas.
display: unidad de visualización; monitor; pantalla.
download: descargar, bajar. Transferencia de información desde Internet a una computadora.
dpi: dots per inch: puntos por pulgada. En las impresoras, la calidad de la imagen sobre el papel se expresa en dpi. Medida de la densidad y nitidez de una impresión gráfica.
DSL: Digital Subscriber Line: Línea Digital de Suscripción. Tecnología que permite enviar gran cantidad de información a disco.
display: unidad de visualización; monitor; pantalla.
download: descargar, bajar. Transferencia de información desde Internet a una computadora.
dpi: dots per inch: puntos por pulgada. En las impresoras, la calidad de la imagen sobre el papel se expresa en dpi.
Draw: operación en la que los datos se leen inmediatamente después de grabados en un videodisco para determinar errores.
Drive device: unidad de transporte.

DSL: Digital Subscriber Line: Línea Digital de Suscripción. Tecnología que permite enviar mucha información a gran velocidad a través de líneas telefónicas.
Dúplex: medio de comunicación bidireccional que permite la transferencia simultánea en los dos sentidos
DVD: Digital Versatile Disc: Disco Versátil Digital. Disco que posee gran capacidad de almacenamiento y sirve también para almacenar películas.
Dynamic HTML: variante del HTML (Hyper TextMark-up Language) que permite crear páginas web más animadas.

E

echo: eco. Reflexión hacia la impresora o monitor de un carácter introducido por teclado.
Editor: programa sencillo para introducir textos en la computadora sin o con escaso formato
ELIZA: programa que simula la inteligencia artificial. Fue desarrollado en 1966 por el doctor Joseph Weizenbaum, quien se basó en la entrevista psicoanalítica para elaborar un modo de interacción entre el ser humano y la máquina. El programa trabajaba con patrones de reconocimiento y reemplazo de palabras clave por frases predeterminadas. Permite a una computadora mantener una conversación simple. La versión original fue escrita en LISP.
e-mail: correo electrónico.
emulación: emulation. Mediante ella una computadora imita a otro mediante la utilización de un software.
encriptar: proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.
end: instrucción que determina el fin de un programa y luego devuelve el control de la computadora al teclado.
Enter: es la tecla que ordenala puesta en memoria de la secuencia tecleada. También se llama Return.
Environment: entorno.
ergonomía: consideración del elemento humano en el diseño de ingeniería. Estudio del diseño de dispositivos con el objetivo de ofrecer comodidad y eficiencia.
ESC: abreviatura del carácter escape.
extranet: parte de una intranet de acceso disponible a clientes y otros usuarios ajenos a la compañía.

F

Fatal error: error que cuando se produce durante la ejecución de un programa lo traba y no permite seguir ejecutándose.
fax. Facsimil. Equipo y proceso de transmisión de material impreso mediante la conversión de las imágenes en señales eléctricas que luego se recomponen en su forma original en la estación receptora.
FAQ: frequently-asked questions. Las preguntas más frecuentes (y sus respuestas) sobre temas especialmente de sitios web.
Feedback: realimentar.
fibra óptica: tecnología para transmitir información como pulsos luminosos a través de un conducto de fibra de vidrio. La fibra óptica transporta mucha más información que el cable de cobre convencional.
file: archivo.
file not found: no se encuentra el archivo.
field: campo. Zona lógica dentro de una instrucción, dirección o comentario.
firewall: mecanismo de seguridad y protección. Se utiliza para impedir el acceso a una red.
fixed disk: disco fijo.
flag: bandera o indicador de estado. Es una señal permanente que se conserva en un registro como indicador.

floppy disk: disquete o disco flexible.
flowchart: cursograma. Es la representación gráfica, mediante símbolos convencionales, de los diferente pasos que llevan a la resolución de un programa.
flow diagram: diagrama de flujo.
folder: carpeta. Cursograma que describe la utilización de un algoritmo con el fin de resolver un problema.
font: fuente. Es una variedad completa de caracteres de imprenta de un estilo y tamaño determinados.
format: formato.
formateo: operación para preparar un disco virgen para darle una estructura utilizable por una computadora
FORTRAN: traducción de fórmulas. Es un lenguaje para los cálculos numéricos.
frame: estructura.
Front end: La parte de un sistema que interactuar con el usuario. La intefase, ya sea gráfica o de texto. La parte de un sistema que interactuar con otro sistema, en este caso a través de algún protocolo de comunicación común.
fragmentación: presencia de posiciones de memoria en la memoria principal.
frecuencia: número de ciclos por segundo.
FTP: File Transfer Protocol: Protocolo de Transferencia de Archivos. Se utiliza para enviar y recibir archivos de Internet.
fuente: variedad completa de caracteres de imprenta de un determinado estilo y tamaño.
full dúplex: dúplex integral. Medio de comunicación que permite una transmisión bidireccional simultánea.
función: programa de computación que permite obtener soluciones a problemas. Siempre posibilita la obtención de un resultado único.

G

galletas: mecanismo que tienen los navegadores para aceptar, reenviar y guardar información que los servidores de páginas les envían.
gateway: compuerta. Circuito que realiza una función lógica simple para comunicar redes.
giga: prefijo que indica un múltiplo de 1.000 millones, o sea 109.
gigabit: Aproximadamente 1.000 millones de bits (exactamente 1.073.741.824 bits)
gigabyte (GB): unidad de medida de una memoria. 1 gigabyte = 1024 megabytes = 1.073.741.824 bytes.
global variable: variable global. Variable cuyo valor es accesible desde todas las partes del programa.
grid: grilla. Cuadrícula para representar conjuntos de datos en forma de tabla.

H

hacker. Intruso o incursor.
half duplex: semi duplex. Transmisión de datos en un circuito en un sentido u otro.
handheld: Computadora de tamaño suficientemente pequeño para ser sostenida en la mano o guardada en un bolsillo. También se la llama PDA. En algunas se puede ingresar datos con escritura manual. Otras traen incorporados pequeños teclados.
hard disk: disco rígido. Disco de soporte rígido que se recubre de una sustancia magnética y tiene mayor capacidad de almacenamiento que un disquete.
hardware: Significa fierros o ferretería y comprende todos los componentes físicos de la computadora y sus periféricos.
header: encabezamiento.

help: ayuda.
hertz: hercio. Unidad de frecuencia electromagnética. Equivale a un ciclo por segundo.
hexadecimal: representación numérica con base 16 en la que se emplean los números del 0 al 9 y las 6 primeras letras del alfabeto a fin de representar los valores alfanuméricos del 0 al 15.
holograma: imagen tridimensional creada por proyección fotográfica.
host: anfitriona. Computadora central a la que convergen varias líneas de una red.
hosting: alojamiento. Servicio ofrecido por algunos proveedores, que brindan a sus clientes un espacio en su servidor para alojar un sitio web.
HTML: Hyper Text Mark-up Language. Lenguaje de programación para armar páginas web.

I

ícono: imagen o símbolo que representa un programa u otro recurso. Los sistemas que utilizan este concepto incluyen por lo general un mouse o una pantalla sencible al tacto, o un lápiz óptico, para determinar las operaciones a ejecutar.
ICQ ("I Seek You"): Te busco: Programa para la comunicación online por Internet. Permite enviar mensajes y archivos, chatear, enviar archivos, mensajes de voz, tarjetas, etc.
image map: imagen de una página web que permite cliquear en diferentes áreas para acceder a diferentes destinos.
indexed: indexado. Indexar es clasificar o recuperar información.
infonesia: incapacidad de recordar en qué fuente se vio una información: diarios, televisión, libros, publicidad en la calle, etcétera.
input: entrada
inteligencia artificial: simulación de los procesos de la inteligencia humana, por medio de sistemas de computación.
interface: se trata del intermediario natural entre la computadora y sus periféricos; es decir, el medio que permite la comunicación entre la computadora y y el entorno y por ende, el usuario.
internal bus: barra colectora interna que transpota datos entre diversos registros y hacia o desde la ALU a la unidad de control.
internesia: la incapacidad de recordar en qué sitio de la Web se ha visto una información. Es una manifestación de una condición más general, que se conoce con el nombre de infonesia.
Internet2: proyecto de interconexión entre universidades estadounidenses que incluirá a muchas otras universidades del mundo con el fin de desarrollar una red de altísima velocidad para la educación y la investigación.
intranet: red de redes de una empresa. Su aspecto es similar al de las páginas de Internet.
IP: Internet Protocol. Protocolo de Internet.
IrDA (Infrared Data Association): Organización fundada para crear las normás internacionales para el hardware y el software usados en enlaces de comunicación por rayos infrarrojos. La tecnología de rayos infrarrojos juega un importante papel en las comunicaciones inalámbricas.
IRL: In Real Life: En la vida real. Abreviatura usada en el chateo en Internet.
ISO: International Organization for Standardization. Fundada en 1946, es una federación internacional que unifica normás en unos cien países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de comunicación.
ISP: Internet Service Provider. Proveedor de servicios de Internet.

J

jitter: variación en la cantidad de latencia entre paquetes de datos recibidos.
joystick: palanca vertical que se puede inclinar en todos los sentidos para determinar la dirección de un movimiento. Se trata de un periférico de entrada que se emplea en los juegos electrónicos.
jump: bifurcación.
jumper: puentear. Conductor eléctrico que se utiliza para conectar provisoriamente terminales de un circuito o puentear algún sector del mismo.

K

Kbyte: kilobyte. Unidad de medida de la memoria que equivale a 1.024 bytes.
kernel: núcleo. Rutinas del sistemma operativo responsables del manejo de las funciones básicas del sistema.
keyboard: teclado.
keyword: palabra clave o reservada.
kilobit: 1.024 bits.

L

Label: etiqueta.
LAN Manager: sistema operativo de red.
LAN: Local Area Network: Red de Área Local. Red de computadoras interconectadas en un área reducida, por ejemplo, una empresa.
language: lenguaje. Conjunto de reglas que permiten la comunicación con la computadora.
laptop: computadora portátil del tamaño aproximado de un portafolio. Hay otras más pequeñas como la palmtop.
LCD: Liquid Crystal Display. Pantalla de cristal líquido, usada generalmente en las notebooks y otras computadoras pequeñas.
library: biblioteca. Conjunto de programas.
link: enlace. Imagen o texto destacado, mediante subrayado o color, que lleva a otro sector del documento o a otra página web. También es un programa secundario que asegura el enlace entre dos programas principales.
load: cargar.
Log in, log on: entrar el línea o loguearse.
LOGO: lenguaje de programación destinado a la enseñanza que recurre especialmente a los gráficos. Una "tortuga" realiza los diseños lógicos indicados por el ordenador.
loop: lazo. Se trata de una sucesión de acciones ejecutadas tantas veces como sea necesario hasta la aparición de una señal de alto o salida.

M

Mac: Macintosh.
machine: máquina, procesador, computadora.
Macintosh: computadora que Apple empezó a fabricar en 1984. Fue la primera computadora personal que incorporó una interfase gráfica, con el propósito de facilitar un uso más intuitivo de la máquina. Tiene su propio sistema operativo. Es muy utilizada para el diseño gráfico por computadora.
macro: una sola instrucción que representa una determinada secuencia de instrucciones.

mailing: correspondencia.
mailing list: lista de correo.
mainframe: estructura principal. Computadora de gran tamaño de tipo multiusuario, utilizada en empresas.
mainframe: unidad principal.
Majordomo: pequeño programa que automáticamente distribuye mensajes de e-mail a usuarios suscriptos a una lista de correo.
MD5: es un algoritmo para validar la integridad de un conjunto de datos, es mucho más confiable que otros métodos para hacer lo mismo.
megabit: Aproximadamente 1 millón de bits. (1.048.576 bits).
megabyte (MB): megaocteto. Unidad de medida de una memoria. 1 megabyte = 1024 kilobytes = 1.048.576 bytes.
Megahertz (MHz): Un millón de hertz o hercios.
memoria caché: pequeña cantidad de memoria de alta velocidad que incrementa el rendimiento de la computadora almacenando datos temporariamente.
Memoria: dispositivo que puede almacenar datos registrados en él y del cual se pueden recuperar.
Message: mensaje.
Middleware: Se dice del software o sistema que hace las veces de capa intermedia entre dos sistemas distintos. También se le nombra gateway y generalmente tiene una labor de traducción o de conversión de datos, mensajes y protocolos.
microprocesador (microprocessor): micropastilla o chip principal de una computadora. Su velocidad se mide en MHz (Megahertz).
microprograma: programa especial que asegura la secuencia de la unidad de control de un procesador.
minicomputer: minicomputadora: computadoras que no necesitan de un entorno especial y operadores altamente especializados.
mirror site: sitio espejo. Sitio web copiado a otro servidor para facilitar el acceso a él desde otros lugares.
MMX: MultiMedia eXtension. Microprocesador Pentium diseñado para dar mayor velocidad a aplicaciones multimedia.
módem: modulador-demodulador. Periférico que permite la comunicación entre dos computadoras.
motherboard: placa madre.
mouse: ratón. Puntero electrónico de mano que se desplaza sobre una superficie y determina los movimientos del cursor sobre la pantalla del monitor.
MP3: MPEG-1 Audio Layer-3. Formato y tecnología estándar para comprimir sonido en archivos muy pequeños (de aproximadamente la duodécimaparte de su tamaño original), preservando la calidad de la emisión.
MPEG: el Moving Pictures Expert Group desarrolla estándares para video digital y compresión de audio. Tiene el auspicio de la ISO.
MS-DOS: Microsoft Disk Operating System: Sistema operativo del Disco Microsoft.
multicasking: multitarea o varias tareas al mismo tiempo.

N

nano: prefijo que significa una milmillonésimaparte.
nanosegundo: milmillonésima de segundo. Es una medida común para determinar el tiempo de acceso a la memoria RAM.
navegador: programa para recorrer sitios web.
netiquette: conjunto de reglas de etiqueta tácitas dentro de Internet.

network: red. Sistema electrónico de comunicaciones que enlaza varias computadoras, periféricos y unidades de memoria y permite compartir recursos.
newsgroup: grupo de discusión que se comunica por Internet.
nodo: dispositivo o grupo de dispositivos que unen dos o más unidades adicionales en una red.

O

offline: fuera de línea.
online: en línea, conectado.
OSI: Open Systems Interconnection: Interconexión de Sistemas Abiertos. Norma universal para protocolos de comunicación.
output: salida.
overlay: superposición.
overwrite: sobreescribir.

P

paquete (packet): conjunto de programas para una aplicación específica. También son las fracciones en que se divide la información para viajar por Internet.
PASCAL: lenguaje de programación de alto nivel creado por Niklaus Wirth.
password: contraseña.
performance: desempeño, rendimiento.
pixel: combinación de "picture" y "element". Elemento gráfico mínimo con el que se componen las imágenes en la pantalla de una computadora.
Plataforma: combinación unica sistema operativo con hardware, por ejemplo Linux corriendo sobre procesadores i386, Lintel.
plug & play: significa "enchufar y usar". Reconocimiento inmediato de un dispositivo por parte de la computadora, sin necesidad de instrucciones del usuario.
PoP: Point of Presence. Punto de acceso a Internet.
POP3 (Post Office Protocol 3): Protocolo 3 de Correo. Es un protocolo estándar para recibir e-mail.
Port: puerta de entrada-salida a una computadora.
print: imprimir.
procesador (processor): dispositivo capaz de realizar operaciones con los datos.
programa: secuencia de instrucciones correspondientes a un algoritmo.
protocolo: conjunto de reglas que determinan los formatos por los cuales se puede intercambiar información entre diferentes sistemas.
proveedor de servicios de Internet: compañía que ofrece una conexión a Internet, e-mails y otros servicios relacionados, tales como la construcción y el hosting de páginas web.
puerto paralelo: conexión por medio de la cual se envían datos a través de varios conductos. Una computadora suele tener un puerto paralelo llamado LPT1.
puerto serial: conexión por medio de la cual se envían datos a través de un solo conducto. Por ejemplo, el mouse se conecta a un puerto serial. Las computadoras tienen dos puertos seriales: COM1 y COM2.
prompt: listo, preparado o dispuesto. Indicación visible de la computadora con la que esta señala que se requiere una respuesta por parte del operador.

Q

Quality of Service: Calidad de servicio. En Internet y otras redes, designa la posibilidad de medir, mejorar y, en alguna medida, garantizar por adelantado los índices de transmisión y error. Es importante para la transmisión fluida de información multimedia: por ejemplo, para los usos académicos de Internet2.

query: consulta. Búsqueda en una base de datos.

queue: cola de espera

R

RAM: Random Acces Memory: Memoria de acceso aleatorio . Es de lectura y escritura.Memoria donde la computadora almacena datos que le permiten al procesador acceder rápidamente al sistema operativo, las aplicaciones y los datos en uso. Se mide en megabytes.

Realidad virtual: Simulación de un medio ambiente real o imaginario que se puede experimentar visualmente en tres dimensiones. La realidad virtual puede además proporcionar una experiencia interactiva de percepción táctil, sonora y de movimiento.

reboot: rebutear.

rebutear: volver a cargar el sistema operativo de una computadora que se ha "colgado".

record: registro activo.

red: en tecnología de la información, una red es un conjunto de dos o más computadoras interconectadas.

reset: puesta a cer.

residente: programa alojado en memoria.

RIPEMD-160: es una función de hash de cifrado de 160 bits, diseñada por Hans Dobbertin, Antoon Bosselaers, y Bart Preneel. Se considera como un reemplazo de funciones como MD4, MD5 y RIPEMD

ROM: Read Only Memory: Memoria de sólo lectura. Memoria incorporada que contiene datos que no pueden ser modificados. Permite a la computadora arrancar. A diferencia de la RAM, los datos de la memoria ROM no se pierden al apagar el equipo.

router: ruteador. Sistema constituido por hardware y software para la transmisión de datos en Internet. El emisor y el receptor deben utilizar el mismo protocolo.

RPC: Remote Procedure Call, mecanismo para ejecutar o utilizar programas remotos a través de una interfase de programación.

run: procesar, pasar.

S

sampling: muestreo.

save: grabar o guardar

ScanDisk: programa de Windows que revisa un disco, detecta errores y los corrige.

search: búsqueda.

server: servidor.

servidor: computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas.

shortcut: atajo. Véase acceso directo.

sílice: compuesto resultante de la combinación del silicio con el oxígeno. Abunda en la naturaleza y forma el cuarzo, el pedernal, etc.

silicio: metaloide (sustancia química que tiene la apariencia de un metal) sólido, amarillento, difícil de fundir e insoluble en el agua. Se extrae de la sílice.
Silicon Valley: Valle del Silicio. Región del Norte de California, EE.UU. (cerca de San Francisco), donde están instaladas la mayoría de las empresas que desarrollan productos para la tecnología informática.
simulación: método de enseñanza que sitúa al sujeto en condiciones hipotéticas a fin de probar su comportamiento ante situaciones determinadas.
sistema operativo: programa que administra los demás programas en una computadora.
software: término general que designa los diversos tipos de programas usados en computación.
Skip: salto.
Slot: ranura
spam: correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a Internet.
suite: Conjunto de programas que se comercializan en un solo paquete.

T

tag: etiqueta. Colección de caracteres o dígitos asignados a un registro como medio de identificación del mismo.
talk: charlar.
tamagotchi: pequeño juguete digital.
task: tarea.
TCP/IP: Transfer Control Protocol / Internet Protocol. Es el protocolo que se utiliza en Internet.
terminal: aparato compuesto generalmente por un teclado, pa, un circuito de control y a veces un módem, que permite la comunicación a distancia con una computadora.
toolbar: barra de herramientas.
tools: herramientas.
touch pad: pequeña superficie sensible al tacto, incorporada al teclado de una computadora. Cumple las mismás funciones que el mouse.
tree: árbol. Estructura de datos donde los registros son almacenados de una forma jerárquica.
Troyano (caballo de Troya): programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del disco rígido.

U

Unix: sistema operativo multiusuario desarrollado por los laboratorios Bell. Fue muy importante en el desarrollo de Internet.
unppack: descomprimirr.
updating: actualización de ficheros.
USB (Universal Serial Bus): es una interfase de tipo plug & play entre una computadora y ciertos dispositivos, por ejemplo, teclados, teléfonos, escáners e impresoras.

V

variable: entidad simbólica que se utiliza en un programa.
VC: Virtual Community: comunidad virtual.
vector: programa de graficación, parámetros que verifican la dirección y distancia de un punto al otro.

videoconferencia: conversación entre dos o más personas que se encuentran en lugares diferentes pero pueden verse y oírse. Las videoconferencias que se realizan fuera de Internet requieren que en cada lugar donde se encuentran los participantes se disponga de una videocámara especial y de dispositivos para presentación de documentos. En la Web, productos como CU-SeeMe y NetMeeting permiten hacer chat con video.

virtual PC: programa que emula Windows 95 en una Macintosh.

virus hoax: falsa alarma sobre virus que suele llegar por e-mail.

virus: pequeño programa que "infecta" una computadora; puede causar efectos indeseables y hasta daños irreparables.

W

WAIS: Servicio de Información de Area Amplia (Wide Area Information Service). Es una herramienta que permite encontrar información almacenada en archivos o en bases de datos a través de Internet.

WAN: Red de área mundial (World Area Network). Puede extenderse a todo un país o a muchos a través del mundo.

Web: Vea World Wide Web.

Web PC ó Web TV: Vea Network Computer.

Website: Conjunto de páginas web que comparten un mismo tema e intención y que generalmente se encuentra en un sólo servidor, aunque esto no es forzoso.

Windows : Sistema operativo desarrollado por Microsoft que tiene la particularidad de trabajar por ventanas.

WinZip: programa de Windows que permite comprimir archivos.

wireless: inalámbrico.

word: palabra.

World Wide Web: Sistema basado en hipertextos cuya función es buscar y tener acceso a documentos a través de la red. Vea Altavista, CGI, Hipertexto, Herramientas de búsqueda, HTML, HTTP, Internet Explorer, Java, Mosaic, Netscape, Plugins, Visualizador, Yahoo!.

Write Pages: Listas de usuarios de Internet. Existen varios lugares donde los usuarios pueden registrarse y realizar búsquedas de personas.

WWW: Vea World Wide Web

workstation: estación de trabajo. Computadora personal conectada a una red. Puede ser usada independientemente de la mainframe, dado que tiene sus propias aplicaciones y su propio disco rígido.

WYSIWYG: Lo que se ve es lo que se obtiene. Característica de los programas avanzados de graficación que permite ver los trabajos en o pantalla en iguales proporciones en que se serán impresos.

X

Xerographics printer: impresora xerox en la que el papel está cargado eléctricamente en las zonas donde se van a representar caracteres.

XHTML: XML Hyper Text Mark-up Language. Lenguaje de programación para armar páginas web, que a diferencia del tradicional HTML es más estricto en su construcción y al apego del formato DTD que lo define.

Y

Y2K: Year 2 K: Año 2000. Muchos sistemas de computación utilizan software que registra las fechas con los últimos dos dígitos del año; por ejemplo, 97 representa el año 1997. Al llegar el año 2000, los dos últimos dígitos serán 00, y muchas computadoras los leerán como 1900, lo que podría causar fallas y hasta colapsos en los sistemas.

Z

Zero: cero. En lenguaje informático el cero se puede representar barrado para que no se confunda con la letra o.

zip drive: periférico para almacenamiento de datos. Cada zip drive puede contener hasta 100 MB (megabytes) o el equivalente a 70 disquetes.

zip: formato de los archivos comprimidos.

zipear: comprimir.

zona: sección de la memoria central reservada para una función o uso particular.

Glosario de traducciones

Expresión en inglés Traducciones preferidas Otras Traducciones
API (Applications Program Interface) API (Interfaz de los programas de aplicación)
Attachments Ataduras
Benchmarking Experimentación Prueba
Binding Ligadura
Browser Navegador
Clustering Agrupamiento
Compliant Compatible Conforme
Customize Personalizar
Dynamic Function
Linker Enlazador dinámico de funciones
Extent Extensión de la clase Extensional
Framework Marco de aplicación
Impedance mismatch Desadaptación de impedancias
Intension Intensional
Interface Interfaz
Late-binding Ligadura tardía
Lifetime Vida Duración
Map, Mapping Hacer corresponder,"mapear" Correspondencia
Method Materialization Materialización de métodos
Middleware Software intermedio
Object Request Broker Gestor de peticiones de objetos Intermediario entre objetos
ODL (Object Definition Language) Lenguaje de definición de objetos
ODMS (Object Data Management System) SGDO (Sistemas de gestión de objetos)
OID (Object Identifier) IDO (Identificador de objetos)
OIF (Object Interchange Format) Formato de intercambio de objetos
OML (Object Manipulation Language) Lenguaje de manipulación de objetos
Overloading Sobrecarga (de métodos)
Overriding Redefinición (de métodos) Anulación
Path expressions Expresiones de camino
Persistence capable classes Clases susceptibles de ser persistentes
Persistent Persistente
Pointer swizzling Transformación de punteros
RDBMS (Relational Database Management System) SGBDR (Sistema de gestión de bases de datos relacionales)
Reflection Reflectividad
Roots Raíces
Safeness Fiabilidad
Stores Almacenes
Table driven Dirigido por tablas
Transient Temporal Transitorio
Traversal paths Caminos de recorrido
Triggers Disparadores
Wrapper Envoltorio Mediador

Bibliografía

R. Fielding, UC Irvine, J. Gettys, J. Mogul, DEC, H. Frystyk, T. Berners-Lee, MIT/LCS, *Hypertext Transfer Protocol -- HTTP/1.1 RFC 2068*, http://www.ietf.org/rfc/rfc2068.txt, 1997

Tim Tsai, Navjot Singh, *Libsafe Protecting Critical Elements of Stacks*, http://www.research.avayalabs.com/project/libsafe/, 2001

Tim Tsai, Navjot Singh, *White paper describing the detection of format string vulnerability exploits*, http://www.research.avayalabs.com/project/libsafe/, 2001

Tim Tsai, Navjot Singh, *White paper describing the design, implementation, and performance of libsafe on Linux*, http://www.research.avayalabs.com/project/libsafe/, 2001

Sander Klein lids@roedie.nl, *Linux Intrusion Detection System FAQ*, http://www.lids.org/lids-faq/lids-faq.html

Huagang Xie (xie@lids.org), *The LIDS Project*, http://www.lids.org/about.html, 2003

Xie Huagang (xie@chinacluster.com, http://www.lids.org), *Build a Secure System with LIDS*, Oct 4, 2000

Xie Huagang (xie@chinacluster.com, http://www.lids.org/), *LIDS Installation*, http://www.lids.org/install.html, 2000

Tim Tsai, Navjot Singh, *Libsafe Protecting Critical Elements of Stacks*, http://www.research.avayalabs.com/project/libsafe/, 2001

Erich Stefan Boleyn, *Grub*, http://www.gnu.org/software/grub/, 21/03/2004

Erich Stefan Boleyn, *Página de manual de Grub*, http://www.gnu.org/software/grub/manual/html_node/index.html, versión 0.93, 25/01/2004

Roland McGrath, Ulrich Drepper y otros, *Página de manual de ld*, http://www.die.net/doc/linux/man/man8/ld.so.8.html, 2001

PHP documentation team, *Documentación PHP*, http://www.php.net/, 2002

MySQL AB, *MySQL Reference Manual*, http://www.mysql.com/doc/en/index.html, 2004

Zeev Suraski Zend Technologies Ltd., www.zend.com info@zend.com, *Zend Accelerator User Guide*, 16, 23/9/2001

Barry Hischfield Zend Technologies Ltd., www.zend.com info@zend.com, *Zend Encoder Unlimited 1.1 Technical FAQs*, 4, 16/7/2001

Barry Hischfield Zend Technologies Ltd., www.zend.com info@zend.com, *Zend Encoder Unlimited 1.1 User Guide*, 6, 16/7/2001

Andi Gutsman, Zeev Sursaki Zend Technologies Ltd., www.zend.com info@zend.com, *Zend Engine Version 2.0*, 37, 26/6/2001

Barry Hischfield Zend Technologies Ltd., www.zend.com info@zend.com, *Zend Optimizer User Guide*, 4, 12/8/2002

Lincoln D. Stein, *Web Security : A Step-by-Step Reference Guide*, 448, Addison-Wesley Pub Co, December 31, 1997

Sandip Bhattacharya, *Professional Apache Security*, 384, primera edición, Wrox Press Inc, 2003

Gene Spafford, Simson Garfinkel, Alan Schwartz, *Practical Unix & Internet Security*, 984, 3era edición, O'Reilly & Associates, 2003

Red Hat, Inc., *Kickstart guide*, http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/custom-guide/ch-kickstart2.html, 2002

Red Hat, Inc. *Manuales RedHat Linux*, http://www.redhat.com/docs/manuals/linux/, 2002

eZ systems, *Documentación eZ Publisher*, http://doc.ez.no/, 2003

OpenSSL team, *OpenSSL reference manual*, http://www.openssl.org/docs/apps/openssl.html, 2003

The Apache Software Foundation, *Manuales Apache*, http://httpd.apache.org/docs-2.0/, 2004

The Apache Software Foundation, *Manuales Apache mod_ssl*, http://httpd.apache.org/docs-2.0/mod/mod_ssl.html, 2004

Ralf S. Engelschall rse@engelschall.com www.engelschall.com, *Manuales mod_ssl*, http://www.modssl.org/, 2001

Tatu Ylonen, Aaron Campbell, Bob Beck, Markus Friedl, Niels Provos, Theo de Raadt and Dug Song Markus Friedl, Niels Provos and Markus Friedl, *Documentacion sshd*, http://www.openbsd.org/cgi-bin/man.cgi?query=sshd, 1999

T. Ylonen, T. Kivinen, M. Saarinen, T. Rinne, and S. Lehtinen, *SSH Protocol Architecture, draft-ietf-secsh-architecture-12.txt*, 2002

M. Friedl, N. Provos, and W. A. Simpson, Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol, draft-ietf-secsh-dh-group-exchange-02.txt, 2002

Tripwire, Inc., *Manual de Tripwire (twintro(8), twadmin(8), twprint(8), siggen(8), twconfig(4), twpolicy(4), twfiles(5))*, http://www.tripwire.org/qanda/index.php, 2001

Gene Kim, Eugene Spafford, The Design and Implementation of Tripwire: A UNIX File Integrity Checker. Purdue Technical Report CSD-TR-93-071, 1993

Greg Wettstein (greg@wind.enjellic.com) , Martin Schulze (joey@linux.de) , Steve Lord (lord@cray.com), Greg Wettstein greg@wind.enjellic.com, Stephen Tweedie sct@dcs.ed.ac.uk, Juha Virtanen jiivee@hut.fi, Shane Alderton shane@ion.apana.org.au, Martin Schulze Infodrom Oldenburg joey@linux.de, *Man syslog (8) syslog.conf(5), klogd(8), logger(1), syslog(2), syslog(3), services(5), savelog(8)*, Version 1.3, 12 October 1998

W3 consortium, *Página de manual de bind*, http://www.w3c.org/, 1998

Thomás Aeby, Jörg Fritsch, *Introducing: Network Monitoring with BigSister: Always There*, www.linux-magazine.com, 2004

Thomás Aeby, Jörg Fritsch, *BigSister documentation*, http://bigsister.graeff.com/pdoc/README.html, 2003

Tony Byrne, tbyrne@idev.com, *Surveying the CMS marketplace* http://cmf.zope.org/Members/tseaver/dc_xml_ug/byrne_notes, 2001

Sean Michael Kerner Builder.com, *Consider these criteria to choose the right open source CMS solution*, http://web.zdnet.com.au/builder/program/web/story/0,2000034810,20274073,00.htm , 2003

Hartman Communicatie BV, *Todo sobre administración de contenido*, http://www.hartman-communicatie.nl/extra/tools.htm

Plain Black LLC, *10 content management tools to compare at once*, http://www.cmsmatrix.org/

Craig H. Rowland crowland@psionic.com, *HostSentry Config File*, http://www.psionic.com/, 1998

Craig H. Rowland crowland@psionic.com, *logSentry Config File*, http://www.psionic.com/, 1999

Jon Coyle jonco@sco.com, *Documentación portsentry*, http://www.psionic.com/, 1999

Paissan María Herminia, Glosario de términos informáticos, http://www.educainformatica.com.ar/recursos/edu/glosario/index.html, 2003

Nokin Jerome, *Jay's Iptables Firewall*, http://firewall-jay.sourceforge.net/, 2002

Notas

[i] El sistema pasará por un conjunto de pruebas y procedimientos de aseguramiento de calidad que están orientados a eliminar las fallas.

[ii] No tiene mucho sentido llamarle cronograma cuando se han omitido los tiempos, sin embargo dado que las actividades aquí descritas siguen un orden cronológico para su realización se mantuvo el título.

[iii] Una distribución es el conjunto de programas y kernel de Linux que han sido compilados y preparados por alguna organización o compañía para su instalación y a los que se tiene acceso, ya sea a través de una caja con discos compactos y manuales o bien bajándola de Internet como imágenes para grabar discos compactos o como archivos independientes.

[iv] Estamos haciendo referencia a rpm, tanto como herramienta como formato de paquetes. Entiéndase por paquete al conjunto de archivos, tanto binarios como no binarios, específicos, de una plataforma o no, que han sido preparados y agrupados bajo un formato específico. Ejemplos de formatos de paquetes tenemos .rpm, .deb, .tgz, pkg. Ejemplo de paquete tenemos kernel-2.4.22.i686.rpm

[v] Ninguno de los productos de Zend viene con la distribución, sin embargo, los productos sí existen en versiones para RedHat Linux.

[vi] Kickstart es la herramienta de instalación automática de RedHat Linux.

[vii] A lo largo de este trabajo se considera como código no sólo aquel específico de la aplicación, programado en PHP, sino también archivos de configuración y archivos de ejecución por lotes (shell scripts).

[viii] The CMS Matrix - cmsmatrix.org - The Content Management Comparison Tool, Web Content Management System Reports – CMSWatch, cmsInfo - CMS Resources New CMS Comparison Site - The CMS Matrix.

[ix] Entiéndase por contenido toda aquella información de carácter informativo estática, no de generación individual, en contraposición a información del tipo interactiva o estadística, por ejemplo.
[x] A los sistemas de administración de contenido también se les conoce como CMS por ser las siglas de su nombre en inglés – content management system.
[xi] En nuestro caso la traducción y adecuación para el español de México la realizó el mismo autor de esta tesis.
[xii] Donde diseño es el nombre del estilo que se seleccionó para el sitio o sección.
[xiii] El patrón MVC o Model-View-Controller, es una recomendación para la construcción de aplicaciones que establece como una buena práctica el mantener por separado en el código la presentación de la información (view), el procesamiento (controller) y el acceso a los datos (model).
[xiv] Cabe destacar aquí que, si bien en los sistemas de backend bancario del Banco se cuenta con un catálogo de los bancos del sistema mexicano, mismo que actualiza Banco de México un principio de construcción para todo el sistema, no sólo para la parte de contenido, fue el de no intercambiar datos con el sistema bancario, sólo realizar transacciones. Por ello nosotros necesitamos un catálogo al que se le dará mantenimiento manualmente.
[xv] Para más información ver http://www.phppatterns.com/index.php/article/articleview/31/1/1/
[xvi] eZ Publish Desktop Edition también fue traducido por el autor de esta tesis, sin embargo, por una razón circunstancial, se presenta aquí en inglés.
[xvii] Una parte importante son las practicas seguras en la administración de sistemas operativos, tales como los servicios activos, los usuarios que están dados de alta en el equipo, la selección de claves de difícil adivinación, el cambio frecuente de claves, la no desatención de sesiones activas, el respeto a la normatividad de seguridad marcada por el banco.
[xviii] Su forma de operación se describe en el capítulo 4.

[xix] Es posible hablar de secuestro de la sesión sólo en un caso muy especial, que sería el de que el atacante lograra acceso a la máquina donde está la sesión autenticada, robando las credenciales del usuario y utilizándolas para hacerse pasar por él. Hay que resaltar que si bien la información viaja cifrada entre el servidor y el cliente no la almacenan así los navegadores en el equipo del cliente.

[xx] Tales como una longitud mínima de x, un número mínimo de caracteres en minúsculas, un número mínimo de caracteres en mayúsculas y un número mínimo de números. Por ejemplo.- las claves deben tener cuando menos una longitud de 10 caracteres, 4 minúsculas, 4 mayúsculas y 2 números.

[xxi] Entiéndase aquí por firma al conjunto de actividades que realiza un usuario en una sesión.

[xxii] Se han dejado los nombres en inglés de los módulos puesto que ese es su nombre a nivel de código y configuración.

[xxiii] Cabe señalar que el sistema dado que está enfocado a proteger servidores que corren un sistema operativo tipo Unix, tiene ciertos elementos que son netamente aplicables sólo en sistemas operativos tipo Unix.

[xxiv] Estamos hablando aquí de un cálculo matemático tipo hash aplicado al contenido de un archivo y que nos devuelve un valor contra el que podremos después comparar.

[xxv] No se han traducido los nombres de las vulnerabilidades por considerarse que son nombres propios de las mismas.

[xxvi] Es posible hablar de secuestro de la sesión sólo en un caso muy especial, que sería el de que el atacante lograra acceso a la máquina donde está la sesión autenticada, robando las credenciales del usuario y utilizándolas para hacerse pasar por él. Hay que resaltar que, si bien la información viaja cifrada entre el servidor y el cliente, no la almacenan así los navegadores en el equipo del cliente.

[xxvii] Tales como una longitud mínima de x, un número mínimo de caracteres en minúsculas, un número mínimo de caracteres en mayúsculas y un número mínimo de números. Por ejemplo.- las claves deben tener cuando menos una longitud de 10 caracteres, 4 minúsculas, 4 mayúsculas y 2 números.

[xxviii] Se habla aquí de dos servidores pensando en dos roles, el rol de servidor de información y el rol de servidor aplicativo o transaccional.
[xxix] Se habla aquí de configuración en el sentido de la distribución de servidores y servicios versus equipo.
[xxx] El sistema pasará por un conjunto de pruebas y procedimientos de aseguramiento de calidad que están orientados a eliminar las fallas.
[xxxi] Denial of service, o denegación del servicio. Ni implican un sistema comprometido ni una intrusión. Se reflejan como una falta de respuesta o una respuesta muy lenta.
[xxxii] iBest es un concurso de sitio de Internet que cuenta con la participación de dos grupos, el primero un panel de expertos elegidos por el sitio que realiza el concurso, el segundo los usuarios de Internet que emiten su voto por un candidato, para convertirlo en ganador.