UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

ARQUITECTURA INTEGRAL DE SISTEMAS SEGUROS EN INTERNET

Tesis para optar el título profesional de

INGENIERO DE SISTEMAS

Harold Valentín Campos Urquiza

Lima-Perú

2003

INDICE

SUMARIO EJECUTIVO

Seguridad en Internet es un término muy amplio dentro de las Tecnologías de Información. Es así que el desarrollo de este proyecto se ha realizado dentro de un amplio contexto que no ha sido restringido a ciertos tipos de aplicaciones, si no también a los procesos que se llevan a cabo dentro de una organización. Es de vital importancia reconocer cada uno de los factores que hacen necesario un esquema de seguridad como el planteado en este trabajo. Algunos puntos, se pueden mencionar a continuación:

- El Crecimiento exponencial del mercado potencial de Internet. Como muestra de este crecimiento se está desarrollando una nueva versión del protocolo para redes IP (versión 4 actualmente) que contempla un mayor soporte de direcciones IP y un mejor formato de comunicaciones en redes.
- El Crecimiento real de negocios en Internet. En nuestra realidad nacional los negocios en Internet van creciendo de dos formas: Los Negocios entre compañías para brindar un servicio o satisfacer una necesidad y los negocios hacia el consumidor.
- El ofrecimiento de una imagen de seguridad al Cliente de una compañía ante eventos indeseables tales como ataques a sus sistemas y la posible pérdida de recursos de las compañías o de sus clientes. La protección

interna de la compañía a eventos que puedan alterar la consecución de sus procesos y el correcto desempeño de sus trabajadores.

- La Pérdida de información crítica del negocio o de los servicios claves de este.

Es por ello y ante todas las vulnerabilidades que se encuentran expuestos los Sistemas de información que se propone el desarrollo de una Arquitectura Integral de Sistemas Seguros en Internet, basada en experiencias pasadas, mejores prácticas de software y estudios que se fundamentan a lo largo del proyecto de tesis.

DESCRIPTORES TEMATICOS

Los siguientes son los Descriptores Temáticos considerados en el desarrollo del Presente Trabajo de Tesis:

- COMERCIO
- INTERNET
- WWW
- REDES
- ARQUITECTURA
- SEGURIDAD
- INTEGRACION
- INFRAESTRUCTURA
- ATAQUES

INTRODUCCION

Construir redes y aplicaciones seguras no es fácil. Este requiere un excelente entendimiento de Tecnologías de Información y un claro entendimiento de los negocios y sus objetivos, combinados con un conocimiento de amenazas y las herramientas para lidiar con dichas amenazas.

La Proliferación de redes y nuevos modelos de negocios basados en el Uso de Internet ha movido claramente mucho más rápido nuestro entendimiento de las amenazas de Internet y nuestra habilidad para manejarlas.

Por más de siete décadas el uso de la criptografía (La ciencia de la codificación y el cifrado) para proteger información fue asociado primariamente con la milicia y los negocios diplomáticos. Nuestra historia militar está llena de ejemplos excepcionales de cómo la criptografía ha jugado un papel mayor en la victoria de batallas y guerras. En la actualidad mejorada por el advenimiento de la tecnología de llave pública, la criptografía forma la base de la protección de aplicaciones y Sistemas de redes modernos.

Sin embargo, la tecnología, no es suficiente para construir Sistemas de Negocios Seguros. Las personas pueden deshacer los Sistemas más seguros por su falla al implementar los procesos y procedimientos que acompañan el uso propio de la tecnología en el mundo real. Por ejemplo, La máquina alemana **Enigma,** fue un dispositivo de encriptación muy robusto en su concepto y diseño. Debidamente utilizada, podía conseguir que sus mensajes encriptados por el algoritmo incluido en ella sean descifrados por un ataque de Fuerza Bruta de las computadoras más poderosas en aproximadamente unos 7000 años. Sin embargo, por procedimientos incorrectos usados por la marina alemana los códigos del Enigma fueron vulnerados por computadoras electromecánicas primitivas durante los inicios de la segunda guerra mundial y dieron como resultado la caída del 85% de la flota alemana de submarinos en sólo nueve meses. Este evento memorable, fue resultado del esfuerzo extraordinario de criptoanalistas [1] que fueron capaces de explotar los problemas y equivocaciones de los usuarios del Sistema Enigma para dar con los códigos. Hoy la realidad de Sistemas refleja un comportamiento semejante al de varios años atrás, es decir refleja vulnerabilidades.

Son estas vulnerabilidades motivo principal del esfuerzo por alcanzar un entendimiento claro de las verdaderas necesidades de seguridad que poseen

---

[1] Analistas de Criptografía. Expertos en criptografía aplicada.

las empresas. Este trabajo se enfoca en el análisis de estas necesidades y la propuesta de una Arquitectura Óptima de Seguridad destinada a prevenir situaciones, corregir caminos errados para de esta manera incrementar el margen de ganancias de las compañías, asegurando la integridad sus recursos, manteniendo la visión de que las organizaciones deben tener como misión crítica realizar sus negocios adecuadamente, sin cerrarse como fortalezas impenetrables.

CAPITULO I

HIPOTESIS DEL PROYECTO

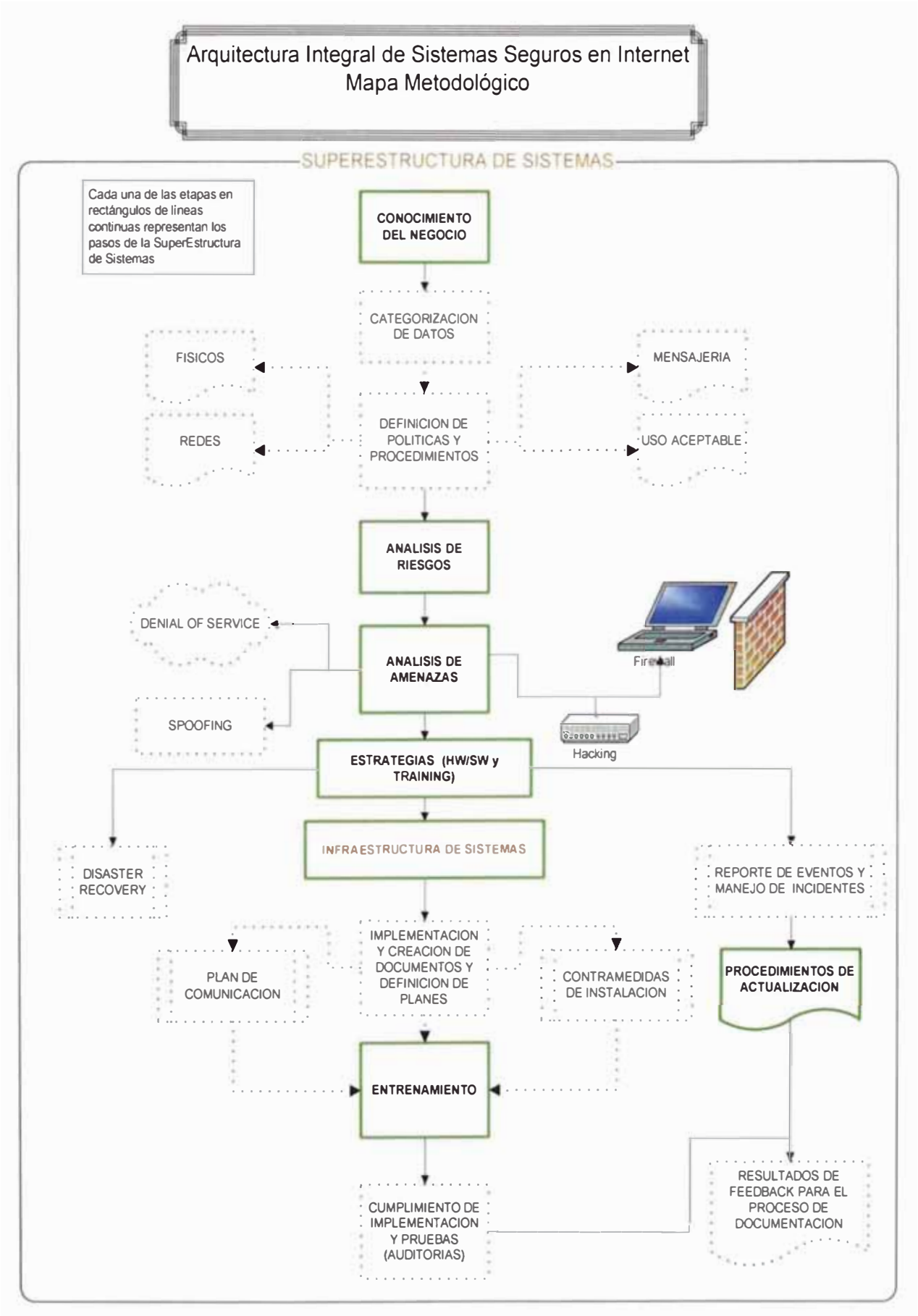
La Hipótesis sobre la cual se formula el presente trabajo es la siguiente:

Las organizaciones que poseen Sistemas que utilizan a Internet como medio de negocios, están expuestas a amenazas tecnológicas y sociales, como parte del funcionamiento diario de sus procesos de negocio. Las amenazas tecnológicas pueden ser evitadas mediante la implementación de la metodología tecnológica propuesta basada en la ejecución sistemática de reglas de protección tecnológica y la implementación de Sistemas de información; mientras que las amenazas sociales pueden ser mitigadas mediante la implementación de la metodología social basada en el análisis interno del negocio y sus factores exógenos. El resultado de esta combinación de metodologías genera como entregable final una Arquitectura Integral de Sistemas Seguros en Internet.

Se espera que las investigaciones, análisis, planteamientos y conclusiones del proyecto, brinden una guía eficiente y adecuada a sus necesidades y presupuestos, de como proteger sus Sistemas de Información en Internet mediante la implementación de la metodología social sistémica (llamada en adelante “Superestructura”), una Arquitectura Tecnológica Flexible (“Infraestructura") y finalmente regla sistemáticas de protección de Sistemas.

EL proyecto se ha organizado de acuerdo al siguiente esquema:

Arquitectura Integral de Sistemas Seguros en Internet
Mapa Metodológico



Este esquema permite apreciar las fases de la Arquitectura propuesta y que ha sido planteada en el capítulo III.

CAPITULO II

MARCO REFERENCIAL DEL PROYECTO

MARCO CONCEPTUAL

Los Negocios Electrónicos no son un concepto nuevo. Compañías y consumidores han estado usando por años medios electrónicos para conducir sus transacciones comerciales. A la fecha, los negocios electrónicos han sido inhibidos por los altos costos y la complejidad. La complejidad se origina en el establecimiento de líneas de comunicación e incluso más por la carencia de aplicaciones estándares y seguras para ver y compartir información una vez conectados. Internet, específicamente la World Wide Web, ha cambiado este escenario radicalmente. Ahora la conectividad sobre Internet es menos costosa y está caminando sobre un gran proceso de estandarización que está facilitando la comunicación directa con cualquier organización.

El Comercio en Internet representa un Mercado que vale potencialmente cientos de millones de dólares habiéndose iniciado en sólo unos cuantos años.

Este mercado presenta fascinantes oportunidades de negocios. Primero, Un creciente medio estándar de negocios para automatizar y perfilar cómo se negocia con otros negocios: **Comercio business-to-business (B2B) o de Negocio a Negocio**. El Comercio Business-to-business incluye comercio en línea, donde se venden bienes y servicios a otros negocios sobre la Web. En las compras corporativas basadas en Internet, los negocios se combinan en un Sistema donde empleados hacen compras de materiales de oficina y suministros utilizando una Intranet Corporativa. Con negocios de cadena de suministros sobre Internet, los negocios trabajan cercanamente juntos vía la Internet para automatizar y perfilar la provisión de bienes de producción y su distribución.

El Comercio en Internet también provee un creciente canal dinámico para la entrega eficiente de bienes y servicios a los consumidores: **Comercio business-to-consumer (B2C) o de Negocio a Consumidor**. En el Comercio business-to-consumer, las compañías mercadean bienes físicos a consumidores en línea en un entorno personalizado y dinámico. El Comercio Business-to-consumer incluirá progresivamente intuirá la entrega digital de bienes—software, medios electrónicos, e información. Los Consumidores

buscarán con mayor frecuencia en Internet para realizar la entrega de servicios, incluyendo ticketing, reservaciones, y servicios financieros.

Existen otros tipos de soluciones de negocios que involucran a Internet como medio de transmisión de información y que serán discutidos en detalle secciones en secciones posteriores.

En resúmen, El Comercio electrónico—business-to-business (B2B) y business-to-consumer (B2C) — impactarán dramáticamente la forma de cómo los bienes y servicios son administrados, comprados, y vendidos del productor al consumidor.

MARCO TEORICO

AMENAZAS TECNOLOGICAS

Los Sistemas que utilizan a Internet como medios de transmisión de información están expuestos a una serie de amenazas que cada vez son más complejas. Básicamente, estas amenazas están representadas tecnológicamente por dos tipos de agentes: Los Hackers y los Crackers.

AMENAZAS DE HACKERS

Los Hackers son agentes que por lo general tienen un amplio domino de lenguajes de programación, y un firme conocimiento del Protocolo TCP/IP (Protocolo estándar en Internet). Aunque no es el único protocolo, es el mas conocido en Internet.

Un Hacker busca hoyos internos y externos de los Sistemas, errores nativos y configuraciones inadecuadas de Sistemas. En algunos círculos de Hackers va contra su ética alterar datos de los registros que son necesarios para limpiar el seguimiento de sus ataques.

DENIAL OF SERVICE (DOS ATTACKS) O ATAQUES DE BLOQUEO DE SERVICIOS

Este tipo de ataque es indirecto a la organización. Los Hackers no tratan de ingresar los Sistemas por si mismos, pero si tratan de mantener a cualquier otra persona ingresando al mismo. Uno de los más famosos ataques fue el "IP PING TO DEATH" (Ping IP de la muerte), documentado en Enero de 1998. El Ping de la muerte se basa en los defectos de la Implementación del TCP/IP. El Ping de la muerte no amenaza la seguridad de los Sistemas que ataca, pero algunas veces puede liderar ataques más directos en cuentas o en información almacenada en un Sistema. Algunos software de Firewalls, por ejemplo, pueden ser engañados permitiendo la sobrecarga de tráfico inautorizado sobre legítimos puertos TCP/IP.

Se han visto numerosos artículos sobre los ataques en los grandes Sitios Web como Yahoo e eBay. Estos ataques premeditados muestran las varias debilidades en el armamento que rodea varios de los Sitios Web líderes en el Internet de hoy en día. Hemos visto Hackers bajando enormes Sitios Web corporativos como David lo hizo a Goliat. Pues estos ataques DoS (Denial of Service) no son ciertamente un fenómeno nuevo. Es fácil sobrecargar una central corporativa. Por ejemplo, realizar llamadas repetitivamente a los números telefónicos 0-800 para prevenir sobre recibir llamadas legítimas de negocios. De acuerdo a CERT: "Un ataque DoS está caracterizado por un intento explícito de Hackers de prevenir usuarios legítimos de un servicio del uso del mismo servicio".

Un ejemplo de estos ataques DoS incluyen inundar una red de con falso tráfico. Para esto se valen de herramientas simples de mantenimiento de redes para probar números IP. Esto es el Ping de la Muerte.

El Siguiente es el código fuente básico de un ataque DoS del tipo LAND:

```
// IP header.
struct iphdr {
   uchar     version : 4;      // IP version.
   uchar     ihl : 4;          // Header length.
   ushort    len;              // Packet length.
   ushort    id;               // Packet ID.
   ushort    frag_offset;      // Fragment offset.
   uchar     ttl;              // Time to Live.
   uchar     protocol;         // Protocol (TCP, UDP, ICMP, etc.).
   ushort    checksum;         // Checksum.
   ulong     saddr;            // Source address.
```

```
    ulong      daddr;          // Destination address.
};

// TCP header.
struct tcphdr {
    ushort     source_port;      // Source port.
    ushort     dest_port;        // Destination port.
    ulong      seq;              // Sequence number.
    ulong      ack;              // Acknowledgment sequence number.
    uchar      unused1 : 4;
    uchar      offset : 4;       // Data offset.
    uchar      flags;            // Flags (SYN, ACK, etc.).
    ushort     window;           // Window.
    ushort     checksum;         // Checksum.
    ushort     urgent_ptr;       // Urgent.
};

// TCP flags.
enum {TH_FIN = 0x1,  TH_SYN = 0x2,  TH_RST = 0x4,
    TH_PUSH = 0x8, TH_ACK = 0x10, TH_URG = 0x20};

// Get the address of the target host (172.91.11.2).
struct sock_addr sin;
ZeroMemory(&sin, sizeof(sin));
sin.sin_family = AF_INET;
struct hostent *host = gethostbyname("172.91.11.2");
CopyMemory(&sin.sin_addr, host->h_addr, host->h_length);

// Get the port (80).
sin.sin_port = htons(80);

// Build the IP header.
// Note that the source and destination addresses are the same;
// this is the essence of the LAND attack.
struct iphdr ip;
ZeroMemory(&ip, sizeof(ip));
ip.version = 4;
ip.ihl = sizeof(strust iphdr) / 4;
// LAND attack has no body; it's just a bogus header,
// hence the length is just the size of IP and TCP headers.
ip.len = htons(sizeof(struct iphdr) + sizeof (struct tcphdr));
ip.id = htons(0xF1C);
ip.ttl = 255;
ip.protocol = IP_TCP;
ip.saddr = sin.sin_addr.s_addr; // Source address is "spoofed."
ip.daddr = sin.sin_addr.s_addr;
// Build up the TCP header.
```

```
// Note that the source and destination ports are the same;
// this is the essence of the LAND attack.
struct tcphdr tcp;
ZeroMemory(&tcp, sizeof(tcp));
tcp.source_port = sin.sin_port;
tcp.dest_port = sin.sin_port;
tcp.seq = htonl(0xF1C);
tcp.offset = sizeof(struct tcphdr) / 4;
tcp.flags = TH_SYN; // The first part of the handshake _ SYN.
tcp.window = htons(2048);
tcp.checksum = checksum(); // Checksum is calculated.

int sock = socket(AF_INET, SOCK_RAW, 255);
sendto(sock, ...);
closesocket(sock);
```

DISTRIBUTED DENIAL OF SERVICE O ATAQUE DISTRIBUIDO DE BLOQUEO DE SERVICIOS

Los Hackers lanzan sus ataques de varias computadoras que trabajan juntas y simultáneamente, haciendo difícil su ubicación y detención. Hasta los ataques DDoS de febrero del 2000, se asumía que los computadores de los atacantes que residían en largos “Túneles” (Conexiones con un ancho de banda increíble), podrían no verse seriamente afectados por ataques de saturación de redes. Como los grandes ISP encontrados, este no es el caso. Utilizando varias conexiones de redes pequeñas, un individuo puede inundar el ISP más grande y consumir todo su ancho de banda.

SMURFING (VARIANTE DE DOS)

Este tipo de ataque no tiene nada que ver con las criaturas de los dibujos animados (“Los Pitufos: The Smurfs”). Este es un tipo específico de ataque DoS donde los Hackers inundan una computadora con pequeños pedidos de cortas respuestas. En un Ataque como este, el individuo falsifica un paquete (Una unidad de datos que es ruteada entre un origen y un destino sobre Internet) de la dirección IP de la víctima a la dirección de red de un intermediario. Si el intermediario no ofrece resistencia, el recibirá el paquete, y será generado un paquete de respuesta y enviado a la víctima, inundando su red. La red del intermediario es también inundada. Esto es hecho a miles de intermediarios en menos de un segundo. Una manera de de frustrar el smurfing es inhabilitar el direccionamiento broadcast IP en cada ruteador de red, ya que son raramente usados.

Por ejemplo la siguiente porción de código en lenguaje de programación Perl realiza un ping a una subnet entera con un paquete de transmisión ICMP:

```
@ip = (157,59,133,100);    ' Ingresando un número IP
@mask = (255,255,252,0); ' Ingresando una sub-máscara de red.

$subnet =  (($ip[0] | ~$mask[0]) & 0xFF) . '.' .
           (($ip[1] | ~$mask[1]) & 0xFF) . '.' .
           (($ip[2] | ~$mask[2]) & 0xFF) . '.' .
```

```
            (($ip[3] | ~$mask[3]) & 0xFF);


`ping $subnet >&2`; # backticks (`) alrededor del llamado al ping.
```

TRINOO O ATAQUE DE LOS TROYANOS

Esta es una herramienta utilizada para lanzar ataques DoS coordinados de una variedad de orígenes. Un programa caballo de Troya (Uno con código dañino o malicioso e programación aparentemente inofensiva); Trinoo apareció por primera vez en febrero del 2000. El Caballo de Troya Trinoo es instalado cuando el usuario sin conocimiento lo ejecuta. Este copia un archivo ejecutable en el directorio de Sistema Operativo Windows\System. Una vez ejecutado por el usuario, este instalará de forma que estará activo permanentemente. Mientras el usuario está conectado a Internet, si el programa está corriendo, cualquiera que esté corriendo el programa cliente Trinoo puede ingresar a la computadora del usuario sin permiso y sin su conocimiento. Esto causa un serio riesgo de seguridad al usuario afectado.

FOOTPRINTING O TANTEO

Este es un proceso donde el Hacker obtiene información sobre el entorno de cómputo. Los Hackers tienen varios orígenes públicos a su disposición: Nombres en Internet y orígenes de registros, orígenes de negocios e

información privada. Una vez que los Hackers obtienen esta información, ellos pueden iniciar sus ataques. Esta información incluye usualmente direcciones IP, nombres de dominio nombres de servidores SMTP y más. Footprinting es como el ladrón que primero “Revisa el entorno” que esta contemplando romper.

```
void EnumUsers(LPWSTR wszServer) {
    const DWORD dwLevel = 1;
    const DWORD MAX ENTRIES - 100;
    DWORD dwIndex = 0;
    DWORD dwEntryCount;

    wprintf(L"EnumUsers on %s\n\n",wszServer);

    NET_API STATUS err = ERROR_MORE_DATA;
    while (err == ERROR MORE DATA) {
        char *pUsers;
        err = NetQueryDisplayInformation(
                    wszServer,
                    dwLevel,
                    dwIndex,
                    MAX ENTRIES,
                    MAX ENTRIES * 2,
                    &dwEntryCount,
```

```
                (LPVOID *)&pUsers);

if (err != NERR_Success && err != ERROR_MORE_DATA)
    Error(err); // Error function is elsewhere.

for (DWORD i=0; i < dwEntryCount; i++) {
    NET_DISPLAY_USER *pStart =
       (NET_DISPLAY_USER*)pUsers;
    NET_DISPLAY_USER pUser = pStart[i];

    wprintf(L"Name : %s\n", pUser.usri1_name);

    if (lstrlen(pUser.usri1_full_name))
        wprintf(L" %s\n", pUser.usri1_full_name);
    if (lstrlen(pUser.usri1_comment))
        wprintf(L" %s\n", pUser.usri1_comment);
    wprintf(L" RID: %d\n", pUser.usri1_user_id);

    if (pUser.usri1_flags & UF_ACCOUNTDISABLE)
        wprintf(L" Account is disabled\n");
    if (pUser.usri1_flags & UF_LOCKOUT)
        wprintf(L" Account is locked out\n");

    wprintf(L"\n");
```

```
            dwIndex = pUser.usri1_next_index;
        }

        NetApiBufferFree(pUsers);
    }
}
```

Cuya salida:

```
EnumUsers on exair

Name : Administrator
 Built-in account for administering the computer/domain
 RID: 500

Name : Guest
 Built-in account for guest access to the computer/domain
 RID: 501
 Account is disabled

Name : exair
 Dummy account for development
 RID: 1037
```

```
Name : test
```

RID: 1035

NETWORK SCANNERS O HERRAMIENTAS DE SCAN DE REDES

Hay cientos, si no miles de herramientas que pueden ser usadas para realizar un “scan” de un Sistema o página Web. Estas herramientas pueden ser descargadas de Internet por cualquiera y usadas con poca o sin modificación. Ellas buscarán una red o un Sistema Operativo, buscando vulnerabilidades y reportándolas a los Hackers. El Hacker puede aprovechar de esas “Puertas Abiertas”. Muchos Scanners de Internet específicamente buscan por archivos e impresoras compartidas sobre las que puedan tener acceso protegidas o no por passwords. Los malos tipos dejan corriendo estos scanners durante noches y días, recolectando direcciones IP, para luego mapear las unidades compartidas a sus discos duros para ganar acceso total a los archivos de otras computadoras. Los Tipos malos específicamente usan herramientas que les permitan scanear sigilosamente. NMap es una herramienta que sirve para olfatear hoyos y servicios de red que están maduros para ser atacados. Otras conocidas son: Sam Spade, Port Scanner, Internet Maniac y SATAN (Security Administrator's for Analyzing Networks).

Por ejemplo el siguiente código muestra un recorrido ficticio de una trama de datos desde Seattle, Washington, a Zambia en África Central:

```
D:\>tracert mang.bnet.zm

Tracing route to mang.bnet.zm [196.7.240.10] over a maximum of 30 hops:

 1   180 ms   190 ms   191 ms  sdn-ar-003waseat004t.dial.net [178.191.230.2]
 2   161 ms   180 ms   180 ms  sdn-hr-003waseat004t.dial.net [178.191.230.1]
 3   220 ms   160 ms   171 ms  sdn-pnc2-sea-5-1-T1.dial.net [217.143.225.105]
 4   331 ms   190 ms   200 ms  sl-bb3-sea-1-0.link.net [217.143.223.173]
 5   160 ms   190 ms   191 ms  sl-bb51-sea-0-2.link.net [154.232.5.36]
 6   161 ms   180 ms   160 ms  sl-bb3-sea-4-0-0.ink.net [154.232.5.21]
 7   170 ms   200 ms   200 ms  Hssi5-2-0.BR1.FOO1.ALTER.NET [147.39.243.50]
 8   210 ms   201 ms   190 ms  105.ATM3-0.XR2.FOO1.ALTER.NET [156.188.199.72]
 9   161 ms   190 ms   200 ms  294.ATM4-0.TR2.FOO1.ALTER.NET [156.188.199.123]
10   230 ms   251 ms   260 ms  110.ATM5-0.TR2.FOZ1.ALTER.NET [156.188.136.75]
11   270 ms   290 ms   311 ms  198.ATM6-0.XR2.FOZ1.ALTER.NET [156.188.242.111]
12   271 ms   300 ms   290 ms  194.ATM8-0-0.GW1.FOZ1.ALTER.NET [156.188.242.145]
13   861 ms   871 ms   892 ms  bnet-gw.customer.ALTER.NET [167.130.64.82]
14  1012 ms   941 ms   931 ms  mang.bnet.zm [186.7.240.110]
```

ATAQUES DE SISTEMA OPERATIVO

Los Ataques de SO explotan errores en un específico Sistema Operativo por ejemplo: Windows 98 o MacOS. Las herramientas son realmente fáciles de hallar: Solo basta revisar o comprar una página de seguridad de un vendedor de seguridad en la Web y uno puede aprender como conducir dichos ataques. En general, cuando esos problemas son identificados, ellos son arreglados por el vendedor de software rápidamente. Entonces como un primer paso, siempre debemos estar seguros de tener la última versión de nuestro Sistema Operativo, incluyendo todas las correcciones de cada error. Estos ataques son conocidos también como Windows Nuke o Windows OOB bug.

Ataque	Comentarios
"::$DATA" bug	Permite al atacante ver el código fuente de páginas ASP.
"." bug	Igual que el superior, pero el archive a se accedido tenía un " " al final.
".htr" buffer overflow	Un pedido especial formateado a un archivo .htr que ejecuta código arbitrario en el contexto de seguridad del Servidor Web.
Vulnerabilidad RDS	Un pedido especial formateado de Remote Data Services que ejecuta código arbitrario en el contexto de seguridad del Servidor Web.
Ejemplos	Algunos ejemplos contienen código para ver código fuente. Nunca instalar dichos ejemplos en un servidor de producción.

ACCESO REMOTO

Este es uno de los ataques más antiguos y aún es fácil utilizando las herramientas correctas. Muchas compañías no bloquean sus líneas analógicas para mantener estos ataques lejos. Hay dos herramientas básicas para conducir un ataque de acceso remoto: Un "War Dialer" y una herramienta de hacking de passwords. Este "War Dialer" es una simple Base de Datos acompañada de un script de MODEM que marca cada número telefónico en un grupo designado por el usuario. Después de conectarse satisfactoriamente con el tono de un MODEM, el "War Dialer" guardará el número telefónico en la Base de Datos. El Individuo puede entonces revisar la Base de Datos y seleccionar un objetivo para intentar hackear. La segunda herramienta es un password hacker, que usa un diccionario para crackear los passwords.

ATAQUES DE VIRUS

Estos son programas que han sido puestos en una PC o en una estación de trabajo sin autorización del usuario. Estos programas no son siempre dañinos, pero muchas veces pueden causar daño o que los Sistemas de cómputo se sobrecarguen a si mismos y detengan sus servicios. Los Virus son transmitidos a menudo por medio de correos electrónicos, archivos descargados de Internet, etc. Algunos actúan inmediatamente, mientras que otros se disparan bajo determinadas condiciones de los Sistemas.

AMENAZAS DE CRACKERS

ATAQUES DE FUERZA BRUTA

La Definición de un Cracker es una persona que intenta romper la seguridad de un Sistema vía la suposición o la resolución de un usuario o passwords de sistemas usando “la fuerza bruta”, en otras palabras esto incluye las adivinanzas. A menudo se utiliza estos términos indistintamente, el de Cracker por el de hacker. El nivel de conocimientos y educación de un Cracker y sus propios trabajos son típicamente más bajos que los de un hacker. Se considera que mientras los Hackers construyen programas, los crackers los destruyen.

AMENAZAS SOCIALES

Las amenazas de seguridad no solo vienen de fuera. Muchas amenazas vienen del interior de la organización. Estas pueden ser tan simples como el Síndrome del Usuario Estúpido o tan complejas como las represalias de un Administrador por haber sido despedido. Un empleado interno puede abusar, y puede causar tanto daño como un hacker, y estos ataques son muy reales. De acuerdo al FBI, el 70% de todas las computadoras en Internet han tenido

algún tipo de incidente inautorizado. De acuerdo al informe del CSI[2] de respuestas de quienes reconocen uso inautorizado, 43% han reportado al menos uno de los cinco incidentes fuera de la organización, 37% han reportado de uno de los cinco incidentes dentro de la organización. También se tiene elevados porcentajes por abuso de privilegios de acceso a Internet (Como descarga de pornografía, software pirata, o involucrándose en el uso inapropiado de Sistemas de correo electrónico).

La Respuesta completa de porque las personas atacan empresas probablemente nunca será conocida, sin embargo esta claro que la mayoría de ataques son realizados por personas con intenciones maliciosas; muchas de ellas son realizadas por gente que quieren un poco de desafío intelectual. Naturalmente, esto no significa que se deba bajar la guardia. Inclusive si un pequeño porcentaje de gente buscara atacar un servidor, aún es una cantidad considerable de gente.

Los siguientes tres factores generalmente están asociados a los ataques:

Motivación:

---

[2] Computer Security Institute

Las personas que realmente desean dañar, especialmente aquellas que intentan atacar el Sitio Web de una compañía, probablemente no les agrada la compañía por sus transgresiones ambientales percibidas, políticas, algo que la compañía dijo, o una de mil razones. Se debe recordar que se está tratando con humanos, que tienen emociones, y las emociones pueden conducir a comportamientos irracionales o antisociales.

Los Ataques desde el interior de una compañía son comúnmente iniciados por empleados disgustados. No se debería pasar por alto la posibilidad de ataques del interior.

La razón más importante para un ataque de revelación (en que los secretos de la compañía o documentos son accedidos) es espionaje industrial.

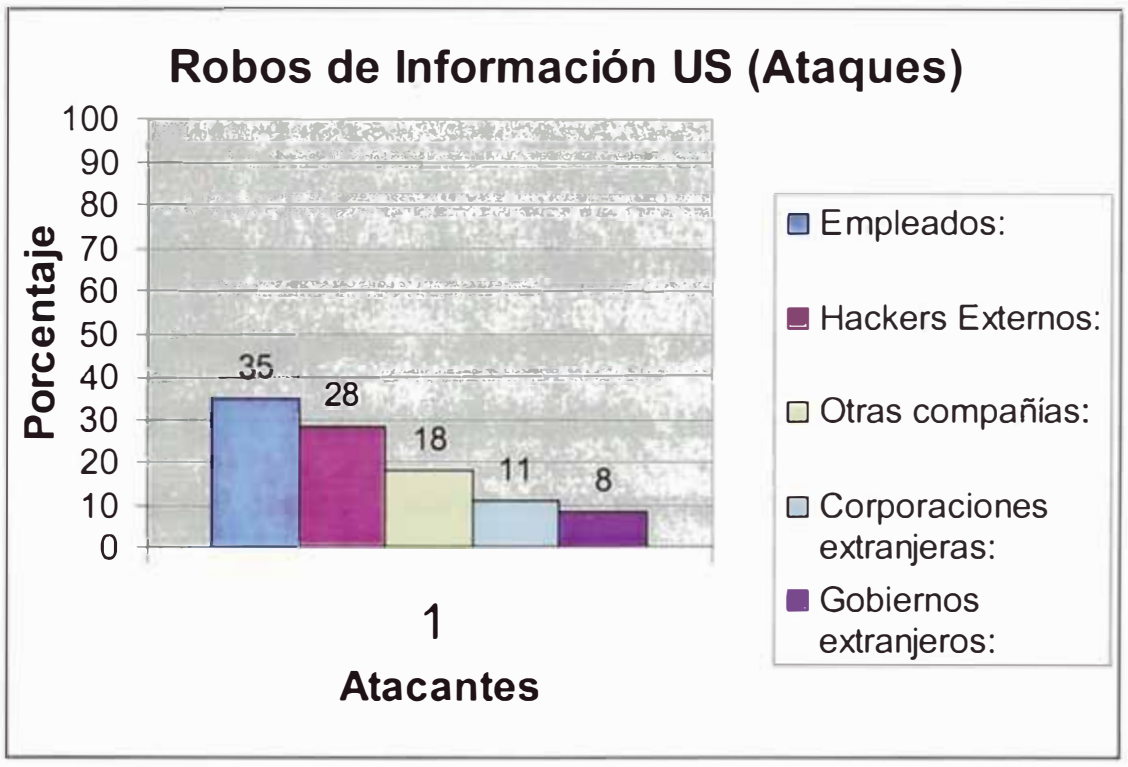
Justificación Personal:

Una persona que es motivada para montar un ataque debe justificar sus acciones. Por ejemplo, un empleado descontento (o empleado original) puede racionalizar la destrucción de un sitio Web como algo mínimo comparado a la angustia mental que significa resistir a alguna acción realizada por la compañía (como la de despedirlos).

Oportunidad:

Finalmente, el atacante debe encontrar el tiempo correcto para realizar el asalto. Desafortunadamente, par alas computadoras en la Web este puede

ser cualquier momento porque los sitios Web trabajan 24 horas de servicios. A continuación se adjunta una tabla con información de porcentajes de ataques a las empresas en EEUU, realizado por Michael G. Kessler & Associates, una firma de seguridad de New York[3].



Como se ha podido apreciar en la tabla referencial anterior, aunque la información proviene de EEUU, se consideran una buena aproximación para tomar en cuanta una necesidad urgente en la organización, como se menciona en las cifras del CSI líneas atrás, y este muestra que el mayor

[3] Para mayor información:
http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html.

porcentaje de incidentes de ataques provino del interior de la organización. Es por ello, que parte de la metodología que debe abordar una arquitectura integral de sistemas seguros, involucra no sólo variables tecnológicas, sino también sociales.

SITUACION TENOLOGICA ACTUAL

REDES CORPORATIVAS SEGUN TOPOLOGIA

Actualmente las organizaciones protegen más sus límites convirtiéndolas en fortalezas inexpugnables y negando la posibilidad de explotar nuevas oportunidades de negocios con asociados, tales como proveedores, agentes y compradores, que asegurar en si sus procesos internos.

Para realizar la definición adecuada del tipo de infraestructura física se recurre al apoyo de un Documento de Despliegue de Infraestructura (DDI). Este documento resume las necesidades físicas de una Arquitectura de Hardware de acuerdo a las características del negocio y las aplicaciones que se desean implementar en una compañía. No constituye exclusivamente un documento de estrategias de seguridad, por lo que las empresas muchas veces desarrollan su arquitectura y su seguridad en proyectos separados (Algo muy negativo), pero la recomendación es que en la elaboración del DDI se considere la seguridad del negocio como un factor fundamental.

Referencialmente se mostrarán algunas de las arquitecturas de Sistemas sugeridas más comunes de acuerdo al tipo de solución vertical que implementan en sus empresas. Se han omitido las configuraciones de seguridad para mostrar el esquema complementario a continuación:

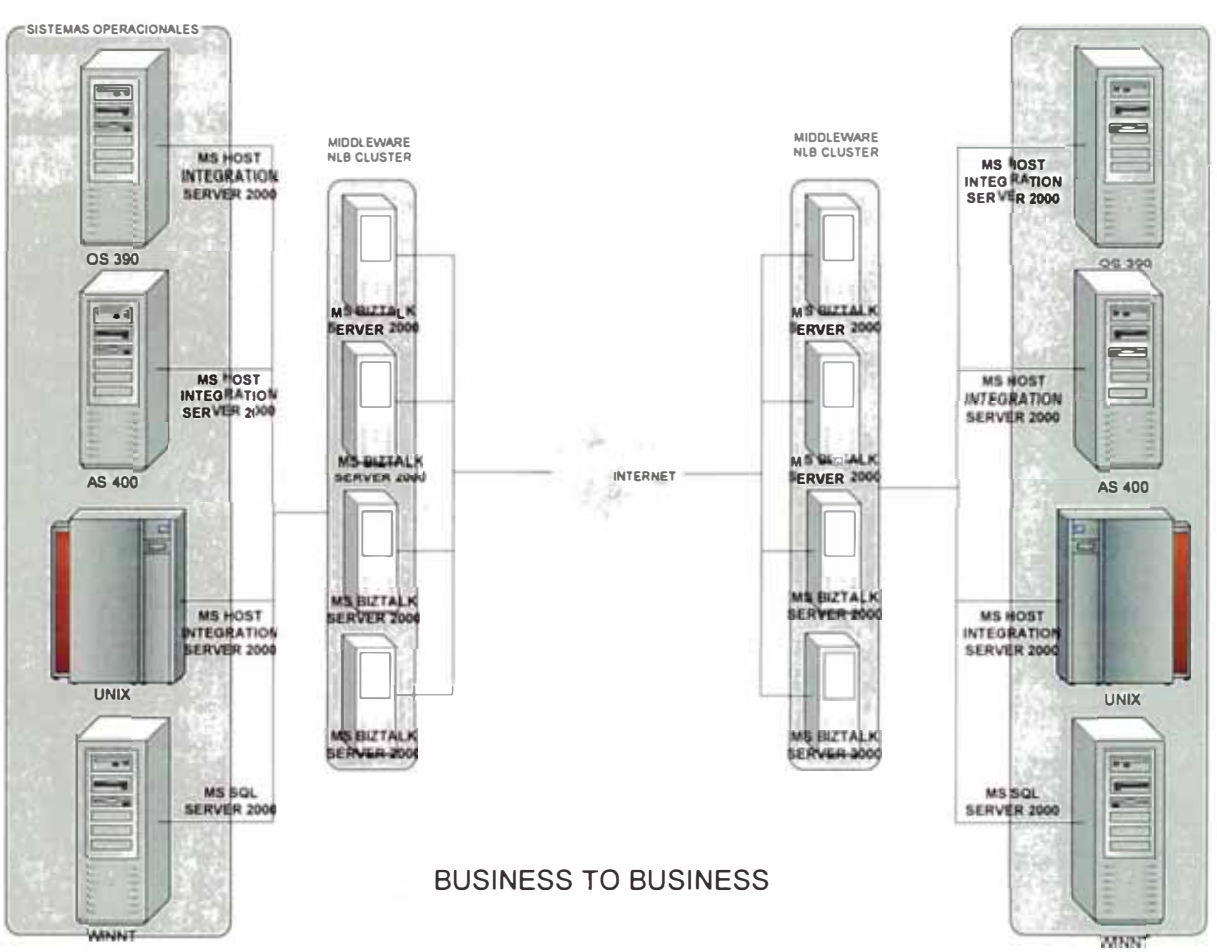
- **Solución de Negocio a Negocio (B2B o Business to Business):**

El área de soluciones de Comercio Electrónico entre Negocios es la que más beneficios ha generado en términos económicos pues las empresas han encontrado una forma más económica para realizar transacciones comerciales. Por otro lado han surgido nuevas empresas y nuevos modelos de negocio en Internet dedicados a facilitar los negocios en línea con las soluciones de Marketplaces[4] en diversas modalidades.

En lo que respecta al mercado peruano este tipo de soluciones son las que prevalecerán con fuerza respecto a las soluciones al consumidor pues tanto por los montos como por el retorno a la inversión las empresas son más atractivas para estas últimas.

---

[4] Marketplace, Sitio donde concurren compradores y vendedores en Internet.

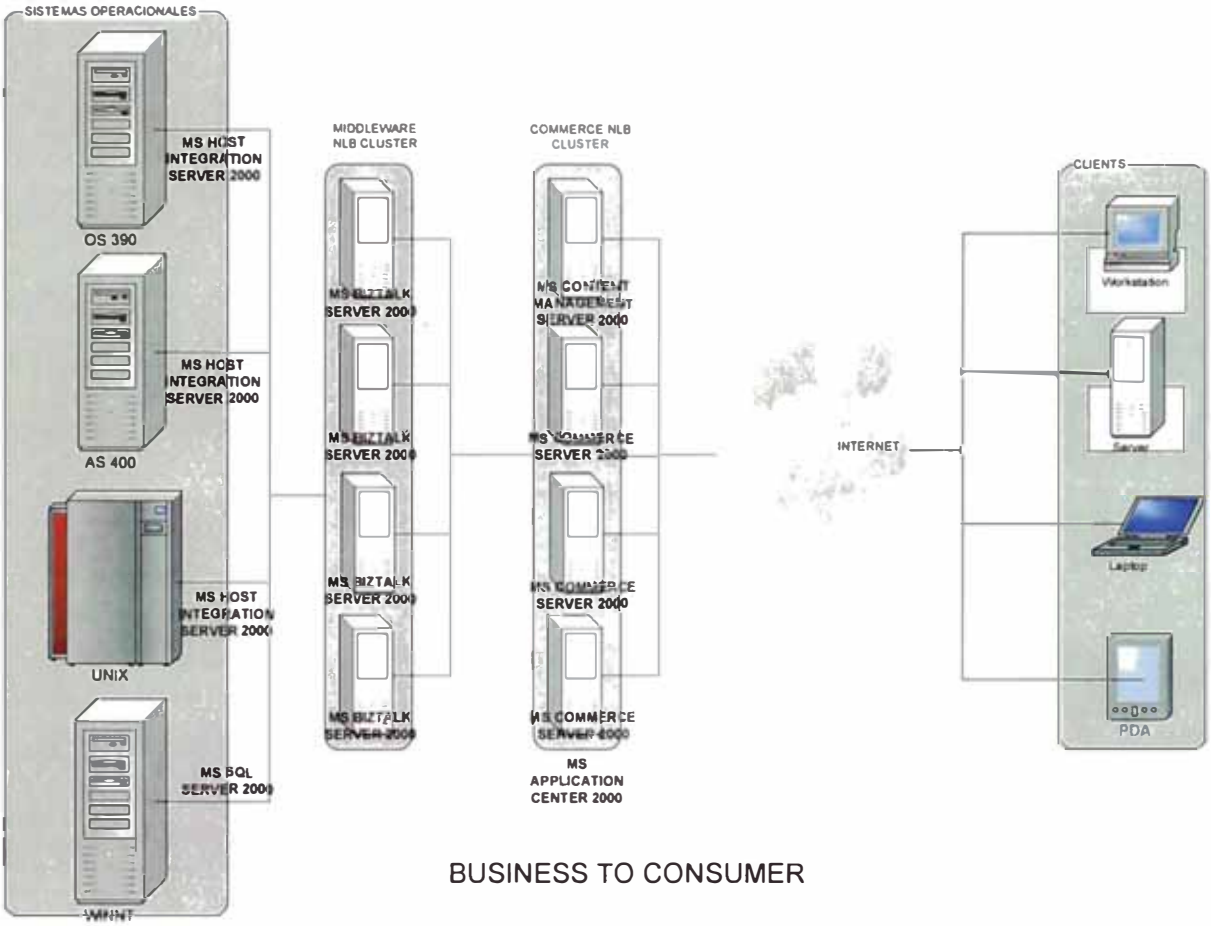


- **Solución de Negocio para el Consumidor (B2C o Business to Consumer):**

El Área de Comercio al Consumidor es reciente para el medio peruano y factores propios relacionados a la infraestructura y realidad económica del país han impedido un desarrollo más rápido de este tipo de soluciones. De todas formas las empresas vienen implementando soluciones de comercio para clientes y muchas veces internas para empleados corporativos.

Un aspecto clave en las soluciones de comercio es la capacidad de integración con los sistemas back end pues normalmente las empresas ya

establecidas cuentan unos sistemas de operación en dónde se encuentran la información relacionada a clientes, productos, etc.

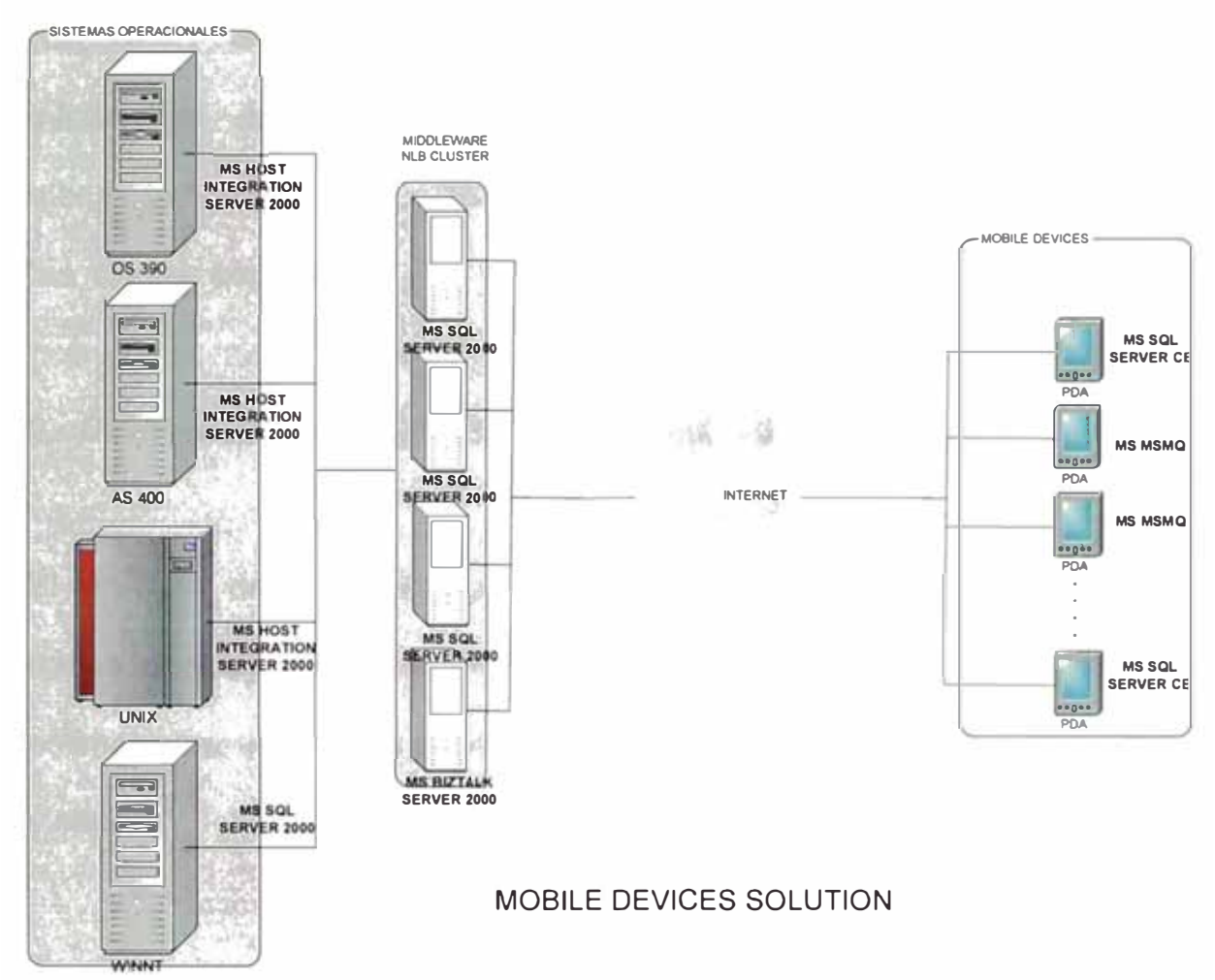


BUSINESS TO CONSUMER

- **Solución de Dispositivos Móviles:**

Las Soluciones para dispositivos móviles (agendas electrónicas, computadoras de bolsillo y eventualmente teléfonos inteligentes) es un área de crecimiento en la industria de TI debido al gran retorno a la inversión de un proyecto de este tipo. Esto se debe a la gran productividad que se gana al automatizar los procesos o trabajos de campo. La productividad se gana reduciendo los tiempos de proceso, reduciendo el número de transportes a localidades centrales, reduciendo los errores por entradas manuales y

disponiendo de información de mejor calidad y oportunidad al estar en el campo.



MOBILE DEVICES SOLUTION

MARCO METODOLOGICO

La Metodología empleada en el desarrollo del proyecto ha sido la metodología experimental. Cada uno de los pasos de la afirmación a demostrar han sido experimentados en proyectos como el adjunto en la parte final del documento. Los pasos a seguir para el desarrollo del tema de investigación, su evaluación e implementación han sido los siguientes:

1. Captura de Información

El Proceso de captura de información se realizó a todo nivel. Desde el nivel corporativo hasta el nivel de la pequeña y mediana empresa. Se capturó información de transacciones financieras, comerciales, notificaciones y alertas generadas entre sistemas con acceso de cara a Internet y dentro de las mismas empresas.

2. Determinación de espacios de casos dentro de un universo

El proceso de determinación de espacios se realizó por volumen de transacciones y por sector vertical. Se crearon grupos uniformes para lograr estimaciones adecuadas y que se ajusten al proceso de evolución tecnológica y social.

3. Evaluación Teórica de los casos agrupados

El Proceso de evaluación técnica se dividió por sector tecnológico. Es decir se evaluaron los tipos de ataques, frecuencia de ataques, compañías de software, compañías de hardware, y estadísticas de cada parte.

4. Discusión a nivel tecnológica

El Proceso de Discusión a nivel tecnológica fué abordado desde la perspectiva de la experiencia y los casos abordados por Microsoft Premier

Support, dentro de Microsoft Corporation. Es decir se el ser han fundamentado en dicha tecnología y realizado sus planteamientos con ese fundamento.

5. Discusión de impacto y repercusión de alternativas tecnológicas elegidas

El Impacto y repercusión de cada tipo de ataque y el abordamiento de cada tipo de tecnología fue apoyado del punto anterior, realizando sesiones con expertos en cada sector.

6. Planteamiento Formal de la plantilla tecnológica:

Constituyó la consolidación de pasos a nivel tecnológico, para plantear una infraestructura de sistemas.

7. Planteamiento Formal de la Plantilla Social

Constituyó la consolidación de pasos a nivel tecnológico, para plantear una Superestructura de sistemas.

8. Publicación del Proyecto

Es la fase final y más importante donde se discutirá el aporte del proyecto de seguridad a la organización.

CAPITULO III

MODELO PROPUESTO DE ARQUITECTURA DE SISTEMAS SEGUROS EN INTERNET

El Modelo Propuesto de Arquitectura Integral de Sistemas Seguros en Internet consta de dos partes:

SUPERESTRUCTURA DE SISTEMAS

La Superestructura de Sistemas o Arquitectura Social Segura de Sistemas es el conjunto de normas, políticas y procedimientos dentro de la organización, destinados a organizar, controlar, auditar y presupuestar los procesos que involucren la manipulación de información crítica, cuyos riesgo pueda alterar el funcionamiento normal de la organización o representar la pérdida de la misma bajo circunstancias inesperadas.

INFRAESTRUCTURA DE SISTEMAS

La Infraestructura de Sistemas es el conjunto de Arquitecturas Tecnológicas de Seguridad Óptimas, destinadas a proteger la inversión en tecnología de la organización de amenazas tecnológicas externas, tales como los ataques de hackers, crackers y virus.

En suma, tenemos:

ARQUITECTURA INTEGRAL DE SISTEMAS SEGUROS=

[(SUPERESTRUCTURA DE SISTEMAS) + (INFRAESTRUCTURA DE SISTEMAS)]

Donde cada una de las variables, será definida dentro del alcance del proyecto de tesis.

SUPERESTRUCTURA DE SISTEMAS

La Superestructura de Sistemas se organiza en 6 etapas. Cada una de estas etapas constituye el resultado de la evaluación de la implementación de diversas metodologías de seguridad y sus resultados en las empresas y del esfuerzo profesional en determinar las mejores para convertirlas en políticas de uso aceptable.

CONOCIMIENTO DEL NEGOCIO

El primer paso es el Proceso del conocimiento de los requerimientos y estado del negocio y que niveles de servicio deben ser alcanzados por la organización (existente o a iniciarse). Esto se obtiene mediante una revisión interna del negocio. Para las organizaciones existentes este paso debería incluir el determinar las nuevas adquisiciones. La infraestructura tecnológica es la encargada de habilitar y brindar soporte al negocio. Esta debe ser un recurso utilizable. En este paso es cuando muchas organizaciones se

percatan de las fuerzas externas que afectan sus negocios. La Empresa debe integrar la seguridad como parte de la estrategia general del negocio. A continuación se presentan los pasos que se deben seguir para realizar la revisión del negocio:

REVISION DEL NEGOCIO

Para realizar la revisión del negocio, se considera que se debe tener claro el concepto y base del negocio, es decir comprender los orígenes del negocio, su razón de ser, para involucrarse en el y obtener el compromiso esperado. Se ha considerado que se deben seguir los siguientes pasos:

1. Revisar el estado actual de los negocios
2. Entender las metas del negocio
3. Analizar que tecnología está siendo usada actualmente que tecnología se usara
4. Implementar un Análisis Inicial de Riesgos
5. Iniciar el Proceso de Implementación

Sin embargo, en la mayoría de compañías, que ya existe algún tipo de seguridad se debe realizar un proceso de evaluación para revisar la brecha que existe entre la seguridad actual y la objetivo. Se propone los siguientes pasos para identificar los requerimientos de seguridad de una compañía:

1. Identificar los Negocios Clave
2. Identificar los usuarios Involucrados con el Tema
3. Compilar demografía de clientes
4. Identificar los proveedores
5. Identificar los socios de negocios
6. Identificar la competencia
7. Identificar las tendencias y estándares industriales

A continuación se detalla los pasos necesarios para realizar una adecuada identificación de requerimientos de seguridad del negocio:

1. IDENTIFICAR LOS NEGOCIOS CLAVE

Un error común de las compañías es dirigirse primero a la seguridad y luego al negocio. Para se debe entender cual es el negocio clave y porque necesita una interfase con Internet.

2. IDENTIFICAR LOS STAKEHOLDERS O USUARIOS INVOLUCRADOS DIRECTAMENTE

Se deben identificar todos los involucrados con cada proceso de la empresa que necesite estar seguro.

3. COMPILAR DEMOGRAFIA DE CLIENTES

Se debe entender la compañía desde todas las perspectivas: Internas y Externas, identificando el número de empleados, la base de clientes y el volumen de ventas.

4. IDENTIFICAR LOS PROVEEDORES

Es muy importante identificar los proveedores con los que la compañía se conecta directamente a los Sistemas de Procesamiento de Datos.

5. IDENTIFICAR LOS SOCIOS DE NEGOCIOS

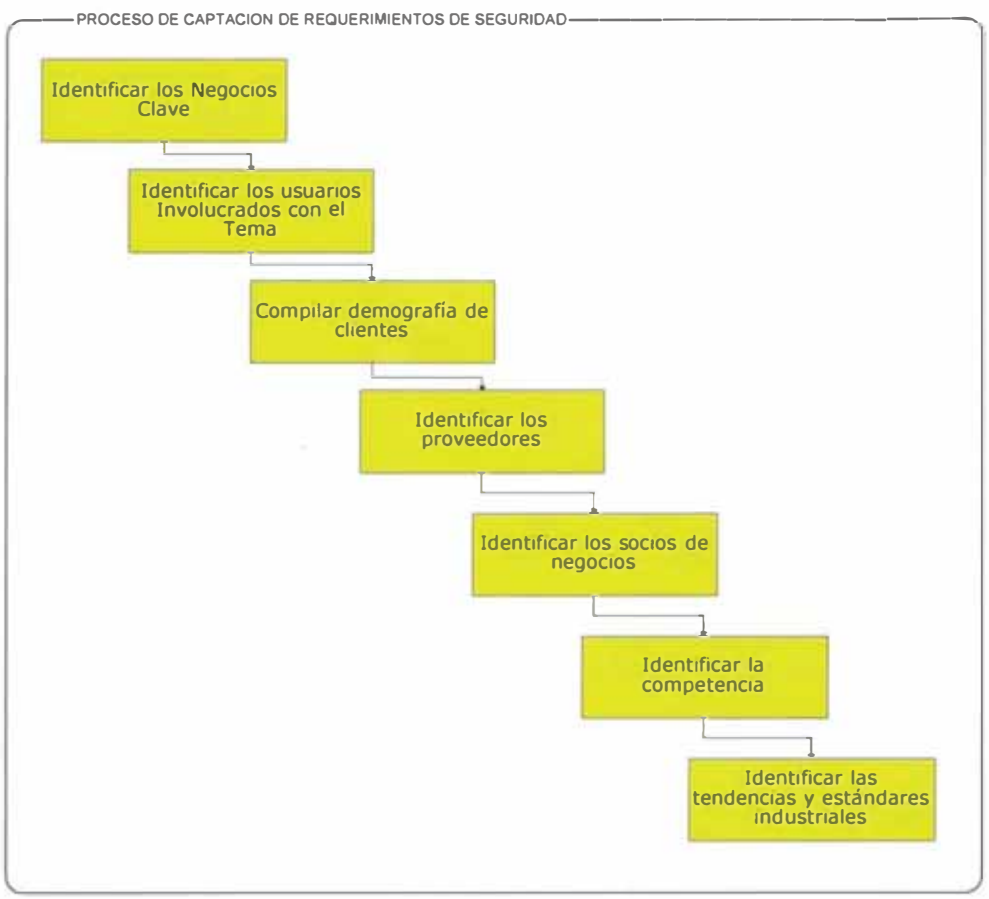
Se debe identificar claramente los socios de negocios, que muchas veces no son proveedores.

6. IDENTIFICAR LA COMPETENCIA

La Competencia a menudo realiza un seguimiento de las compañías. Por ello se debe identificar las tendencias y estándares industriales.

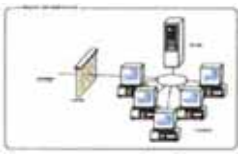
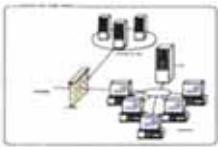
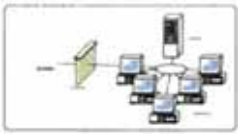
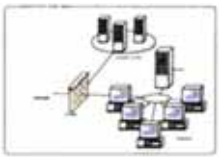
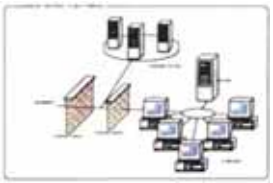
7. IDENTIFICAR LAS TENDENCIAS Y ESTANDARES INDUSTRIALES

Las Tendencias sirven para determinar hacia donde se deben enfocar los esfuerzos tecnológicos que se van a realizar.



En nuestro país, el siguiente puede ser un cuadro sugerido de inversión en Seguridad de empresas, este está clasificado por distribuciones de seguridad. Cada una de esas distribuciones de seguridad se explicará en la sección posterior:

Tipo de Empresa	**Escenarios Sugeridos**	**Distribución de Arquitectura Recomendada**	**Descripción de Entorno de Negocios**	**Montos Aproximados Anuales**
Pequeña Escala	Empresas de Servicios de Internet	Proveedores de Internet	Cabinas públicas de servicios de Internet	Menor a 10,000
	Empresa de sector de negocio	Hosting vía Proveedores de Internet	Pequeñas compañías de comercio de productos	Menor a 20,000
	Empresa de servicios	Hosting vía Proveedores de Internet	Pequeños proveedores de servicios	Menor a 30,000

Mediana Escala	Empresa de sector vertical de negocios	 Bastion Host	Sector Bancario, Sector pesquero, Constructoras	De 30,000 a 100,000
	Empresa de servicios	 Three Hommed	Sector de servicios de almacenamiento y publicación de información	De 100,000 a 200,000
Gran Escala	Empresa de sector vertical de negocios	 Bastion Host	Corporaciones nacionales, Entidades gubernamentales, Corporaciones transnacionales	De 200,000 a 300,00
	Empresa de servicios	 Three Hommed	Entidades gubernamentales	De 300,000 a 500,000
	Corporaciones empresariales	 Back to Back Three Hommed	Sector bancario, Telcos, Entidades gubernamentales	De 500,000 a más

Donde:

Empresa de Pequeña Escala:

Podemos definir una empresa de pequeña escala con una inversión en infraestructura de Sistemas menor a US$ 30,000 anuales. Es decir cuyo ingreso resultante bordea esa cantidad. Por lo general en esta categoría se incluyen compañías que subcontratan los servicios de otras para la publicación de información, y cuyos montos se deben en gran parte al uso

licencias de antivirus corporativos y pagos de almacenamiento y línea dedicada.

Empresa de Mediana Escala:

Podemos definir una empresa de mediana escala con una inversión en infraestructura de Sistemas mayor a US$ 30,000 y menor a US$ 200,000 anuales. Es decir cuyo ingreso resultante bordea esa cantidad. En este caso, las empresas poseen su propia infraestructura de hardware y además invierten en software de seguridad y antivirus corporativos.

Empresa de Gran Escala:

Podemos definir una empresa de mediana escala con una inversión en infraestructura de Sistemas mayor a US$ 200,000. Es decir cuyo ingreso resultante bordea esa cantidad. En este caso, las empresas poseen su propia infraestructura compleja de hardware y además invierten en software de seguridad y antivirus corporativos.

Una vez realizada la revisión del negocio, la organización se debe enfocar en la obtención de un entorno de seguridad. La Seguridad en Internet no es un simple conjunto de herramientas, documentos o software. Es una actitud holística para proteger los negocios de nuestras empresas- Un estado mental.

La siguiente, es una fórmula genérica[5] de seguridad que se cumple para un entorno de negocios en Internet:

$$ES \quad (P^2 + H) * C$$

ES (Entorno Seguro)= **[P2*(**Politica y Procedimientos**)+H (** rr r a **)]*C** (Compromiso)

Cada ítem es muy importante:

La Política y los Procedimientos manejan la seguridad del entorno; Las Herramientas ayudan a implementar los requerimientos de seguridad; y el Compromiso es requerido para realizar todo el trabajo. Como la fórmula muestra, si una organización crea la mejor política en el mundo y luego compra las mejores herramientas disponibles pero carece de algún compromiso, la seguridad del entorno del negocio fallará (Esto está garantizado).

[5] Esta fórmula ha sido tomada de los estudios de Timothy Speed, Arquitecto de Seguridad de Lotus Professional Services (LPS) de IBM.

A continuación, la descripción de cada uno de los pasos de este proceso:

COMPROMISO:

La Organización necesita integrar la seguridad en cada faceta del negocio. A esto le podemos llamar "Enfoque de arriba hacia abajo y de abajo hacia arriba". Primero, necesitamos administración para manejar la importancia de la seguridad. La Seguridad se inicia en los alto de la organización y se mueve individualmente hacia abajo hacia cada contribuyente. No es sólo una carga que se debe revisar anualmente como parte del proceso de presupuesto, pero si es una parte integral de cada proceso y subsistema. La Seguridad esta implementada desde lo más alto de la organización, sobre los CxOs (Algún Gerente de la organización: CEO, CIO, CFO o si la empresa no es una corporación, podemos partir de los Gerentes Generales). El Gran error que una empresa que da la cara a Internet puede cometer es considerar la Seguridad en Internet un **"Mal Necesario"**. La Seguridad en Internet debe ser vista como un bien competitivo. Cómo sus funciones del negocio dicen mucho sobre la calidad de la compañía, incluyendo su seguridad.

POLITICAS Y PROCEDIMIENTOS

Una política de seguridad es la fuerza dictatorial de que seguridad es necesaria y donde. Las Políticas pueden manejar los procedimientos y

herramientas que es necesario identificar y crear. Los procesos de creación de dichas políticas tomarán en cuenta los requerimientos del negocio, los riesgos del negocio, los riesgos de Internet y los costos de proteger los varios componentes del negocio.

Las políticas pueden también ser definidas de la siguiente manera:

- Requerimientos de la compañía para la protección adecuada de información.
- Los Procedimientos adecuados para prevenir y responder los incidentes de seguridad.
- Los requerimientos estratégicos para asegurar la conducción del negocio hacia la e-empresa.

Los Procedimientos de seguridad definen los pasos necesarios para proteger una empresa, incluyendo procesos, estándares y guías. A continuación se presenta los puntos críticos donde se deberían definir políticas de seguridad:

POLITICAS DE SEGURIDAD FISICA

AUTENTICACION

Existen diversos métodos que pueden ser utilizados para realizar la autenticación de un usuario:

- Nombre de usuario y Password: Es fácil de configurar e Implementar La mayor parte de Sistemas Operativos y Servidores Web tienen algún tipo de autenticación de nombre de usuario y password.
- Certificados (X.509v3): Lo más importante de los certificados es que permiten ser usados por los usuarios finales para asegurar su identidad. Aunque las soluciones PKI no son muy comunes y son costosas no deja de ser una buena opción para las empresas que desean asegurar la autenticación a determinado nivel.
- Anónimos: Este tipo de autenticación consiste en otorgar acceso a los usuarios a los recursos que no necesitan autenticación previa. Por lo general el usuario ingresa "anonymous" como un user id. De la misma manera, por lo general el password es fijado por defecto o generado por el servidor.Es por ello que este es un Método de Autenticación y Autorización a la vez. Este Sistema se apoya de las ACL ("Access Control Lists") y los logs de auditoria.

TARJETAS INTELIGENTES

Una Tarjeta inteligente es un dispositivo del tamaño de una tarjeta de crédito que posee un procesador central integrado que es capaz de almacenar información tal como información personal del poseedor de la tarjeta- Fecha de nacimiento, información de cuentas bancarias, registros médicos, etc. La seguridad es mantenida a través de combinaciones de medidas tales como números de pin, llaves públicas y privadas y passwords.

BIOMETRICAS

Un Sistema de Autenticación de Biométricas usará dispositivos como impresoras dáctiles o scanners digitales. Este tipo de dispositivos puede asegurar una gran seguridad para entornos de alto riesgo que necesitan limitar y controlar el acceso a Sistemas Sensibles. Es costoso de implementar, si embargo la persona es la autenticación (Muy difícil de impersonar).

ACCESO

Una política de Seguridad Física de acceso es requerida para cada compañía. Esto es donde los Administradores de Sistemas de Redes y usuarios finales necesitan tomar precauciones para prevenir brechas de seguridad físicas. La Seguridad Física puede incluir acceso a los Servidores, routers, closets de cableados, departamentos específicos, o algún lugar asociado a información del negocio. Esta también incluye controlar el acceso a passwords de software e inclusive el método de bloquear los Sistemas al alejarse de los computadores.

Un Documento de Políticas de Seguridad Física debería incluir los siguientes aspectos:

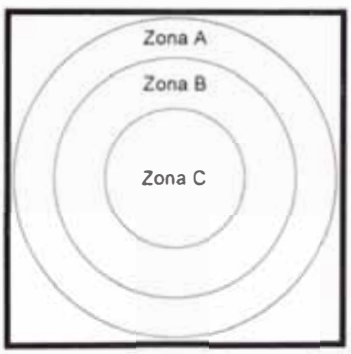
ZONAS DE ACCESO

Es recomendable definir zonas de acceso físico al público en general y a los empleados.

Zona A: Areas abiertas al público.

Zona B: Áreas cerradas al público, pero abiertas a los empleados.

Zona C: Áreas protegidas. Accesibles sólo con identificación, tarjetas o biométricas. Los visitantes no están permitidos.



Los requerimientos de cada compañía serán diferentes. Una compañía con sólo 10 personas pueden ser fácilmente capacitadas para pedirle información a extraños acerca de que hacen en su edificio. Pero una compañía con 10000 empleados quizás no distinga entre un empleado y un visitante.

ACCESO A SALAS DE SERVIDORES

Las Salas de Servidores deben pertenecer bloqueadas si es posible con tarjetas electrónicas o de escáner electrónico.

BACKUPS:

Los Backups son partes integrales de cualquier Sistema de Cómputo. Estos pueden estar enlazados a procesos de recuperación de Desastres. A continuación se presentan algunas sugerencias a tomar en cuenta en la implementación de Sistemas de Backups:

Los Medios de Backups deben estar almacenados en áreas bloqueadas o salas bloqueadas.

Los Backups regulares deben ubicarse fuera de las instalaciones de la compañía.

En el caso de almacenar Backups en las instalaciones de un tercero, de un tercero no descuidar los aspectos legales.

Usar monitoreo ambiental y seguridad en el mantenimiento del sitio.

MEDIA:

Disquetes, CD's, cintas y discos removibles son a menudo un medio de acceso a la red para los virus. Se deben mantener políticas de seguridad de dispositivos, a fin de evitar la contaminación y filtro de información.

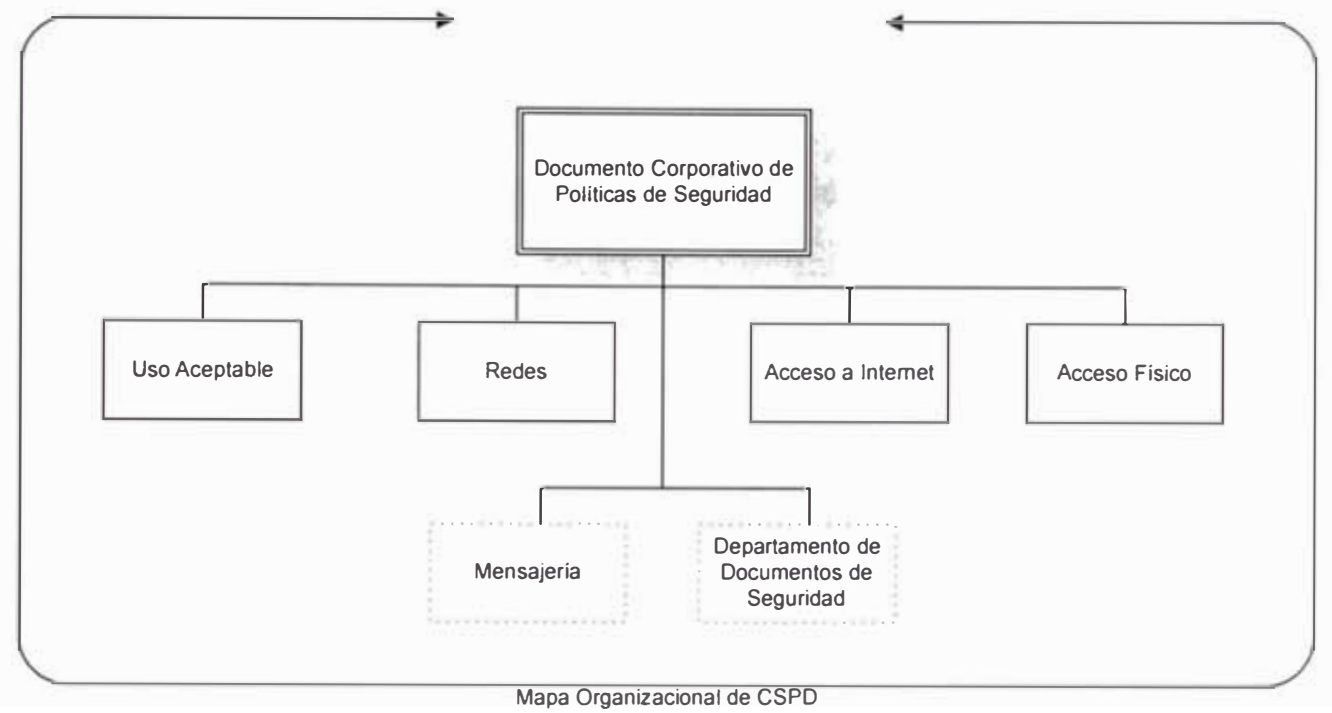
COMPUTADORES:

En esta parte se deben considerar puntos como los siguientes:

- Administración de Políticas. Por ejemplo en Windows NT.
- Passwords y bloqueos de las computadoras.
- Seguros físicos para las laptops
- Encriptación de data confidencial en las laptops.
- Se debe contemplar el uso de Antivirus

DOCUMENTO DE POLÍTICAS DE SEGURIDAD CORPORATIVA

El Documento que se debe crear en la organización es el Documento de Políticas de Seguridad Corporativa (DPSC). Este documento debe ser un reflejo de todas las políticas consideradas en este paso. El DPSC debe incluir las políticas y dirección que apoye a la misión de la organización en la protección de recursos corporativos. El DPSC debe establecer políticas uniformes, responsabilidades y autoridades para llevar a cabo el Programa Corporativo de Seguridad.



Mapa Organizacional de CSPD

El Alcance del DPSC debe incluir las compañías de la empresa, vendedores, comunidades y clientes. Uno de los más grandes errores que se encuentra es que las compañías pasan por alto los temas de seguridad cuando se fusionan o se retiran de la empresa. Todos estos tópicos deben ser considerados en el DPSC. El DPSC debe hacer declaraciones específicas acerca de cómo serán manejadas la adquisición y los productos desde una perspectiva de seguridad. Los componentes de software y hardware que constituyen los bienes de la empresa representan una inversión monetaria cuantificable que debe ser protegida. De igual manera para la información almacenada en Sistemas de Línea de Negocio, algo que quizás ha tomado grandes cantidades de recursos en generar y posiblemente nunca pueda ser reproducida.

El DPSC debe tener una declaración de Misión que discute las metas y métodos específicos que la compañía intentará lograr en su búsqueda de seguridad. Se recomienda que se incluyan los siguientes puntos en la

Declaración de la Misión de Alto Nivel:

- El Diseño e Implementación de Seguridad
- Explicación de la necesidad de Seguridad
- Medidas de Seguridad: Físicas y Sociales
- Las responsabilidades de seguridad para los diversos roles en que cada miembro de la compañía quizás desempeñe.
- Niveles de apropiados de seguridad a través de estándares y guías
- Clasificaciones de Seguridad
- Consideraciones Legales
- Manejo de Incidentes
- Auditoria

HERRAMIENTAS

A nivel interno se tienen las herramientas. Estas incluyen el software y/o hardware usado para implementar el dictado de una política. Esto puede incluir, pero no está limitado a, software de scan de virus, Firewalls, software de firmado de aplicaciones, network scanners, herramientas de

administración de hacking y herramientas de revisión de eventos de seguridad en Sistemas Operativos.

Firewall:

Es un elemento de seguridad de redes que brinda el control de accesos desde y hacia Internet, Intranet y Extranet con fuerte autenticación, encriptación, traducción de direcciones (NAT[6]) y servicios de seguridad del contenido para brindar una solución integrada y escalable para cubrir las demandas de toda organización.

Software de Detección de Intrusos:

Es un sistema automatizado de detección y respuesta en tiempo real a intrusos en los sistemas de información. Provee vigilancia las 24 horas del día, y permite interceptar y responder automáticamente a brechas de seguridad y abusos de la red interna, antes de que se vean comprometidos los sistemas. Asimismo, monitorea discretamente el tráfico de la red, a la vez que detecta y responde automáticamente a las actividades sospechosas, brindando los máximos niveles de seguridad.

---

[6] NAT: Network Address Translation

Network Scanners:

El Network Scanner evalúa la seguridad desde la perspectiva de los servicios TCP/IP. Sistemáticamente prueba cada dispositivo de la red para verificar las vulnerabilidades de seguridad. Los dispositivos de red pueden incluir un host UNIX, un sistema Windows 95/Windows NT, un router, un servidor Web, e inclusive un terminal X.

Realiza evaluaciones automatizadas de seguridad de redes TCP/IP desde una estación de trabajo Windows NT o UNIX. Utilizando el más completo conjunto de pruebas de penetración disponibles, el software busca las debilidades que los intrusos explotan más comúnmente para obtener acceso no autorizado a la red. Detecta riesgos y provee amplios reportes y acciones correctivas recomendadas.

ANALISIS DE RIESGOS

Es muy importante determinar los prospectos de amenazas internas y externas, para realizar una adecuada clasificación de riesgos. Se debe tomar en cuenta la pérdida potencial en el caso que alguna de las amenazas sea satisfactoria. Esta es una evaluación del entorno computacional de la compañía para determinar que bienes son valuables de proteger y hasta donde deben ser protegidos. Podemos obtener una lista de todos los bienes de TI de la compañía, que incluyen ambos, tangibles, como servidores y

estaciones de trabajo e intangibles, como software y datos. Para conducir el análisis de riesgos se pueden seguir los siguientes pasos:

El Análisis de Riesgos es el proceso de determinación de los puntos donde se deben focalizar el tiempo, esfuerzos, y recursos financieros para realizar la implementación de seguridad. Este proceso incluirá el Análisis de amenazas, impacto de aquellas amenazas, y sus correspondientes riesgos. Una vez ejecutado el proceso las debilidades y riesgos de negocios más significativos serán más evidentes, y esto será de de gran utilidad para el desarrollo de las contra-estrategias.

Un enfoque discreto para afrontar la determinación de un riesgo es el siguiente:

Riesgo = Impacto + Amenazas + Oportunidades

El Riesgo está constituido por la suma del impacto, amenazas y oportunidades en un entorno. El Análisis de riesgos se apoya de la Revisión de seguridad tecnológica y la Tabla de riesgos de entorno.

Revisión de Seguridad tecnológica

La revisión de seguridad tecnológica es un proceso que se encarga de revisar cada tecnología o servicio dentro de la organización. Definamos dos términos: Exposiciones y Controles. Una exposición es todo aquello que puede hacer que alguno de los sistemas sea vulnerable a algún incidente. El Control es lo que puede ser hecho en vez de aceptar ser atacado. Por ello, a continuación se muestran los pasos básicos para realizar una revisión de seguridad tecnológica:

Primer Paso:

Realizar una plantilla de Revisión de Seguridad Tecnológica

- Un Web Site
- El Sistema Operativo usado en el Web Site
- El Servidor Web
- La DMZ

Revisión de Seguridad Tecnológica

Nombre de Tecnología o Servicio revisado: _____

Usuario actual o esperado del servicio: _____

Exposición: _____

Exposición # _____

Resúmen de Exposiciones _____

Orígen de Exposiciones (Testing, Cert) _____

Control sugerido # _____

Control sugerido a detalle _____

Costo o impacto al negocio de este control _____

Controles requeridos # _____

Controles requeridos a detalle _____

Costo o impacto al negocio de este control _____

Comentarios _____

- Clientes externos
- Empleados
- Vendedores
- Clientes internos (Empleados que cargan a su Centro de Costo)

Segundo Paso:

En este paso se listan las exposiciones, que se han conseguido identificar. Una buen enfoque es el de por ejemplo en el caso de trabajar con un proveedor de software, contactarles y ver que exposiciones conocidas existen. De la misma manera es recomendable revisar sites de seguridad y hacking tales como http://www.10pht.com/, y listados tales como el de CERT para su software, http://www.cert.org. A continuación una muestra de algunas exposiciones:

Exposición # (Algún # de Seguimiento)	**Resúmen de Exposiciones**	**Orígen de Exposiciones (testing, Cert)**
1001	SO se cae debido a un ataque DDoS	Advertencia de CERT XXX.xx.V3
2023	Usuarios pueden enviar información confidencial fuera de la compañía	Encriptación de mails está disponible pero no se puede forzar a los usuarios a usarla.
3011	Herramienta de hacking puede brindar acceso de administradores para cualquier usuario	Del site de un hacker.
4067	Ninjas ingresaron al piso 30 del edificio y forzaron a todo el mundo a entregarles sus claves de usuarios	No ocurrencias conocidas de este tipo de ataque.

Tercer Paso:

El Tercer Paso consiste en listar por cada exposición potencial, algunos controles sugeridos que pueden contrarrestar la lista de ataque:

Exposición # (Algún # de Seguimiento)	**Control sugerido a detalle**	**Costo o impacto al negocio**
1001	Actualizar firewall a versión 3.1	La Actualización es gratis por el vendedor
2023	Entrenar una armada de ninjas	$ 1,000,000

Cuarto Paso:

El Cuarto Paso consiste en listar por cada exposición potencial, controles requeridos que puedan contrarrestar la lista de ataque:

Exposición # (Algún # de Seguimiento)	**Control requerido a detalle**	**Costo o impacto al negocio**
2023	Entrenar a los usuarios en S/MIME	Costo agregado por entrenamiento de $10 más por usuario
3011	Actualizar SO con Service Pack 9	La Actualización es gratis por el vendedor

Quinto Paso:

El quinto paso consiste en asignar un impacto al negocio. Este podría pertenecer a las siguientes categorías:

Escape de Datos:

Por ejemplo enviar información a algún individuo externo a la organización, información a la que no debería tener acceso.

Integridad de Datos comprometida:

El mejor ejemplo es el de la información de tarjeta de crédito robada de varios Web Sites.

Pérdida de confidencialidad del cliente:

El caso de colocar pornografía en un Web Site de un cliente.

Impacto de red:

Esto es cuando alguien ataca la red corporativa y la deja en estado de colapso

Impacto de mensajería:

Cuando los sistemas de mensajería son vulnerados

Tabla de Riesgos del Entorno:

Tabla de Riesgos del Entorno consta de dos tablas: La Tabla de Impacto y la Tabla de Costos. Representa un resumen de la información mostrada

anteriormente agrupada por categorías y cruzada por costos, de la siguiente manera:

Potencial	Área de Impacto				
	Fuga de datos	Integridad de datos comprometida	Perdida de confidencialidad del cliente	Impacto de red	Impacto de mensajería
Alto	$ 1500	$ 5000	$ 1500	$ 15300	$ 45000
Medio	$ 1500	$ 9000	$ 1800	$ 7500	$ 38000
Bajo	$ 1500	$ 7500	$ 1500	$ 1500	$ 15000

Las ventajas que nos genera el uso de esta técnica son múltiples y nos ayudan a desarrollar estrategias para:

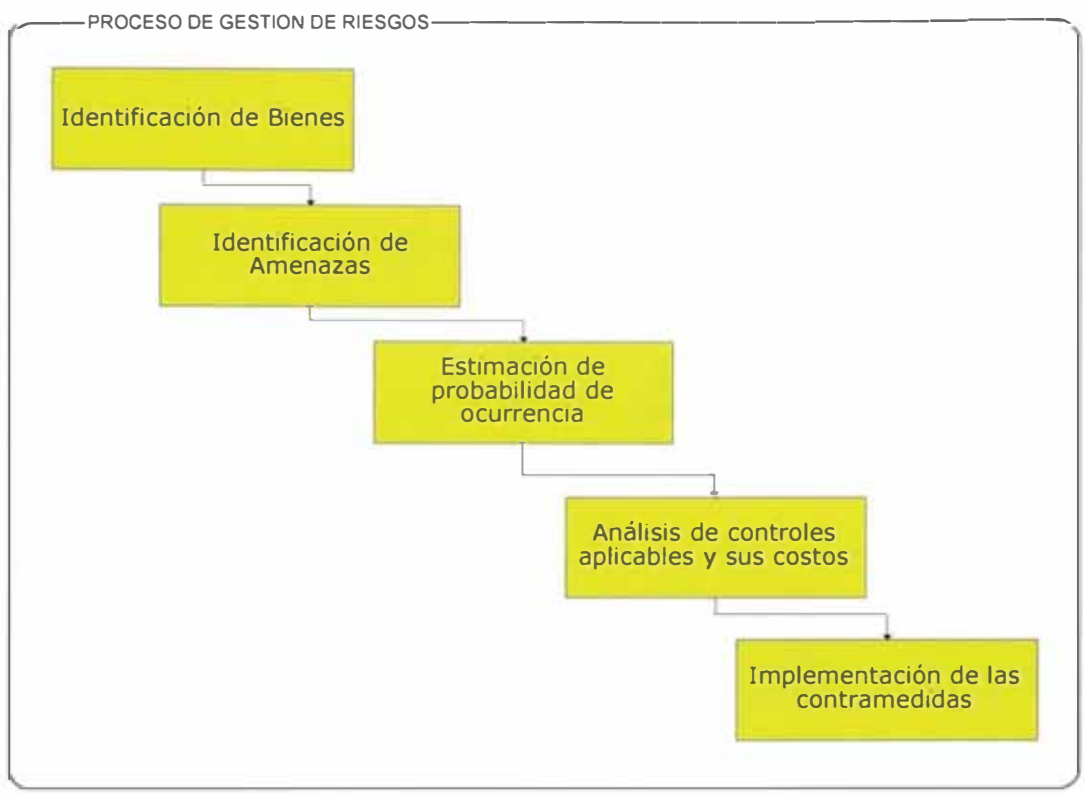
- Eliminar el riesgo
- Reducir el riesgo a un nivel aceptable
- Minimizar el daño de un incidente
- Crear las **contramedidas necesarias** para cada tipo de incidentes.

A medida que se va desarrollando el Análisis de Riesgos, se deberían incluir las siguientes variables:

- Arquitectura física de red
- Firewalls

- Routers
- Servicios de Mensajería
- Servidores Web
- Sistemas Operativos
- Servicios de Aplicaciones
- Servidores de Aplicaciones
- Flujo de datos y Protocolos de niveles de servicios
- Infraestructuras de Autorización y Autenticación
- No repudio
- Implementación de Aplicaciones

Finalmente se pueden considerar como un buen alcance, las siguientes etapas dentro de un proceso de gestión de riesgos:



MANEJO DE INCIDENTES Y MITIGACION E IDENTIFICACION DE AMENAZAS

Este es el proceso de manejo de eventos. Un incidente es un evento no planificado, e inesperado que requiere acción inmediata para prevenir la pérdida de de negocios, bienes, o confidencialidad. Todas las políticas deben tener un componente manejador de incidentes más un componente de feedback. El Ciclo de Feedback es el mecanismo que mantendrá las políticas actualizadas y en uso. Se debe definir un equipo interno de respuesta de incidentes de cómputo (CIRT) que debería tener las siguientes funciones:

- Administración

- Personal Técnico
- Consultoría Legal (Por lo menos en stand by)
- Coordinador de Equipos
- Especialista en comunicaciones

Para conseguir la determinación de amenazas se considera que nos debemos de apoyar en la siguiente Tabla de Funciones de Negocio:

Funciones de Negocio	Definición crítica	Nivel de servicios

Donde:

Las Funciones del Negocio son aquellas que se realizan pero se considera que se realizan mal. Es decir el nivel pesimista de nuestro nivel de servicios.

Las definiciones críticas incluyen la información de las funciones pero a detalle; es decir la importancia y el impacto de la función si el servicio sufre una caída (Por ejemplo).

El nivel de servicios es el porcentaje de rendimiento que esperamos de tiempo de trabajo (En teoría un esquema de alta disponibilidad, donde los servicios trabajan satisfactoriamente el 99,99% de los 365 días del año).

Una amenaza es un peligro que puede impactar la seguridad de los bienes del negocio, que puede conllevar a perdidas potenciales de dinero, daños del capital, o pérdida de confidencialidad del cliente.
Las amenazas a los negocios se pueden originar de diferentes orígenes:

- Errores humanos
- Ataques externos (Hackers)
- Personas deshonestas
- Sabotaje técnico
- Fuego, Inundaciones, actos de Dios
- Empleados actuales o pasados inconformes o decepcionados

Para determinar firmemente las amenazas, se considera que se deben seguir los siguientes pasos:

1. **Definir objetivos de seguridad básicos.** Por ejemplo disponibilidad, confidencialidad, e integridad.

2. **Definir las diversas amenazas y protecciones potenciales**, como usuarios externos, empleados de Internet, Hackers, o consejos CERT basados en soluciones tecnológicas que se tiene para el negocio.

3. **Generar un análisis de impacto de negocios.** Cuál es el impacto si la amenaza es realizada? El impacto es una consecuencia del negocio y no una consecuencia técnica.

4. **Utilizar una escala que evaluará el impacto a los negocios.** Se considera que los siguientes son buenos ejemplos:

    a. **Bajo impacto:** Sin o con un mínimo efecto, la mayoría de las operaciones no son afectadas.

    b. **Menor impacto:** Las Operaciones del negocio no están disponibles por una cierta cantidad de tiempo; algunos ingresos son perdidos, la confidencialidad del cliente no es impactada.

    c. **Impacto Moderado:** Pérdida intermedia a operaciones de negocio con algunas perdidas en la confidencialidad del cliente.

    d. **Impacto Significativo:** La confidencialidad del cliente ha sido significativamente impactada; algunos clientes estarán perdidos permanentemente.

e. **Alto:** El Impacto es alto, pero la compañía quizás sobreviva a considerable pérdida de ingresos.

f. **Desastre**: El efecto es catastrófico; la compañía no sobrevivirá. Se sugiere comenzar a buscar un nuevo trabajo.

5. **Determinar la posibilidad de una amenaza.** Se sugiere la siguiente escala de ejemplo:

a. Es altamente posible que la Amenaza nunca ocurra.

b. Es posible que la Amenaza ocurra una vez en la vida del servicio o del producto.

c. Es posible que la Amenaza ocurra una vez al año.

d. Es posible que la Amenaza ocurra una vez al mes

e. Es posible que la Amenaza ocurra una vez a la semana.

f. Es posible que la Amenaza ocurra una vez al día.

6. **Listar las amenazas.** Se sugiere la creación de un formato extendido de RST (Revisión de Seguridad Tecnológica, anteriormente comentada en la

sección de riesgos). En este formato debería incluirse específicamente cada amenaza.

ENTRENAMIENTO DE EMPLEADOS Y CLIENTES

Crear un esquema de entrenamiento. Debemos estar seguros que empleados y clientes saben que “La Seguridad es parte del negocio” y que “La seguridad es responsabilidad de todos”. Si es posible, añadir seguridad a los planes de rendimiento de los empleados. Debemos ayudar a los empleados a comprender la importancia de la seguridad; si no ellos encontrarán un camino alrededor de esta.

DESARROLLO DE ESTRATEGIAS

A este punto, ya hemos identificado los procesos del negocio, y debemos continuar con la definición de las **políticas de protección** de cada componente.

Los puntos críticos que se deben tener en cuenta son:

- Acceso físico
- Redes
- Software
- Mensajería

- Uso aceptable
- Seguridad de Aplicaciones
- Encriptación
- Sistemas de Control de cambios
- Entrenamiento a usuarios
- Entrenamiento a Clientes

Para implementar todos los puntos que se han discutido se debe formar un comité de Seguridad. Este comité será el encargado de realizar la implementación del Esquema de Seguridad. Esto incluirá dirección inicial, feedback y auditoria. El Comité debe incluir representativos de cada área dentro de la empresa. De esta manera, las políticas creadas satisfarán las necesidades de la compañía entera.

El Comité deberá tener los siguientes miembros del equipo (Dependiendo del tamaño de la organización):

- **Gerente General:**

Necesita ser un miembro virtual del equipo. La Seguridad debe fluir desde lo alto a lo bajo de la organización.

- **Gerente de Tecnología y/o Operaciones:**

Todos los Gerentes de Tecnología necesitan ser miembros del equipo. Es correcto que ellos deleguen roles a personal capacitado y con poder de decisión.

- **Jefe de Seguridad de Información:**

Esta es una elección obvia. El será el conductor de la seguridad de la Información.

- **Representantes de Cada Área Funcional:**

Estos representantes deberían tener poder de toma de decisión.

- **Cuentas:**

Ellos proveerán la información del Análisis de riesgos.

- **Recursos Humanos / Capacitación:**

Ellos necesitan apoyar con capacitación de usuarios e información. Ellos también deben influir el tipo de información que necesita ser asegurada.

- **Expertos en Documentación / Escritores Técnicos:**

Para crear los documentos de necesarios.

- **Departamento de Tecnologías de Información:**

Ellos necesitan miembros que puedan traducir la tecnología en necesidades y requerimientos de negocio.

- **Legal:**

Ellos necesitan mantenerse con las últimas leyes y quizás con el apoyo de un experto de Leyes en Internet.

- **Miembro del Equipo de Respuestas a Incidentes:**

Este equipo manejará incidentes que no están cubiertos por la seguridad implementada.

- **Especialistas en Comunicación:**

En muchas empresas, existe un equipo de comunicaciones. La Comunicación a los usuarios finales sobre seguridad es crítica.

Naturalmente, que un miembro no se ha listado es el usuario individual. Usuario que debería ser cubierto por cada uno de los Representantes de cada Área funcional.

MANTENER LOS PROCESOS ACTUALIZADOS

Establecer la política que determine que los documentos deben mantenerse actualizados. Revisar los documentos en un cronograma. También, actualizar las políticas si cambian la plataforma o el software. Debemos estar seguros de enlazar las políticas de administración al entrenamiento del empleado. Si un cambio es realizado, el entrenamiento debe ser actualizado. Debemos atender el feedback de los empleados.

Definir los procesos de auditoria y usar la misma como parte de un proceso solicitado y también como un mecanismo para mantener la información actualizada.

INFRAESTRUCTURA DE SISTEMAS

SMART BACKBONE

Para la definición de un entorno de seguridad físicamente confiable y altamente disponible, se presentan las arquitecturas ideales de infraestructura. Al conjunto de estas disposiciones se les ha denominado "Smart Backbone", porque son el resultado de investigación de las arquitecturas más óptimas de infraestructura y son flexibles de acuerdo a las características del negocio.

ARQUITECTURAS DE HARDWARE DE SEGURIDAD

Las arquitecturas empresariales descritas en el capítulo II, constituyen las arquitecturas de negocios más comunes en nuestro medio. Aunque el desarrollo de algunas de ellas, aún está en propuestas de negocios, los clientes coinciden en que para invertir en una solución determinada de negocios, deben primero cerciorarse de que su organización no va a estar expuesta a riesgo alguno. He ahí el propósito de este punto. El de presentar

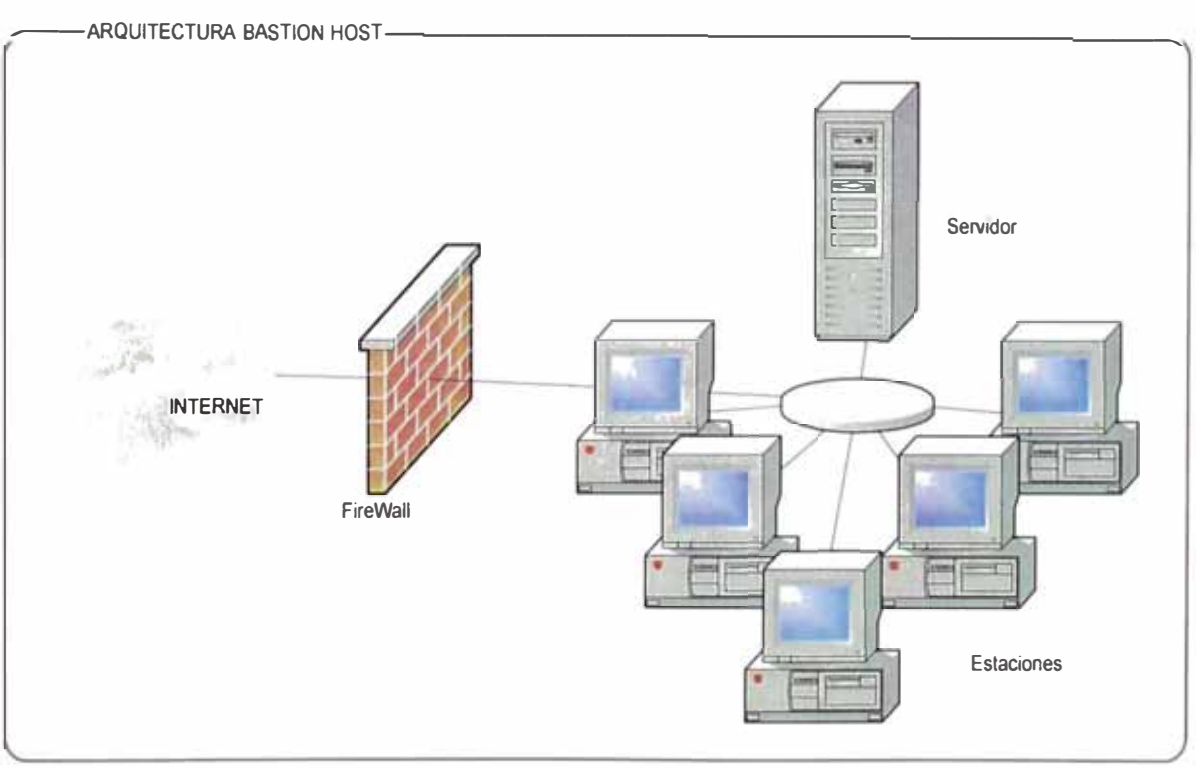
las arquitecturas de seguridad que deberían incluirse en un DDI (Documento de Despliegue de Infraestructura) para mostrar un mayor número de alternativas a la organización.

ARQUITECTURA DE HOST BASTION O BASTION HOST

En este tipo de Arquitectura, existe un computador que es el principal punto de contacto para que los clientes de redes internas obtengan acceso a Internet. Como un Firewall, el bastión host está diseñado para defender ataques a la red interna.

Un bastión host posee dos adaptadores de red, uno conectado a la red interna y otro conectado a Internet. Esta configuración aísla físicamente a la red interna de intrusos potenciales en Internet. Como el bastión host es un único punto de defensa, debe estar muy bien protegido.

Las ventajas de utilizar un Bastión Host están en que minimiza el costo y la cantidad de administración que es requerida por el firewall. Sin embargo, un



Bastión host depende de un único firewall para asegurar toda la red. Si un usuario de Internet compromete el firewall, el usuario de Internet podrá obtener acceso a la red interna de la organización.

ARQUITECTURA DE TRES OBJETIVOS O THREE HOMED

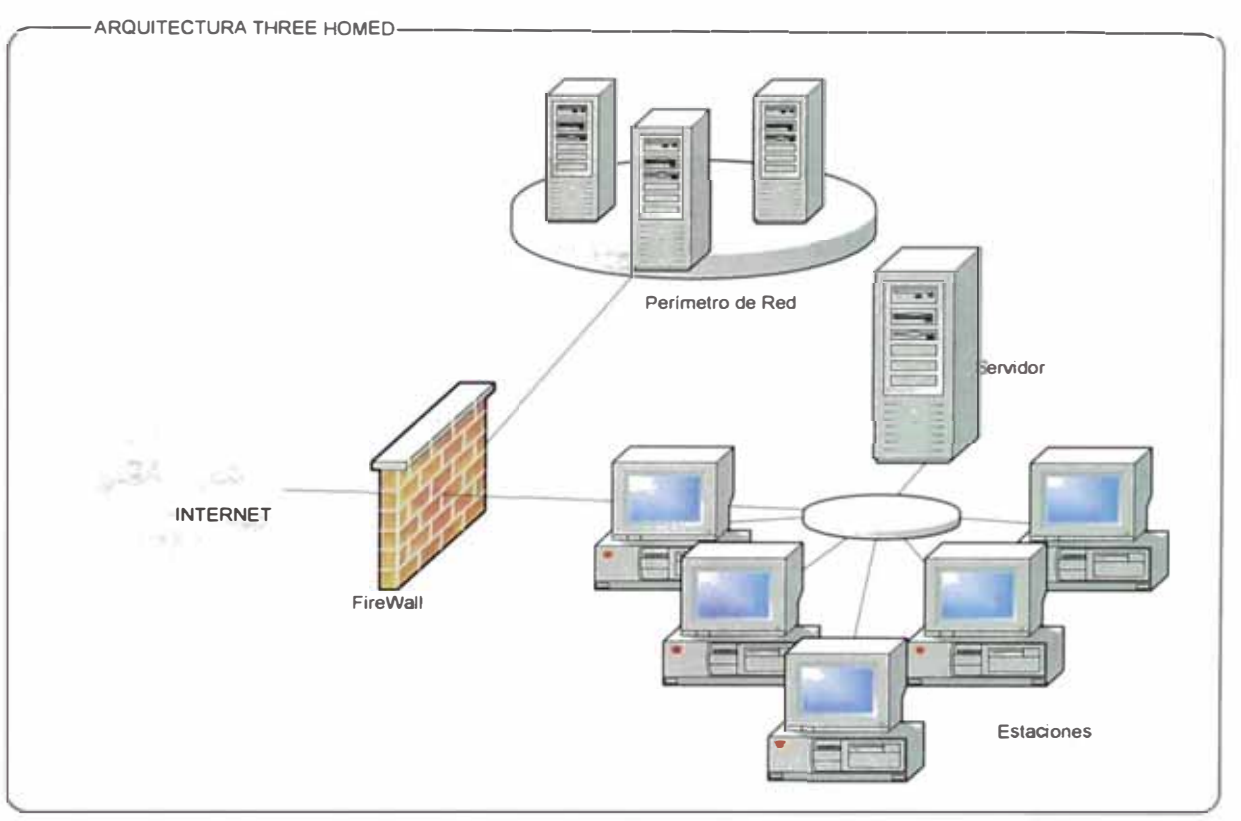
La Arquitectura Three Homed se compone de una red perimetral que contiene recursos que queremos poner al alcance de usuarios de Internet manteniendo la seguridad de dichos recursos. Una red perimetral esta separada de la red interna y de Internet. Una red perimetral permite que los clientes externos obtengan acceso a servidores específicos ubicados en la red perimetral, previniendo así completamente el acceso a la red interna.

Esta arquitectura es típica para implementar Servidores Web y servidores de correo. Una red perimetral puede configurarse en una o dos configuraciones: Three Homed Firewall y Back to Back Firewalls.

En una configuración de red perimetral Three Homed Firewall, el firewall es configurado con tres adaptadores de red. Cada adaptador es conectado a cada una de las siguientes redes:

- Internet
- Servidores de red internos localizados en la red perimetral
- Clientes de red internos

Aunque los servidores en la red perimetral tienen direcciones de Protocolo IP que pueden ser accedidas por clientes externos, el firewall no permite acceso a los recursos que están localizados en la red interna.

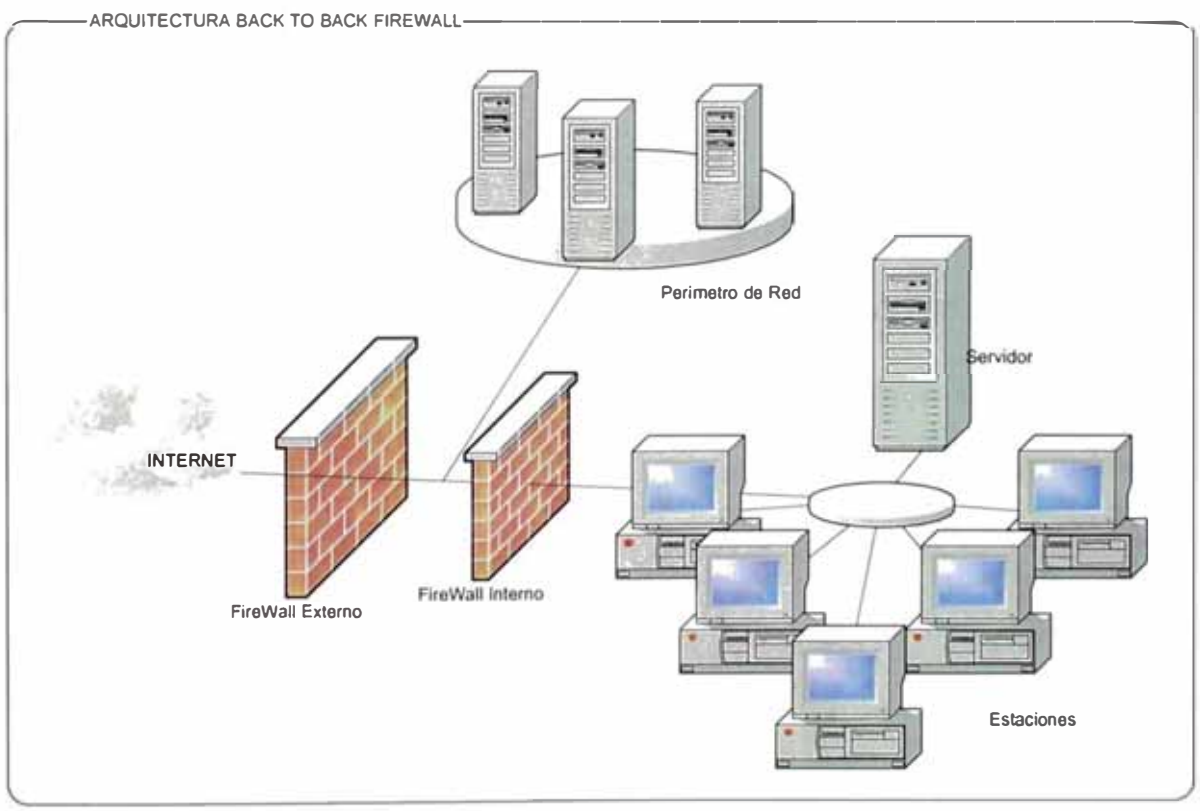


Una Arquitectura Three Homed provee mayor seguridad que una Bastion Host porque permite acceso seguro para algunos recursos de red de Internet sin permitir tráfico de red entre la Internet y la red interna. Un Firewall Three Homed brinda un único punto de Administración para configurar el acceso a la red perimetral y a la red interna.

Sin embargo, un Firewall Three Homed también presenta un único punto de acceso a todos los recursos de la red, por lo tanto se debe tener mucho cuidado en diseñar este punto de acceso.

ARQUITECTURA DE FIREWALL PARALELO O BACK TO BACK FIREWALL

En este tipo de Arquitectura, se colocan dos firewalls en cada lado de la red perimetral. Los dos Firewalls son conectados a la red perimetral, con uno conectado también a Internet y el otro conectado también a la red interna. En esta configuración, no existe un único punto de acceso. Para resolver la red interna, un usuario necesitaría haber pasado entre ambos firewalls.



Se puede configurar reglas de seguridad mas estrictas para Firewalls Back to Back que para un Three Homed, que vuelve la Arquitectura más confiable, así como también es más fácil configurar reglas para un diseño de un Firewall

Back to Back si las políticas de acceso de una organización permiten un limitado y muy controlado tráfico de red entre computadores en la red perimetral y las computadoras elegidas en la red interna.

PROTECCION SISTEMATICA DE SISTEMAS

CRIPTOGRAFIA

1. HISTORIA

La Criptografía es uno de los Sistemas más antiguos de de protección de datos. Los historiadores han encontrado evidencia de ella que data de hace 4000 años. La criptografía es creída por muchos originaria de Egipto, alrededor del 2000 AC. La china milenaria también usó códigos para ocultar el significado de sus trabajos. Sobre los años, han sido usados varios sistemas, desde una simple sustitución de letras o números a complejos teoremas matemáticos.

A través de la historia, todos los gobiernos han usado algún tipo de encriptación. Durante la edad media, la encriptación fue usada más pesadamente. Muchos de los primeros gobiernos europeos usaron criptografía. Esta encriptación fue usada para comunicarse con embajadores de gobiernos.

Con el pasar el tiempo, la encriptación ha sido mejorada por el uso de varias herramientas. Una fue la Rueda de Cifrado que fue inventada por Thomas Jefferson. Esta herramienta consistía de un conjunto de ruedas, cada una con un orden aleatorio de las letras del alfabeto. La Clave del Sistema es el orden de las ruedas. Cada rueda fue ubicada sobre un eje. El mensaje era codificado alineando las letras a través de los ejes con el eje que fue creado.

Cualquier otra fila de letras alineadas puede entonces ser usada como un texto cifrado. La desencriptación de requiere que la persona que ha recibido el mensaje para configurar las letras del texto cifrado a través de los ejes y encontrar un conjunto de las letras que sea legible. El recipiente entonces tiene un mensaje legible.

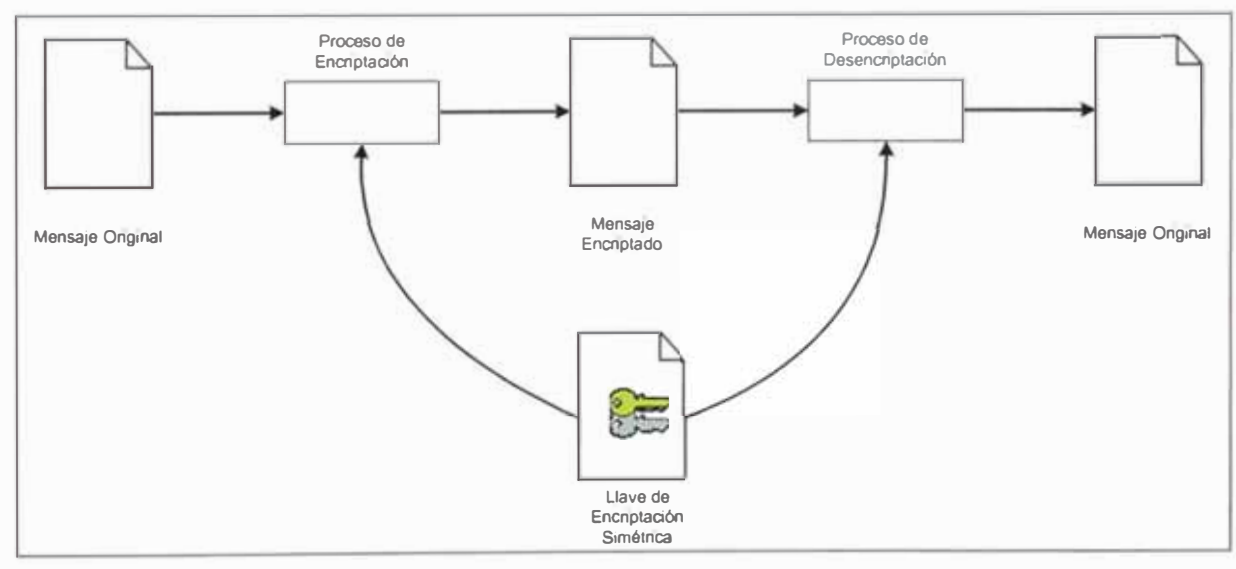
2. TIPOS DE LLAVES

Básicamente existen dos tipos de algoritmos basados en llaves: Simétricos y Asimétricos

ENCRIPTACIÓN SIMÉTRICA:

La Encriptación simétrica requiere la misma llave de encriptación para encriptar y desencriptar un mensaje. Por lo tanto, ambas partes (El que envía el mensaje y el que lo recibe) necesitan tener la misma llave de encriptación.

Una de las fortalezas de la encriptación simétrica es su velocidad. Los Algoritmos de encriptación simétricos están entre los más rápidos de encriptación y desencriptación de mensajes. Una de las principales debilidades de la encriptación simétrica es que ambas partes necesitan tener la misma llave de encriptación. El gran problema alrededor del uso de la encriptación simétrica es como obtener la llave de encriptación en ambas partes sin que esta caiga en las manos de un tercero que pueda estar prevenido de desencriptar los mensajes confidenciales.



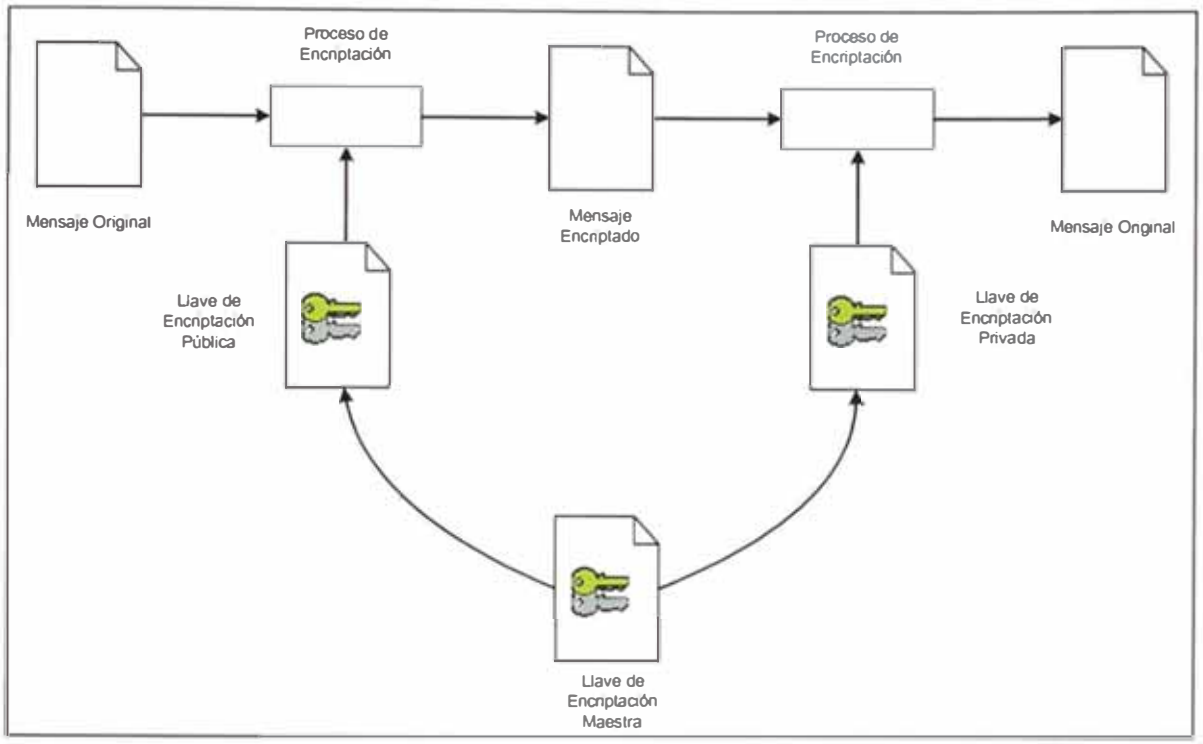
ENCRIPTACIÓN ASIMÉTRICA

La Encriptación Asimétrica o de Encriptación de Llave Pública utiliza dos llaves: Una pública que puede ser distribuida libremente y una privada que es mantenida segura. Cualquier mensaje encriptado usando cualquiera de las dos llaves puede sólo ser desencriptada usando la otra llave. Usualmente el

remitente encripta el mensaje usando la llave pública del destinatario del mensaje. Sólo el destinatario puede desencriptar el mensaje usando su llave privada.

En la Encriptación asimétrica, ambas llaves son derivadas de una llave de encriptación maestra, como se ilustra en la figura siguiente. Cuando las llaves son derivadas de una llave maestra común, las dos llaves son matemáticamente relacionadas, pero ninguna de las llaves puede ser calculada de la otra. Luego que las llaves públicas y privadas han sido derivadas, la llave maestra es destruida.

Como la encriptación asimétrica trabaja correctamente, es ideal para usarse sobre una red pública como Internet. Sin embargo, uno de los grandes problemas con la encriptación asimétrica es su lentitud en comparación con la encriptación simétrica. Como resultado, lo que es más recomendable es una combinación de encriptación simétrica y asimétrica. Una llave de encriptación simétrica es generada para el uso durante la sesión; entonces esta llave es encriptada e intercambiada utilizando encriptación asimétrica. Cuando la sesión finaliza, la llave de sesión es destruida.



OTRAS FORMAS DE ENCRIPTACIÓN

La Encriptación Simétrica y Asimétrica no son los únicos tipos de encriptación que existen. También existen los siguientes:

OR EXCLUSIVO (XOR)

Es una forma simple de Encriptación Simétrica. XOR trabaja a nivel de bits, realizando una operación OR exclusivo entre el mensaje y la llave de encriptación. Para desencriptar el mensaje basta con aplicar una operación XOR entre el mensaje encriptado y la llave de encriptación.

SUSTITUCIÓN Y TRANPOSICIÓN

Son dos de los métodos más antiguos de encriptación. Básicamente, ambas formas de encriptación remplazan cada letra en un mensaje con una letra diferente. La diferencia está en como selecciona la letra a reemplazar.

Con un algoritmo de sustitución, es creada una tabla de sustitución, con letras insertadas aleatoria mente en la tabla tanto cada letra y número en el alfabeto, como cada carácter y símbolo imprimible, teniendo un sustituto (carácter o símbolo) que es usado en su lugar.

Con un algoritmo de transposición, es elegido un número aleatoria mente, y entonces cada letra es transpuesta arriba o abajo del alfabeto por ese número de caracteres. El mensaje resultante luce muy similar a un algoritmo de sustitución. Para desencriptar el mensaje, cada letra es transpuesta el mismo número de caracteres en la misma dirección.

STEGANOGRAFIA

La Steganografía es u tipo de encriptación en la que los mensajes son pasados en una forma que es irreconocible como un mensaje. En este tipo de encriptación, un mensaje es incrustado en algo más, como una imagen u otro mensaje. En una de las formas más antiguas de steganografía, un mensaje contiene un segundo mensaje secreto. En este caso, la primera letra de cada palabra de cada quinta letra u otro patrón de repetición es extraído del mensaje que hace de host para formar un segundo, mensaje secreto.

PROTECCIÓN DE UN TIEMPO

La protección de un tiempo es el único completamente seguro método de encriptación. Es básicamente un flujo de valores de llaves completamente aleatorio. Como cada carácter en el mensaje debe ser encriptado, el valor de la siguiente llave es usado para encriptar, por el método mod-26 o vía XOR con significados electrónicos. Luego que una llave ha sido utilizada, es desechada y nunca más usada.

INFRAESTRUCTURA DE LLAVE PUBLICA (PKI)

PKI

La infraestructura de llave Pública es usada por aplicaciones y para aplicaciones de negocios. Se considera que dichas aplicaciones pueden pertenecer a los siguientes tipos de entornos:

- Cliente a Negocio
- Negocio a Negocio
- Empleado a Negocio

Cliente a Negocio:

Esto es cuando el Cliente usa Internet para interactuar con un negocio. El Acceso del cliente no solo se da para comprar algo. Por lo tanto vemos que existen muchas razones para que un cliente acceda a Internet. PKI[7] presenta una propuesta para autenticación concreta.

Negocio a Negocio:

Aquí es donde PKI puede relucir. Esto se verá cuando PKI permita conocer con quienes se está haciendo negocio, y obtener la información para realizar seguimiento y verificar transacciones. PKI puede ser muy útil además en el mundo móvil y de alto volumen transaccional del Comercio en Internet. Este provee control de administración de riesgos para los Sistemas de Negocios.

Empleado a Negocio:

PKI puede proveer un mecanismo de seguridad para transferir mensajes dentro y fuera de la organización. También existen las ventajas de de estar posibilitado de tener transacciones seguras y un acceso basado en certificados, por ejemplo configurando una Base de Datos central de Certificados (LDAP) y autenticación utilizando un origen autoritativo.

[7] PKI: Public Key Infrastructure

Componentes de PKI:

Los Componentes de PKI son los siguientes:

Autoridad Certificadora (CA):

El CA revisa, detalla, renueva y revoca certificados digitales. Un certificado incluye la llave pública o información acerca de la llave pública y puede inclusive ofrecer un directorio para al almacenar la llave pública.

El Sistema de Administración:

Existen varias implementaciones de PKI en el mercado. Muchas de ellas son empaquetadas en un servidor Web o son ofrecidas como paquetes stand alone. Las llaves son típicamente creadas simultáneamente usando el mismo algoritmo por una autoridad certificadora.

A continuación, se menciona algunas de las características asociadas al uso de PKI:

- Certificación
- Autenticación
- Validación y Expiración
- No Repudio

- Firmas Digitales
- Encriptación de Mensajes electrónicos

X.509

X.509 se basa en X.500. Este último constaba de un directorio de información, cuyos resultados podrían representar cualquier entidad de un Sistema, no solo personas, si no computadores, negocios, etc. Este X.500, podría recibir contener también el Certificado especificando la llave pública de la persona. Ambos (X.500 y X.509) fueron diseñados a mediados de 1980, antes de la aparición de Internet.

El Método de búsqueda que utiliza X.500 está basado en una propiedad llamada DN[8]. El DN debe ser único en el directorio y será ordenado utilizando una Metodología Jerárquica. Esta información jerárquica es almacenada en una Base de Información de Directorio (DIB). La DIB es similar a un árbol que se mira desde la parte superior, pero constituido de atributos.

Las características de un Certificado Digital X.509v2 son las siguientes:

[8] DN: Distinguished Name

Versión:

Este campo identifica que versión del estándar x.509 aplica al certificado.

Número de Serie:

Un número único asignado al certificado por su CA emisora. Esta información puede ser usada de diferentes maneras- por ejemplo, cuando un certificado es revocado, su número de serie es ubicado en una lista de revocación de certificados, o CRL.

Identificador de Algoritmo de Firma:

Este identifica el Algoritmo usado por la CA para firmar el certificado.

Nombre de Emisor:

Este es el nombre de la entidad que ha firmado el certificado. Típicamente es la CA.

Periodo de Validez:

Es el tiempo durante el cual el certificado es válido.

Nombre de Sujeto: El nombre del sujeto ve el estándar X.500, por lo tanto este es único en el directorio (DIB).

Llave pública:

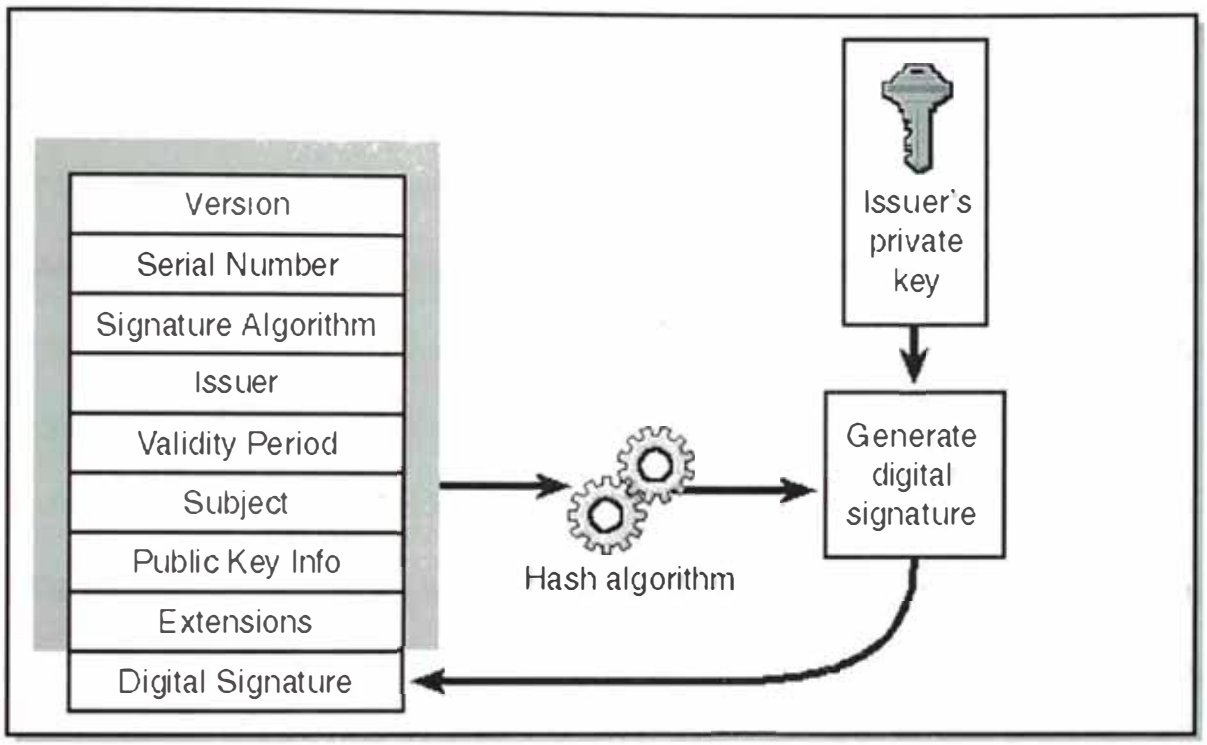
El valor de la llave pública asociado a un Algoritmo identificador, que especifica el Sistema de Criptografía de llave pública a la que la llave pertenece.

Identificador único de Emisor:

Este es un bit opcional que usado para hacer el nombre de la CA no ambiguo en el caso que se le reasigne una nueva entrada.

Identificador único de sujeto:

Este es un bit opcional usado como el campo descrito anteriormente pero con el sujeto.



INTEGRACION DE SISTEMAS EN INTERNET

FLUJO DE INFORMACION A TRAVÉS DE INTERNET

Se ha considerado que habiendo sido abordada la parte de infraestructura de Sistemas en un Smart Backbone [9], es cuando se debe considerar la Integración de Aplicaciones Empresariales interna y a externamente (Es decir con los socios de negocios).

[9] Smart Backbone: Arquitectura Inteligente

Las Aplicaciones, en particular las aplicaciones de misión crítica de las empresas son utilizadas para ejecutarse, como piezas de funcionalidades probadas en un Proceso complejo de desarrollo. A los más altos niveles, ellas realizan las funciones que representan que es lo que la organización hace en el sentido del negocio. Ellas representan la provisión de pedidos, cierre de órdenes de pedidos, etc.

Estas aplicaciones de negocio trabajan separadas en muchas empresas. Por ello, mientras existan aplicaciones separadas, van a existir pasos manuales que sirvan para integrar las aplicaciones existentes. Estos pasos introducen demoras y añaden costo al producto final o al servicio que provee una organización. Cualquier cosa que se haga para reemplazar la integración manual por la Coordinación Ínter procesos es como acelerar la compañía y reducir los gastos generales.

Llevando esta idea un paso más allá, las compañías representan pasos completos en el Proceso Completo. Por ello el intercambio de información debe ser seguro y las aplicaciones que generan dicha información también deben serlo. El Primer paso para esto es definir estándares de intercambio de información, que permitan uniformizar el lenguaje de comunicación en Internet.

DESARROLLO DE ESTÁNDARES DE INTERCAMBIO DE INFORMACIÓN

Actualmente existen una serie de estándares de intercambio de información. Los más conocidos son:

EDI (ELECTRONIC DATA INTERCHANGE)

EDI es un conjunto de estándares de mensajes usado para controlar la transferencia de documentos a través de medios electrónicos. Este viene en dos formas, ambas especifican listas largas de tipos de mensajes diseñados para facilitar el comercio electrónico entre negocios:

UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce and Transport)

Este es el estándar de intercambio de información desarrollado a través de las Naciones Unidas (ONU). Este estándar es comúnmente usado en Europa, como también en Japón y otras regiones y países asiáticos.

```
ISA~00~          ~00~          ~01~0123456789     ~01~081466849
~000829~0613~U~00300~000009056~0~P~>
GS~PO~0123456789~MAXCIM~20000829~0613~8427~X~004010
ST~850~084270001
BEG~00~LB~30-60425-D000829~~20000829
CUR~BT~USD
ITD~01~3~~~~~30~~~~~TERMS NET 030
N1~DU~FABRIKAM,INC
N3~ATTN: ACCOUNTS PAYABLE~457 ACCOUNTANT LN
N4~ANYTOWN~PA~195530403~US
N1~EN~SOME OTHER COMPANY
N3~ONE SOME COMPANY DRIVE
N4~SMALL TOWN~IL~60047~US
REF~AH~20818160ZZS2640
PER~IC~JOE CONTACT
N1~ST~FABRIKAM, INC~91~25
N3~*** OPEN LICENSE PACK ORDER ***~5007 SOME STATE COLLEGE
N4~ANYWHERE~CA~928315335~US
PO1~000001~1~EA~533.2~~MG~063-00331~BP~522561
PID~F~~~~MOL-5.0 WIN NT SVR TRMNL 4.0   VLICBUSINESS 5.0
PO1~000002~100~EA~71.79~~MG~A02-00124~BP~522567
PID~F~~~~MOL-5.0 WIN NT SVR TERMINAL CALVLIC4.0 BUSINESS 5.0
CTT~2~101
AMT~TT~7712.2
SE~22~084270001
GE~1~8427
IEA~1~000009056
```

ANSI X12

Este es el estándar de intercambio de información desarrollado por el Comité acreditado de estándares X12, cuyo trabajo es aprobado por ANSI (American National Standards Institute)

```
ISA*00*            *00*            *AA*02                  *01*A01
*001231*0310*U*00400*000004044*0*P*>~GS*AG*581529575*STFM
SF00014*20001231*0310*4044*X*4010~ST*997*0001~AK1*PO*711~AK2*850*
1054~AK5*A~AK9*A*1*1*1~SE*6*0001~GE*1*4044~IEA*1*000004044~
```

XML

Está basado en el SGML[10] que fue definido por la ISO[11] como el estándar ISO 8879. SGML ha sido utilizado desde entonces por varios sectores industriales en diferentes formatos, uno de los cuales es el HTML. Una gran desventaja es su complejidad por lo que se creó el XML. Este es un subconjunto del SGML simplificándolo, reteniendo los puntos fuertes de del SGML pero simplificándolo.

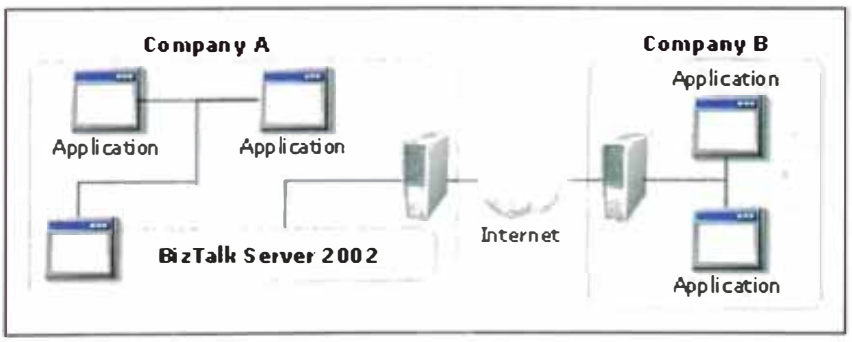
El uso de estos estándares es masivo. Sin embargo, la tendencia mundial ha sido la de sesgarse a este último (XML), debido a su simplicidad y estructura.

[10] SGML: Standard Generalized Markup Language
[11] ISO: International Organization for Standardization

```
<?xml version="1.0" encoding="utf-16" ?>
- <!--
 Generated by using BizTalk Editor on Mon, Oct 02 2000 11:36:14 PM
  -->
- <!--
 Microsoft Corporation (c) 2000 (http://www.microsoft.com)
  -->
- <Schema name="X12_4010_850" b:BizTalkServerEditorTool_Version="1.0"
b:root_reference="X12_4010_850" b:schema_type="850" b:version="1.0"
b:is_envelope="no" b:standard="X12" b:standards_version="4010"
xmlns="urn:schemas-microsoft-com:xml-data"
xmlns:b="urn:schemas-microsoft-com:BizTalkServer"
xmlns:d="urn:schemas-microsoft-com:datatypes">
  <b:SelectionFields />
- <ElementType name="X12_4010_850" content="eltOnly" model="closed">
  <description>Purchase Order</description>
    <b:RecordInfo structure="delimited" delimiter_type="inherit_record"
field_order="postfix" count_ignore="yes" />
  <element type="BEG" maxOccurs="1" minOccurs="1" />
  <element type="CUR" maxOccurs="1" minOccurs="0" />
  <element type="ITD" maxOccurs="*" minOccurs="0" />
  <element type="N1Loop1" maxOccurs="*" minOccurs="0" />
  <element type="PO1Loop1" maxOccurs="*" minOccurs="1" />
  <element type="CTTLoop1" maxOccurs="1" minOccurs="0" />
  </ElementType>
+ <ElementType name="REF_3" content="eltOnly" model="closed">
+ <ElementType name="PO1Loop1" content="eltOnly" model="closed">
+ <ElementType name="PO1" content="empty" model="closed">
+ <ElementType name="PID_2" content="empty" model="closed">
+ <ElementType name="PIDLoop1" content="eltOnly" model="closed">
+ <ElementType name="PER_2" content="empty" model="closed">
+ <ElementType name="N4" content="empty" model="closed">
+ <ElementType name="N3" content="empty" model="closed">
+ <ElementType name="N1Loop1" content="eltOnly" model="closed">
+ <ElementType name="N1" content="empty" model="closed">
+ <ElementType name="ITD" content="empty" model="closed">
+ <ElementType name="CUR" content="empty" model="closed">
+ <ElementType name="CTTLoop1" content="eltOnly" model="closed">
+ <ElementType name="CTT" content="empty" model="closed">
+ <ElementType name="C040_4" content="empty" model="closed">
+ <ElementType name="BEG" content="empty" model="closed">
+ <ElementType name="AMT_3" content="empty" model="closed">
  </Schema>
```

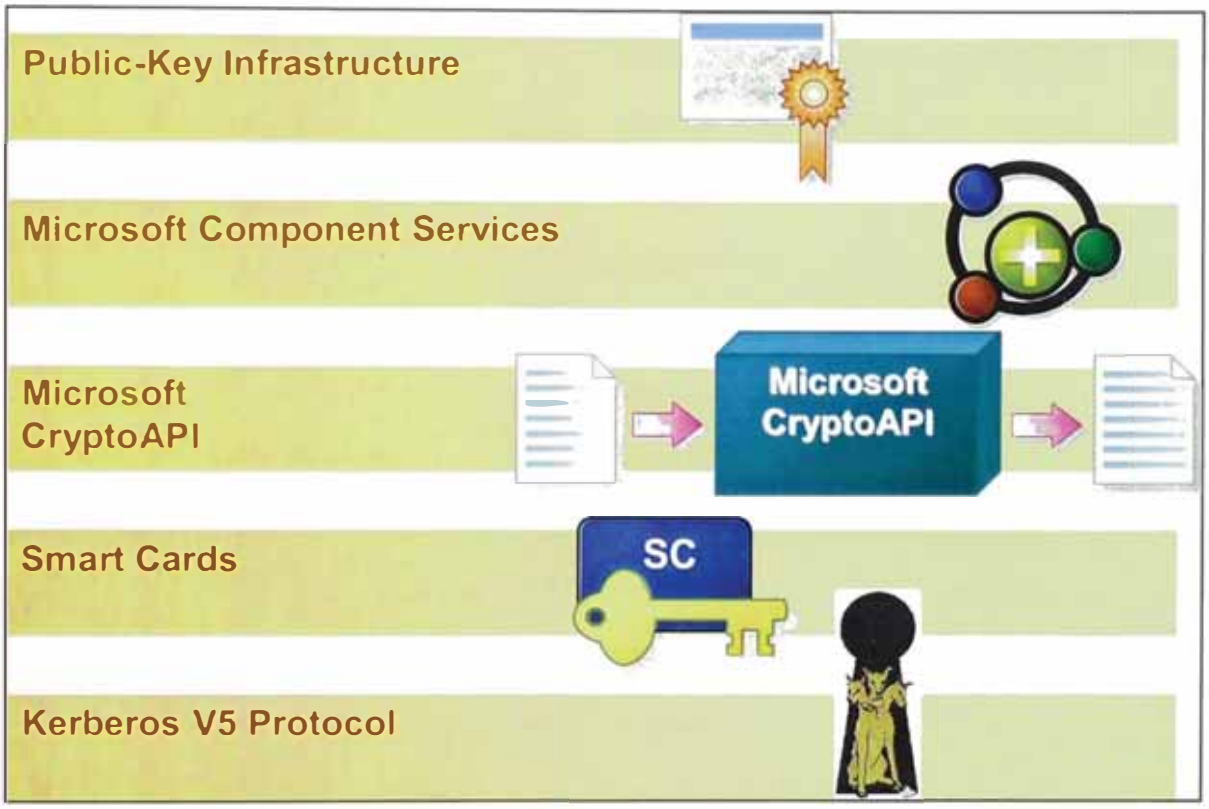
INTERCAMBIO DE INFORMACION SEGURO: INTEGRACION DE PROCESOS EMPRESARIALES A TRAVES DE INTERNET

El Intercambio seguro de información entre nuestra organización y otras organizaciones debe estar garantizado por los métodos descritos anteriormente. Para el intercambio de información, consideraremos como base Tecnología Microsoft, sobre la que se ha desarrollado un producto de Integración llamado MS BizTalk Server 2002 que contribuye a implementar nuestro esquema de integración segura entre empresas a través de Internet, bajo el siguiente esquema:



Por ejemplo, según el gráfico anterior tenemos dos compañías. La compañía A y B, poseen aplicaciones de Sistemas. BizTalk Server 2002 posibilita la integración de las aplicaciones de Sistemas de la compañía A con las de la compañía B, de una manera confiable, segura y de bajo costo.

BizTalk Server 2002 posee cinco niveles de seguridad para integrar el intercambio de información entre aplicaciones empresariales:



Cada uno de los niveles de seguridad pueden ser especificados a continuación en un paralelo con la funcionalidad que realizan:

Característica de Seguridad	**Usado para asegurar**	**Punto de Configuración**	**Herramienta de Configuración**
PKI	Documentos (Firma o encriptación)	Puertos y Canales	BizTalk Messaging Manager
Microsoft Component Services	Componentes COM+	Component Services\Computer\My Computer	Component Services

CryptoApi	Datos BizTalk Server 2002	Puertos y Canales Component Services\Computer\My Computer Redes privadas virtuales (VPN), dial-up, Propiedades de conexión de Redes de Area Local (LAN) Colas de Mensajes	BizTalk Messaging Manager Component Services Network and dial-up connections
Smart Cards	Característica de autenticación de redes basada en certificados que usa Extensible Application Protocol	Redes Privadas Virtuales Dial-up Propiedades de conexión de Redes de Area Local (LAN)	Network and dial-up connections
Kerberos V5 Protocol	Mensajes	Colas de Mensajes	BizTalk Messaging Manager

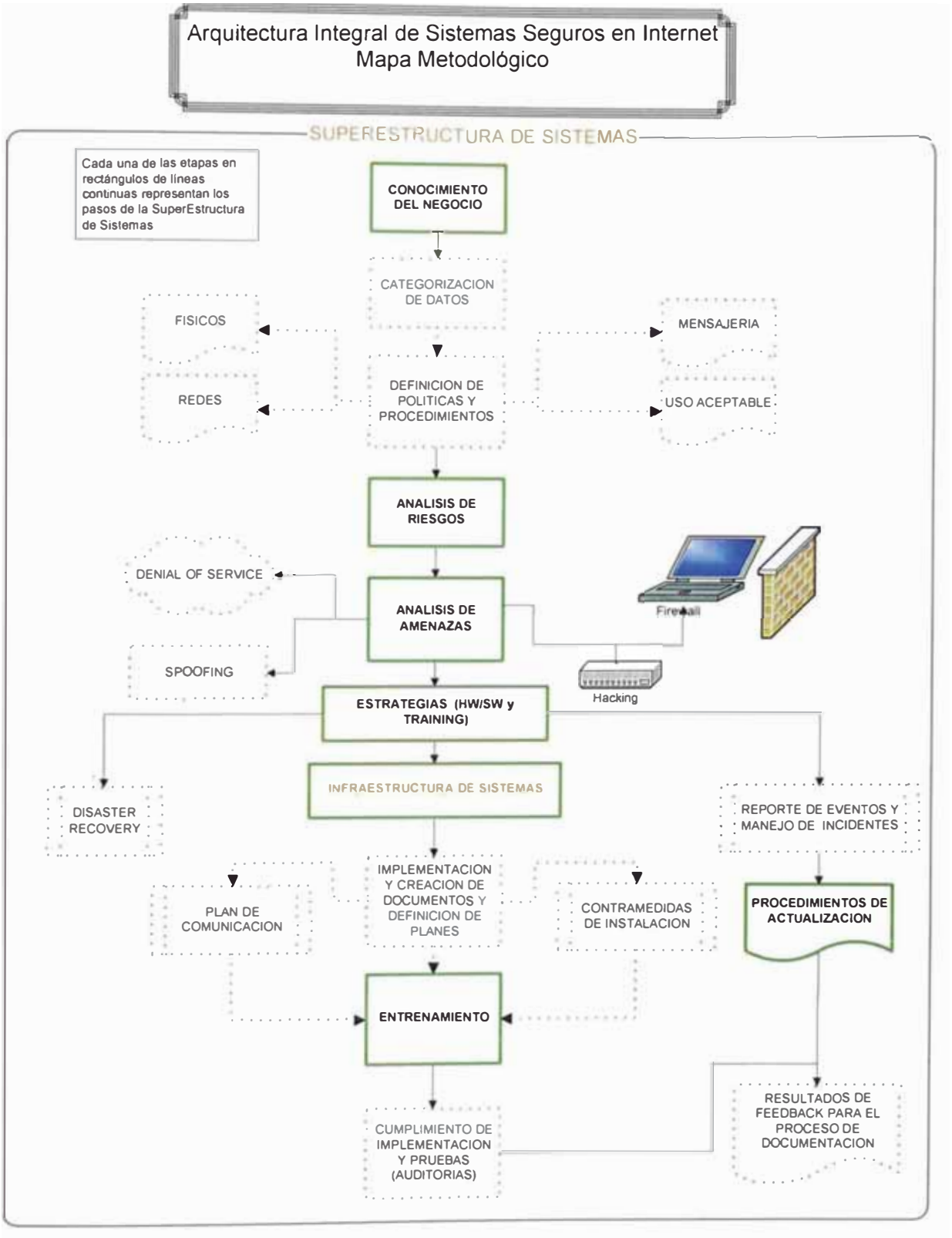
Por ejemplo, para proteger el intercambio de información, en el siguiente diagrama se muestra como los medios internos de mensajería que utiliza BizTalk para enlazar Sistemas puede contener certificados firmados y transmitir información encriptada a través de Internet e Intranet.

Implementación de Esquema de Seguridad BizTalk Server 2002

CAPITULO IV

CONSOLIDACION DE PASOS

Arquitectura Integral de Sistemas Seguros en Internet
Mapa Metodológico



CAPITULO V

IMPLEMENTACION DEL MODELO PROPUESTO

CASO PRACTICO: PROYECTO DE INTEGRACIÓN SEGURA DE SISTEMAS ENTRE COMPRADOR Y PROVEEDORES A TRAVÉS DE INTERNET: "PROYECTO ANTARES"

COMPAÑÍA A (COMPRADORA):

La Compañía A no posee una arquitectura tecnológica preparada para publicar aplicaciones en Internet e intercambiar información de negocios. Sin embargo, la Junta de Directorio ha decidido:

1. **Primera Fase:** Implementar una Arquitectura Integral que les permita integrarse electrónicamente con sus socios de negocios y así romper con sus barreras organizacionales, para así ser más competitivos en el mercado.

2. **Segunda Fase:** Implementar una Solución de Compras Corporativas a Proveedores a través de Internet, pues se ha detectado que existen problemas críticos en las áreas de compras y logística para la compra de sus bienes del negocio, tales como computadoras, útiles de oficina, herramientas, e inclusive insumos de producción.

COMPAÑÍA B (PROVEEDORA):

La Compañía Proveedora posee una arquitectura preparada para publicar aplicaciones en Internet y con una arquitectura básica de seguridad. El interés de ellos es poder procesar localmente por medio de sus Sistemas la atención de pedidos, el mantenimiento de catálogos y otras funciones que les permitirían interactuar de una manera más rápida con su cliente comprador, la compañía A.

DESCRIPCIÓN DE LA SOLUCIÓN

Los Objetivos que busca cumplir el Proyecto Antares son los siguientes:

Crear una organización Funcionalmente segura.

Crear un entorno seguro en la Compañía a nivel de procesos funcionales y tecnológicos

Crear una organización Tecnológicamente segura.

Crear una arquitectura tecnológica capaz de soportar los ataques de agentes tecnológicos externos, mediante el empleo sistemático de reglas de protección basado en software y hardware.

Habilitar la Integración Segura de Sistemas a través de Internet.

Mediante el empleo de Middleware de integración de aplicaciones que posibiliten el intercambio seguro de información.

Asimismo, para la segunda etapa, se considera que siendo el propósito principal habilitar un Sistema de Compras Corporativas en Internet entre la Compañía Compradora A y la Proveedora B, os Siguientes criterios serán utilizado para medir si el proyecto ha sido o no satisfactorio:

Habilitar las compras seguras por Internet.

El Proyecto debe habilitar el cliente para realizar las compras seguras a proveedores socios de negocios por Internet. Esto debería poner fin o por lo menos reducir, gastos independientes.

Reducir los costos de compra.

Los Costos de Compras deben ser reducidos, mediante la reducción de gastos administrativos generales en un 50%.

Aumentar la velocidad de las transacciones.

El Tiempo de compra de ítems, tales como útiles de oficina etc. debe decrecer. El período objetivo de orden a entrega, se va a delimitar regionalmente. Naturalmente, el tiempo de respuesta no solo depende de la administración interna, también los proveedores. Por ello, se debe medir la ganancia total de ambos en términos absolutos (i.e., El Panorama total) como también las ganancias en procesos controlados por la Compañía A (administración, instalación de bienes, etc.).

Facilidad de uso para los empleados.

Las interfaces de usuario deben ser sumamente intuitivas.

Fácil despliegue en la totalidad de la empresa y las unidades operacionales.

Solución de bajo costo.

El proyecto debe ser más bajo en costos que las alternativas de productos elaborados.

Para el cumplimiento de los objetivos de la solución de seguridad integral se siguieron los pasos del presente trabajo de tesis.

En ambas compañías se formaron dos equipos: Comités de Seguridad y Equipos de Respuesta de Incidentes. En ambos casos, la responsabilidad de la solución tecnológica fue designada a las respectivas áreas de Tecnologías de Información de ambas compañías.

La Distribución de los equipos fue la siguiente:

Comité de Seguridad	**Equipo de Respuestas de Incidentes**
Gerente General	Área de Tecnologías de Información
Gerente de Operaciones	Area de Administración
Jefe de Seguridad de Información	Área de Riesgos
Jefes de Cada Área Funcional	
Jefe de Recursos Humanos	
Jefe de Área de Tecnologías de Información	
Analista de Proyectos de Área de Tecnologías	

de Información Representante de División Legal Miembro del Equipo de Respuestas a Incidentes	

El Comité de Seguridad se encargó de desarrollar un Plan que reflejó cada etapa descrita en el presente trabajo, es así que se entregaron los siguientes documentos:

Conocimiento del negocio	Documento de políticas de seguridad corporativa
Análisis de riesgos	Plantilla de revisión de seguridad tecnológica
	Tabla de riesgos de entorno
Identificación de amenazas	Tabla de funciones del negocio
	Listado de amenazas
Desarrollo de estrategias	Listado de estrategias por puntos críticos
Entrenamiento	Plan de capacitación de seguridad
Mantenimiento de procesos actualizados	Plan de actualización de procesos

El Cronograma de la Primera Etapa del Proyecto fue el siguiente:

ID	Task Name	Duration	Start	Finish
1	**Proyecto de Seguridad Etapa Inicial "Antares"**	**101 days**	**Fri 03/08/01**	**Fri 21/12/01**
2	**Visión Alcance**	**11 days**	**Fri 03/08/01**	**Fri 17/08/01**
3	Formación de un Equipo de Seguridad	3 days	Fri 03/08/01	Tue 07/08/01
4	Evaluación de Infraestructura de seguridad	4 days	Wed 08/08/01	Mon 13/08/01
5	Priorización y Análisis de Riesgos	4 days	Tue 14/08/01	Fri 17/08/01
6	Alcance de Proyecto Completado	0 days	Fri 17/08/01	Fri 17/08/01
7	**Planeamiento**	**20 days**	**Mon 20/08/01**	**Fri 14/09/01**
8	**Plan de Revisión del Negocio**	**6 days**	**Mon 20/08/01**	**Mon 27/08/01**
9	Borrador de Políticas de Seguridad Organizacional	3 days	Mon 20/08/01	Wed 22/08/01
10	Operaciones y Documentación de usuario final	3 days	Thu 23/08/01	Mon 27/08/01
11	**Plan de Infraestructura de Sistemas**	**9 days**	**Tue 28/08/01**	**Fri 07/09/01**
12	Diseño de Estandares de Seguridad	5 days	Tue 28/08/01	Mon 03/09/01
13	Estrategias de Migración y Coexistencia	4 days	Tue 04/09/01	Fri 07/09/01
14	Plan de Aseguramiento de Calidad y Pruebas	5 days	Mon 10/09/01	Fri 14/09/01
15	Plan de Implementación	0 days	Fri 14/09/01	Fri 14/09/01
16	**Desarrollo**	**59 days**	**Mon 17/09/01**	**Thu 06/12/01**
17	Desarrollo de Capacitación y Conocimiento de Medidas	8 days	Mon 17/09/01	Wed 26/09/01
18	**Implementación de Infraestructura de Sistemas**	**29 days**	**Mon 17/09/01**	**Thu 25/10/01**
19	**Implementación de Arquitectura Física**	**7 days**	**Mon 17/09/01**	**Tue 25/09/01**
	Autenticación	**2 days**	**Mon 17/09/01**	**Tue 18/09/01**
	Actividades preliminares	**1 day**	**Mon 17/09/01**	**Mon 17/09/01**
22	Preparación del Servidor ACE	1 day	Mon 17/09/01	Mon 17/09/01
23	Preparación del Servidor backup del ACE (Opcional)	1 day	Mon 17/09/01	Mon 17/09/01
24	**Instalación de servidores ACE**	**2 days**	**Mon 17/09/01**	**Tue 18/09/01**
25	Instalación y configuración del ACE Server	1 day	Mon 17/09/01	Mon 17/09/01
26	Instalación y configuración del ACE Server backup	2 days	Mon 17/09/01	Tue 18/09/01
27	Pruebas de la instalación	1 day	Mon 17/09/01	Mon 17/09/01
28	**Instalación del cliente ACE**	**1 day**	**Mon 17/09/01**	**Mon 17/09/01**
29	Instalación de los clientes para la aplicación	1 day	Mon 17/09/01	Mon 17/09/01
30	Pruebas de la instalación	1 day	Mon 17/09/01	Mon 17/09/01
31	**Configuración de Tokens**	**2 days**	**Mon 17/09/01**	**Tue 18/09/01**
32	Carga y configuración de los tokens de los usuarios en e	1 day	Mon 17/09/01	Mon 17/09/01
33	Pruebas	2 days	Mon 17/09/01	Tue 18/09/01
34	**Monitoreo**	**0.25 days**	**Mon 17/09/01**	**Mon 17/09/01**
35	Instalación de la consola de administración	0.25 days	Mon 17/09/01	Mon 17/09/01
36	Instalación del RealSecure Network Sensor	0.25 days	Mon 17/09/01	Mon 17/09/01
37	Instalación del RealSecure Server Sensor	0.25 days	Mon 17/09/01	Mon 17/09/01
38	**Instalación de SMTP Relay**	**4 days**	**Mon 17/09/01**	**Thu 20/09/01**
39	Inspección física de los equipos	1 day	Mon 17/09/01	Mon 17/09/01
40	Instalación del sistema operativo	1 day	Tue 18/09/01	Tue 18/09/01
41	Instalación del Relay	0.5 days	Wed 19/09/01	Wed 19/09/01
42	Pruebas de esfuerzo	1 day	Wed 19/09/01	Thu 20/09/01
43	Instalación de Norton for Firewall	0.5 days	Thu 20/09/01	Thu 20/09/01
44	**Instalación y configuración del firewalls**	**7 days**	**Mon 17/09/01**	**Tue 25/09/01**
45	Inspección física de los equipos	0.5 days	Mon 17/09/01	Mon 17/09/01
46	Instalación del sistema operativo	1 day	Mon 17/09/01	Tue 18/09/01
47	Instalación de la aplicación del Firewall-1 de CheckPoint	1 day	Tue 18/09/01	Wed 19/09/01
48	Configuración de la solución de Alta Disponibilidad (Stone Bea	2 days	Wed 19/09/01	Fri 21/09/01
49	Instalación del WebTrends for firewall	0.5 days	Fri 21/09/01	Fri 21/09/01
50	Modificación de la arquitectura de red	1 day	Mon 24/09/01	Mon 24/09/01
51	Pruebas de conectividad	1 day	Tue 25/09/01	Tue 25/09/01
52	**Security Lock-up**	**12 days**	**Wed 26/09/01**	**Thu 11/10/01**
53	Análisis de aplicativos	5 days	Wed 26/09/01	Tue 02/10/01
54	Análisis de reinstalación de Servidores en Pruebas	3 days	Wed 03/10/01	Fri 05/10/01
55	Server lockups (Pruebas)	4 days	Mon 08/10/01	Thu 11/10/01
56	**Publicación de Sistemas de Seguridad**	**10 days**	**Fri 12/10/01**	**Thu 25/10/01**
57	Definición de políticas de publicación (Aproval pending)	4 days	Fri 12/10/01	Wed 17/10/01
58	Pruebas con servidores abiertos y políticas	3 days	Thu 18/10/01	Mon 22/10/01
59	Pruebas a través de Firewall con servidores asegurados	3 days	Tue 23/10/01	Thu 25/10/01
60	Implantación en servidor asegurado y pre producción	0 days	Thu 25/10/01	Thu 25/10/01
61	**Implementación de Superestructura de Sistemas**	**22 days**	**Fri 26/10/01**	**Mon 26/11/01**
62	Ejecución de Capacitación y Conocimiento de Medidas	7 days	Fri 26/10/01	Mon 05/11/01
63	Estándares de Seguridad Implementados	6 days	Tue 06/11/01	Tue 13/11/01
64	Transición a Gestión de Operaciones	4 days	Wed 14/11/01	Mon 19/11/01
65	**Revisión de Seguridad con StakeHolders**	**1 day**	**Tue 20/11/01**	**Tue 20/11/01**
70	Documento de Políticas de Seguridad Corporativas	4 days	Wed 21/11/01	Mon 26/11/01
71	Entrega de DPSC	0 days	Mon 26/11/01	Mon 26/11/01
72	Establecimiento de Ambiente de Pruebas	3 days	Tue 27/11/01	Thu 29/11/01
73	Pruebas de Pre Producción	5 days	Fri 30/11/01	Thu 06/12/01
74	Evaluación de Implementación	0 days	Thu 06/12/01	Thu 06/12/01
75	**Estabilización**	**11 days**	**Fri 07/12/01**	**Fri 21/12/01**
76	**Pase a Producción y Pruebas Finales**	**11 days**	**Fri 07/12/01**	**Fri 21/12/01**
77	Proveer Entorno de Producción	4 days	Fri 07/12/01	Wed 12/12/01
78	Pase a Producción	7 days	Thu 13/12/01	Fri 21/12/01
79	Milestone. Solución Completa	0 days	Fri 21/12/01	Fri 21/12/01

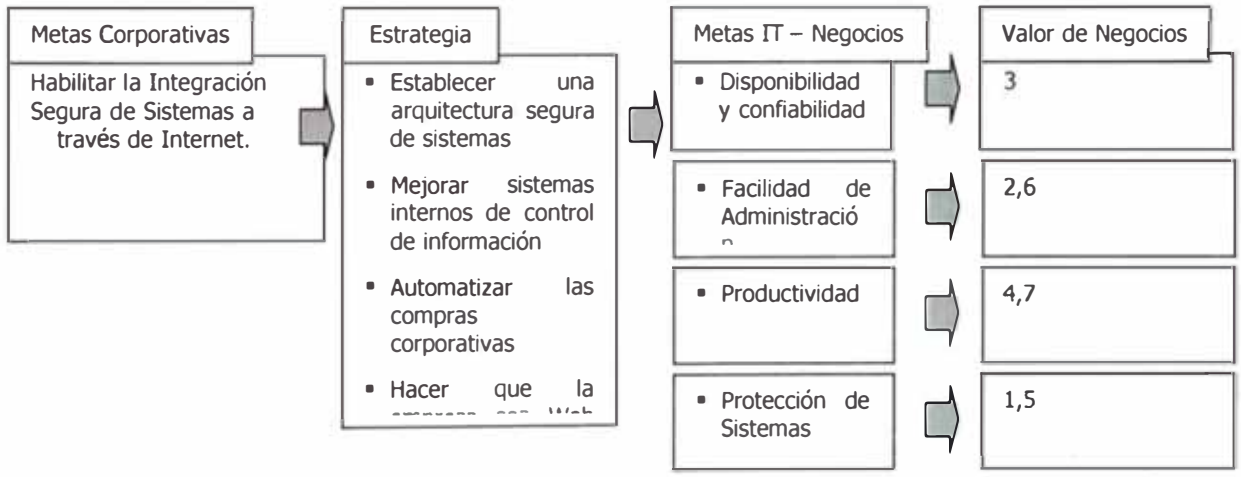
El Cronograma de la Segunda Etapa del Proyecto fue el siguiente:

ID	Task Name	Duration	Start	Finish
1	**Proyecto de Compras Seguras Segunda Etapa "Antares"**	**109.5 days**	**Thu 20/09/01**	**Wed 20/02/02**
2	**Vision**	**10 days**	**Thu 20/09/01**	**Wed 03/10/01**
3	BizTalk Training para los miembros del equipo	5 days	Thu 20/09/01	Wed 26/09/01
4	Kickoff Vision/Alcance	0 days	Wed 26/09/01	Wed 26/09/01
5	Preparación de la Visión-Alcance	4 days	Thu 27/09/01	Tue 02/10/01
6	Preparación de Oferta	1 day	Wed 03/10/01	Wed 03/10/01
7	Milestone: Vision&Alcance	0 days	Wed 03/10/01	Wed 03/10/01
8	**Planeamiento**	**7 days**	**Thu 04/10/01**	**Fri 12/10/01**
9	**Diseño y Arquitectura**	**7 days**	**Thu 04/10/01**	**Fri 12/10/01**
10	Análisis de Procesos del Negocio	2 days	Thu 04/10/01	Fri 05/10/01
11	Análisis de Flujo de Datos	1 day	Mon 08/10/01	Mon 08/10/01
12	Arquitectura Lógica	1 day	Tue 09/10/01	Tue 09/10/01
13	Arquitectura Física (Por cada grupo de servidores BizTalk)	1 day	Wed 10/10/01	Wed 10/10/01
14	Planeamiento de Infraestructura	0.5 days	Thu 11/10/01	Thu 11/10/01
15	Concepto de Seguridad	0.5 days	Thu 11/10/01	Thu 11/10/01
16	Operaciones Administrativas y Planeamiento de Despliegue	1 day	Fri 12/10/01	Fri 12/10/01
17	Milestone: Diseño Completo	0 days	Fri 12/10/01	Fri 12/10/01
18	**Administración del Programa**	**2 days**	**Thu 04/10/01**	**Fri 05/10/01**
19	Administración de Proveedores	1 day	Thu 04/10/01	Thu 04/10/01
20	Análisis de Riesgos	1 day	Thu 04/10/01	Thu 04/10/01
21	Aseguramiento de Calidad y Plan de Pruebas	1 day	Thu 04/10/01	Thu 04/10/01
22	Planeamiento del Proyecto	2 days	Thu 04/10/01	Fri 05/10/01
23	Milestone: Planeamiento	0 days	Fri 05/10/01	Fri 05/10/01
24	**Desarrollo**	**79 days**	**Mon 15/10/01**	**Thu 31/01/02**
25	Proveer el entorno de desarrollo	2 days	Mon 15/10/01	Tue 16/10/01
26	**Desarrollo de Site de eProcurement**	**51.5 days**	**Wed 17/10/01**	**Thu 27/12/01**
27	Desarrollo de Módulo Employee (Commerce Server 2000)	15 days	Wed 17/10/01	Tue 06/11/01
28	Desarrollo de Módulo de Facturación (Manager)	15 days	Wed 07/11/01	Tue 04/12/01
29	Desarrollo de Módulo Manager (Commerce Server 2000)	12 days	Thu 01/11/01	Mon 10/12/01
30	Desarrollo del Módulo Supplier (Intranet)	10 days	Mon 12/11/01	Tue 11/12/01
31	Desarrollo del Módulo Administrador (Commerce Server 2000)	20 days	Thu 29/11/01	Thu 27/12/01
32	**Integración de Suppliers (Por cada clase de Partner)**	**27.5 days**	**Thu 06/12/01**	**Mon 14/01/02**
33	Documentación de Interfaces de Trading Partners	1 day	Thu 06/12/01	Fri 28/12/01
34	Desarrollo de Documentos y Envelopes XML	10 days	Thu 27/12/01	Thu 10/01/02
35	Pruebas unitarias de integración con Trading Partners	2 days	Thu 10/01/02	Mon 14/01/02
36	Despliegue sobre entorno de desarrollo	0.5 days	Mon 14/01/02	Mon 14/01/02
37	**Implementación de Componentes del Negocio**	**6 days**	**Mon 15/10/01**	**Mon 22/10/01**
38	Implementación de Concepto Administrativo	6 days	Mon 15/10/01	Mon 22/10/01
39	Implementación de Concepto Operacional	2 days	Mon 15/10/01	Tue 16/10/01
40	Documentación	4 days	Mon 15/10/01	Thu 18/10/01
41	**Implementación de Procesos del Negocio**	**8 days**	**Tue 15/01/02**	**Thu 24/01/02**
42	Implementación de mapeos	2.5 days	Tue 15/01/02	Thu 17/01/02
43	Implementación de Configuración de BizTalk Server	2.5 days	Tue 15/01/02	Thu 17/01/02
44	Implementación de schedules y componentes XLANG	5 days	Tue 15/01/02	Mon 21/01/02
45	Documentación de Implementación de Procesos del negocio	3 days	Tue 22/01/02	Thu 24/01/02
46	**Implementación de Seguridad en la Solución**	**5 days**	**Fri 25/01/02**	**Thu 31/01/02**
47	Implementación de Seguridad en Componentes de Software	2 days	Fri 25/01/02	Mon 28/01/02
48	Implementación de Cambios por Adición de SSL	3 days	Tue 29/01/02	Thu 31/01/02
49	Milestone: Código Completo	0 days	Thu 24/01/02	Thu 24/01/02
50	**Estabilización**	**13.5 days**	**Fri 01/02/02**	**Wed 20/02/02**
51	**Implementación en Entorno de Integración**	**5 days**	**Fri 01/02/02**	**Thu 07/02/02**
52	Proveer entorno de Integración	1 day	Fri 01/02/02	Fri 01/02/02
53	Implementación de Solución Biztalk sobre entorno de Integración	4 days	Mon 04/02/02	Thu 07/02/02
54	**Pruebas de Integración y Corrección de Bugs**	**4.5 days**	**Fri 08/02/02**	**Thu 14/02/02**
55	Descripción de casos de Pruebas para escenario de integración	0.5 days	Fri 08/02/02	Fri 08/02/02
56	Realización de Pruebas Funcionales	1 day	Fri 08/02/02	Mon 11/02/02
57	Realización de Pruebas de Esfuerzo	1 day	Fri 08/02/02	Mon 11/02/02
58	Implementación y Corrección de bugs de Solución Biztalk mejorada	3 days	Mon 11/02/02	Thu 14/02/02
59	**Pase a Producción y Pruebas Finales**	**4 days**	**Thu 14/02/02**	**Wed 20/02/02**
60	Proveer Entorno de Producción	2 days	Thu 14/02/02	Mon 18/02/02
61	Pase a Producción	2 days	Mon 18/02/02	Wed 20/02/02
62	Milestone: Solución Completa	0 days	Wed 20/02/02	Wed 20/02/02

ANÁLISIS COSTO / BENEFICIO

Valor de Negocios

A continuación se muestran los beneficios que se anticiparon sobre la implementación de la solución de seguridad y de compras corporativas para la **COMPAÑÍA A**



A continuación se muestran las mejoras tecnológicas y funcionales anticipadas de la solución de acuerdo al planteamiento del proyecto:

Referencia	Mejora Anticipada	Tipo de Mejora	Enunciado de Valor	Beneficio Anual (US$)	Mejora x usuario anual
1	Reducción de costos en el COMPAÑÍA A debido a las mejores prácticas habilitadas para la protección de información.	Tecnológica Tangible / Cuantificable	Manejando el modelo de *Total Cost of Ownership* de GartnerGroup, las mejores prácticas aplicadas tendrán una reducción en los costos de Sistemas	$187,347.-	$1247.-
2	Reducción de horas hombre dedicadas a soporte reactivo	Tecnológica Tangible / Cuantificable	Las características de administración de la solución permiten reducir el número de horas de soporte reactivo	$12,528.-	$400.06
3	Incremento en disponibilidad de Solución de Compras Corporativas	Negocios Intangible / Cuantificable	Las características de confiabilidad de la solución, disminuirán la posibilidad de que la aplicación de compras Electrónicas sufra periodos de downtime en horas criticas	$159,305.-	$90.35
4	Incremento en disponibilidad de tiempo del usuario final de compras de la compañía A	Negocios Intangible / Cuantificable	Al sufrir menos downtimes en el escritorio, COMPAÑÍA A dispondrá un número mayor de horas de usuario final de disponibilidad	$1'146,000.-	$366.-
5	Manejo eficiente del ancho de banda de la red corporativa	Tecnologia Intangible / Incuantificable	Por medio de QoS es posible aumentar la disponibilidad interna de los sistemas corporativos críticos	N/D	N/D
6	Administración Centralizada de la red corporativa de COMPAÑÍA A, incluyendo la habilitación de estándares centrales	Tecnologia Intangible / Incuantificable	Active Directory permitirá reducir las horas empleado que se ocupan en el manejo reactivo de TI	N/D	N/D
7	Incremento del tiempo usado para la definición de nuevas tareas de valor para el COMPAÑÍA A	Negocios Intangible / Incuantificable	Liberando recursos de la administración día a día, los elementos de TI podrán dedicar más tiempo a generar sistemas de valor para A.	N/D	N/D
8	Disminución de tiempos para el desarrollo de nuevas aplicaciones en plataforma Microsoft	Tecnologia Intangible / Incuantificable	El uso de BizTalk y COM+ como plataforma de desarrollo, permitirá a COMPAÑÍA A la reutilización de componentes y el manejo de nuevas aplicaciones más rápidamente	N/D	N/D

Validación de Beneficios

Mejora Anticipada	Enunciado de Valor	Medida	Explicación	Fórmula	Beneficio Anual (US$)
Mejor Total Cost of Ownership	Las mejores prácticas que se habilitan la implementación de la solución, permiten a la COMPAÑÍA A, el reducir sensiblemente su TCO.	Actualmente su TCO es de US$6199 72 La reducción estimada es a US$5,289 11	Total Cost of Ownership	Mejores Prácticas de GartnerGroup	6,877.00
Administración Centralizada	La Distribución de Infraestructura permitirá reducir las horas empleado que se ocupan en el manejo reactivo	Actualmente se utilizan aprox. 12,800 hrs. hombre en la COMPAÑÍA A. Se espera reducir a 800 (Multiplicado x US$5.41)	La forma de trabajo actual de COMPAÑÍA A, es básicamente una forma de trabajo reactiva, esto es, (1) No se determinan los problemas sino hasta que ocurren y (2) Hay que trasladar físicamente a los elementos para resolverlos. El salario de US$5.41 x Hora es el sueldo estimado del Staff de COMPAÑÍA A en promedio, incluyendo prestaciones, capacitación, etc.	=Horashombre anteriores (12800) - Horashombre nvas (800) * US$5.41	12,528.00
Sistemas críticos con un incremento en disponibilidad	El incremento en disponibilidad que tendrá el Sistema de Compras evitará pérdidas por downtime del sistema	Mantener el sistema con un máximo de 8.76 hrs. anuales de downtime, de un 438 que se tiene actualmente. La hora de downtime se estima en US$1,281[3].-	La Plataforma propone brindar una disponibilidad segura de los sistemas hasta 99.9%, lo cual implica una reducción en horas de downtime hasta aprox. 9 horas anuales. Este decremento se multiplica por la estimación de hora de downtime que se genera en la Solución de Compras. Este downtime es calculado en *Promedio de hora de downtime por transacción de compra*	=Horasdedowntimehoy(438)*Costodedowntime($1,281) - Horasdedowntimeestimados(8.76)* Costodedowntime(US$1,281)	259,305.00

Incremento en productividad de usuario final por incremento en disponibilidad	El usuario interno cuenta con más tiempo de trabajo, ya que sus aplicaciones están disponibles más tiempo	Mantener los desktops con 95% de disponibilidad vs un 90% actual x US$5	Basado en las cifra de *Cálculo estimado de sueldos* y la disponibilidad que se propone alcanzar al implementar la solución hasta el desktop del usuario final, se estima el ahorro en: Diferencia de horas de uptime * US$7.07	=Usuarios (230)*SalarioPromedio(7.07) *HorasAnuales(1920)*Incremento en Disponibilidad (5%)	$1,146.00

TOTAL BENEFIT OF OWNERSHIP (TBO)

La matriz que se muestra a continuación ilustra los beneficios más importantes que se anticiparon como resultado de la solución. Las flechas muestran algunas de las áreas principales donde el proyecto agrega valor económico al negocio, ya sea incrementando los ingresos, reduciendo los costos, protegiendo ingresos o evitando costos. Cada uno de estos se explican en las notas que siguen.

Matriz de Beneficio REJ 4x7 de la Solución Integral de Seguridad y Compras Corporativas

		Creación de Valor - Area de TI			Creación de Valor - Area de Negocio			
		Tecnologia de Sistemas	Manejo de Sistemas	Desarrollo de Sistemas	Tareas Individuales	Funciones de Negocio	Procesos de Negocio	Cadena de Valor
Maximización de Ganancias	Aumentar ingresos							
	Reducción de Costos	↓	↓		↓			
Mantenimiento de ganancias	Protección de Ingresos						↑	
	Evitar Costos	↓	↓	↓	↓	↓		

COSTOS DE MANEJO DEL PROYECTO

1. En el proyecto de tesis, se consideraron todos los costos posibles, de manera que sea útil en el ejercicio de análisis financiero. el costo incluye recursos internos de la COMPAÑIA A, recursos de socios, manejo de proyecto e inclusive se estimaron costos de la migración inicial de una plataforma. Este es el estimado global.
2. Se realizará una solución integral de seguridad sobre Plataforma Microsoft.
3. La implantación se realizó como un esfuerzo coordinado entre la COMPAÑIA A, un socio tecnológico de Microsoft y Microsoft Consulting Services, teniendo el diseño Microsoft, y el manejo del proyecto la **COMPAÑÍA A.**
4. Los costos por hora para la implantación en **US$** se estimaron en:

Skill 1 - Ingeniero de Partner MSFT		50
Skill 2 - Consultor de Partner		70
Skill 3 - Consultor MCS		130
Staff IT		12
Usuario regular		10

Los cuales están en concordancia con los usados en las otras herramientas para estimación de beneficios. Si existe un cambio en uno, el cambio se refleja automáticamente en el otro

5. Se estima que diez miembros del Staff de **COMPAÑÍA A** tomaron todos los cursos disponibles de seguridad tecnológica y funcional y a su vez reenseñaron al usuario final y asesorarán en la curva de aprendizaje
6. Las horas de diseño fueron calculadas en base a datos históricos de proyectos similares al presente, y se aplicó un factor de complejidad extra de **15%**

COSTOS DE MIGRACIÓN DE SERVIDORES

1. El costo de un servidor nuevo se estimó en **US$ 8,000.-** Este es un costo deliberadamente alto, ya que la intención es el tener el acercamiento más conservador posible al análisis financiero final.
2. Se estimó que el **25%** de los servidores tendrían que ser substituidos
3. Se estimó que el **50%** de los servidores recibirían un upgrade de hardware equivalente al **20%** del costo de un equipo nuevo
4. Se estimó en **10,600** horas hombre, el esfuerzo para realizar la solución integral de seguridad y la de compras corporativas
5. Se estimó en **5,600** horas hombre, las pruebas post-implantación (Aseguramiento de Calidad y curva de estabilización)
6. En estos dos últimos costos, se están estimando las mejoras pertinentes a los sistemas que se requieran, de forma que puedan correr en la nueva plataforma

COSTO DE MIGRACIÓN DE DESKTOP

1. El costo de una desktop nueva se estimó en **US$ 770.-**
2. La COMPAÑÍA A no pagó upgrade de software debido a que estuvo incluido en su Enterprise Agreement
3. Dada la compra de 100 equipos (**43.5%**) el año anterior, y el perfil de los mismos, no es requerido ningún upgrade para la migración. El **15%** de las desktops serán reemplazadas completamente, y el restante necesitará un upgrade de hardware **41.5%,** equivalente al **20%** del costo de un equipo nuevo

COSTOS DE INFRAESTRUCTURA DE HARDWARE DE SERVIDORES DE MISION CRITICA CON ALTA DISPONIBILIDAD

La infraestructura segura debió reflejarse sobre una sólida plataforma de hardware. Por ello los costos resultaron un factor crítico en la solución:

	Cant	Precio Unitario	Número de Procesadores	Marca	Costo Asociado
MIDDLEWARE SERVER					
BIZTALK SERVER	1	10,000.00	01	**IBM**	10,000.00
WEB SERVER					
COMMERCE SERVER	3	8,000.00	01	**IBM**	24,000.00
WAP SERVER					
WAP STARNDARD SERVER	1	8,000.00	01	**IBM**	8,000.00
TOKENS SERVER					
RSA ACE SERVER	1	8,000.00	01	**IBM**	8,000.00
DATABASE SERVER					
SQL SERVER 2000	2	8,000.00	02	**IBM**	16,000.00
FIREWALL					
Equipo Nokia 440 Base system	3	29,000.00	01	**NOKIA**	77,000.00
TOTAL GENERAL EN US$					**143,000.00**

COSTOS DE MANTENIMIENTO DE SOFTWARE

Los Costos de Licencias afrontadas se pueden agrupar a continuación en el siguiente cuadro que presenta el cronograma de pagos por mantenimiento de licencias de software:

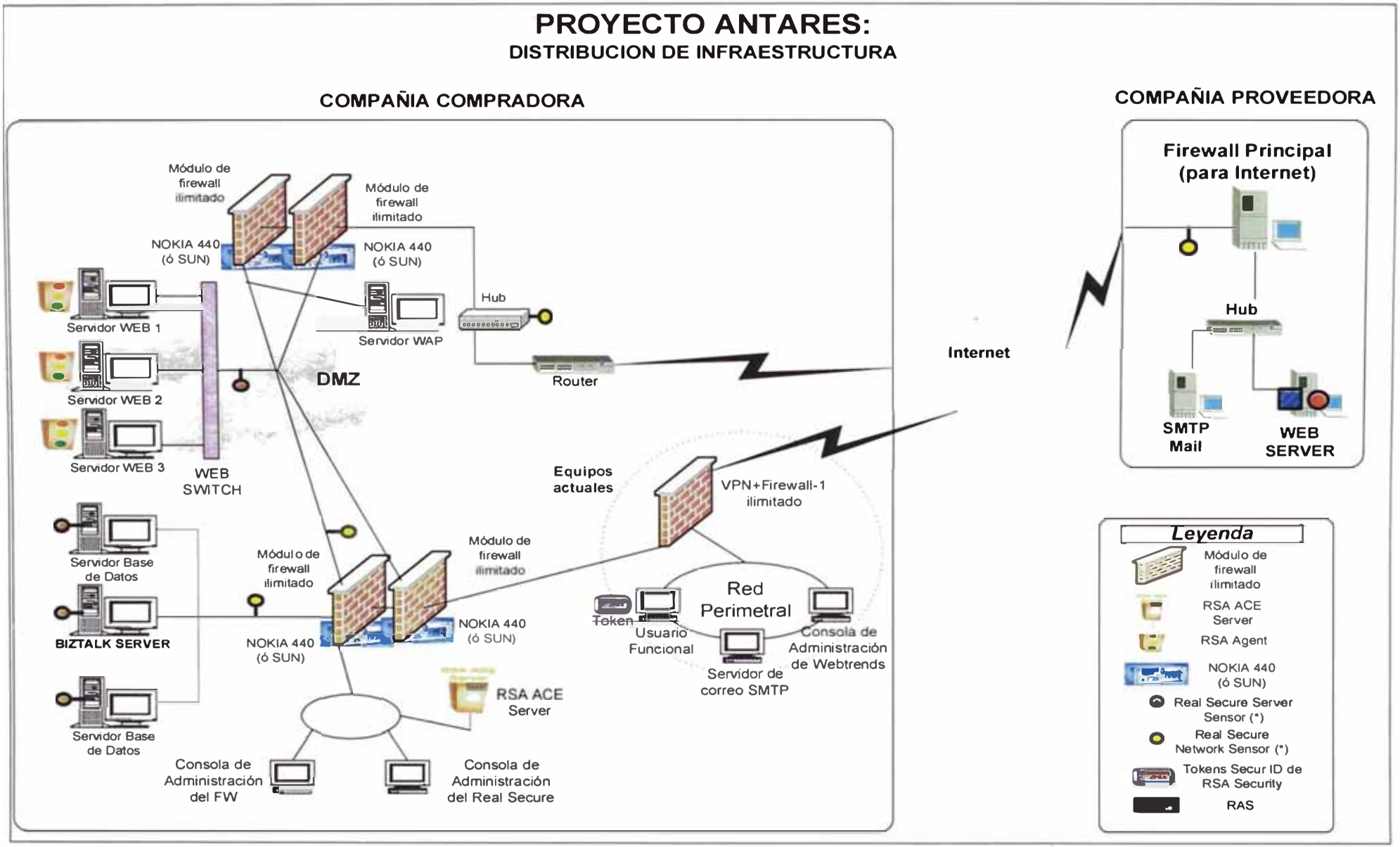
Mantenimiento Anual de Software Proyecto "Antares"

	Cant	Pago Jan-02	Pago May-02	Pago Aug-02	Pago Jan-03	Pago May-03	Pago Aug-03
Check Point							
VPN-1 Enterprise Center/ilimitado	1	2,995			2,995		
Motif GUI	1	145			145		
RSA							
ACE/Server para 250 tokens	1		4,200			4,200	
Websense							
Websense for Microsoft Proxy Server/1000	1		13,000			13,000	
ISS							
RealSecure Network Sensor	2			2,400			2,400
RealSecure Server Sensor 5 device	1			1,200			1,200
Internet Scanner pack 30	1			750			750
System Scanner	2			450			450
Black Ice	3			500			500
Database Scanner	1			500			500
TOTAL GENERAL EN US$		**3,140**	**17,200**	**5,800**	**3,140**	**17,200**	**5,800**

Finalmente, se muestra a continuación el cuadro resumen de Costos beneficios de la solución:

	1	2	3	4
Costos	$6,576	$6,576	$6,576	$6,576
Beneficios	$6,763	$13,526	$20,289	$27,052

PROYECTO ANTARES:
DISTRIBUCION DE INFRAESTRUCTURA




E-PROCUREMENT


E-PROCUREMENT
Catálogos
Carro de Compras
Ayuda
Administrador de Compras
Buscar por
Any information
Empleado
- Productos
- Servicios
Adm. del Site
- Productos
- Servicios
Adm. de Compras
- Productos
- Servicios
Manager
- Productos
- Servicios
Sel.
Nro.
Apellidos
Nombre
Fecha
Estado
Cantidad
Organización
1001 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Completada 284.75
1002 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Enviada 214.35
1003 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Atendida 64.95
1004 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Completada 79.95
1005 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Enviada 284.75
1006 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Atendida 214.35
1007 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Completada 64.95
1009 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Enviada 79.95
1010 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Atendida 284.75
1014 Del Rio y de los Matorrales Sandra Jacinta 2001/10/23 Enviada 214.35
Nro de Registros: 24
Recepcionar
Atender
Detalle
Anterior
Siguiente

CONCLUSIONES Y RECOMENDACIONES

Se ha considerado que luego de la implementación de la metodología se obtuvieron las siguientes conclusiones:

1. La Reducción del impacto de los ataques externos de Agentes Externos: Hackers, debido a un adecuado registro, y la implementación de reglas sistemáticas de protección de Sistemas de Información publicados en Internet.
2. La Reducción de Fisgoneo, Robo de información, pérdida de información y otros imponderables que afectaban considerablemente con el funcionamiento del negocio.
3. El Sustento físico y funcional necesario para tomar la decisión de iniciar negocios electrónicos seguros, que involucren recursos propios de la organización.
4. Poseer personal técnica y funcionalmente capacitado para afrontar situaciones críticas y diarias resultado del funcionamiento propio del negocio a través de Internet y dentro de los límites organizacionales.
5. El Intercambio seguro de información a través de Internet. Esta conclusión es vital en virtud a la necesidad de las organizaciones que comparten procesos de negocio con otras organizaciones fuera de los límites estructurales de las empresas, tales como las pasarelas de pago, los

paneles de seguimiento transaccional y los módulos compartidos de la organización virtual.

6. La reducción de costos de operación de sistemas, soporte reactivo y despliegue de nuevas aplicaciones web enabled.

Se considera necesario brindar a los alumnos laboratorios adecuados de tecnologías de información que posean infraestructura adecuada de software y hardware. Podría sugerir una distribución que posea:

04 Servidores: 02 Windows, 01 Linux, 01 AS/400

20 Estaciones en red: 10 estaciones MS Windows, 10 estaciones LINUX

01 Firewall basado en Hardware

01 Detector de Intrusos (Software)

Es decir 24 computadores y un firewall de hardware en red. Este esquema les posibilitaría realizar la simulación de ataques internos, externos mediante las herramientas descritas y la elaboración de la documentación adecuada para posteriormente incorporar a la currícula de los estudiantes de la facultad.

Otra recomendación es la de realizar convenios (Campus Agreements) con empresas involucradas en la Seguridad de Sistemas en Internet y lograr capacitaciones cíclicas a los estudiantes.

BIBLIOGRAFIA

The Internet Security Guidebook From Planning to Deployment

Juanita Ellis - Timothy Speed

Academic Press

San Diego, California

2001

Designing Secure Web Based Applications for Microsoft Windows 2000

Michael Howard with Marc Levy and Richard Waymire

Microsoft Press

One Microsoft Way

Redmond, Washington

2000

IT Architectures and Middleware Strategies for Building, Large Integrated Systems

Chris Britton

ADDISON-WESLEY

Unisys Corporation

2001

Professional BizTalk

Stephen Mohr and Scott Woodgate

Wrox Press Ltd.

2000

Developing Secure Applications with Visual Basic: The Authoritative Solution

Davis Chapman

Sams Publishing

Indianapolis, Indiana

2000

Course 2379: Developing and Deploying Microsoft Biztalk Server 2000 Solutions

Microsoft Learn Resources

Microsoft Corporation

2001