UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

DISEÑO DE UN CANAL DE COMUNICACIÓN (EXTRANET) ENTRE LA SUPERINTENDENCIA DE BANCA Y SEGUROS Y LAS EMPRESAS DEL SISTEMA FINANCIERO DEL PERÚ

INFORME DE SUFICIENCIA

PARA OPTAR POR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

JUAN EDWIN ZUBILETE JANAMPA

JULIO 2003

LIMA – PERÚ

AGRADECIMIENTOS

Para comenzar doy gracias a Dios por su infinito amor y protección en todos estos años de mi vida. Además, quiero agradecer a mis padres y a mis hermanas por su constante apoyo y ánimo para lograr la titulación.

Quisiera también agradecer a mis compañeros y profesores del Cuarto Programa de Titulación por Actualización de Conocimientos, quienes me ayudaron y alentaron a concluir el presente informe.

Asimismo, muchas gracias a todos los docentes de la Facultad de Ingeniería Industrial y de Sistemas por sus enseñanzas y consejos que contribuyeron a mi formación profesional.

Finalmente, quiero agradecer a mis compañeros de trabajo de la Superintendencia de Banca y Seguros quienes me brindaron su apoyo en la preparación de este informe.

JUAN EDWIN ZUBILETE JANAMPA

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABLAS

DESCRIPTORES TEMÁTICOS

Extranet

Supervisión de bancos

Seguridad en Internet

Análisis costo/ beneficio

Metodología de implementación de sistemas

RESUMEN

"La tecnología ofrece un tremendo potencial para reducir la carga regulatoria, y nosotros estamos explorando agresivamente los medios posibles para automatizar la supervisión. Creo que no está lejos el día cuando la mayor parte de las actividades entre bancos y reguladores se desarrollará a través de sistemas como el BankNet (Extranet entre el ente supervisor y los bancos nacionales de Estados Unidos)". John D. Hawke, Jr. Comptroller of the Currency Administrator of National Banks.

El principal objetivo de este informe es presentar el diseño de un canal de comunicación entre la Superintendencia de Banca y Seguros (SBS) y las empresas supervisadas del sistema financiero utilizando la tecnología Internet, de tal forma que varias actividades de supervisión y nuevos servicios se implementen en forma segura, rápida y oportuna.

El trabajo define los principales servicios que deberían estar incorporados, así como los requerimientos de seguridad y las estrategias necesarias para lograr una implementación exitosa.

El canal es conveniente para las entidades financieras y la SBS. Su uso en las labores de supervisión dependerá principalmente del apoyo de la

Alta Dirección de la SBS y del desarrollo de un piloto con algunas empresas supervisadas antes de su lanzamiento.

Finalmente, debido a la confidencialidad de la información a transmitir, se requiere implementar estrictos mecanismos de control como tener dos niveles de autenticación para comprobar la identidad del cliente y encapsular la información como mínimo a 128 bits.

I. INTRODUCCIÓN

1.1 ANTECEDENTES

La Extranet

Es importante distinguir entre Internet, Intranet y Extranet. La Internet pertenece a todos los usuarios, mientras que la Intranet pertenece a la organización que la mantiene y usa. La Extranet representa el puente entre la Internet pública y la Intranet privada. También se puede decir que la "Extranet es una pieza de la Intranet que provee una ventana pública a otras compañías con el fin de brindar servicios u obtener información" (Loshin 1997).

Aplicaciones de las Extranets

- Grupos privados que cooperan con la empresa y comparten la misma información e ideas.
- Entornos de colaboración, donde algunas empresas colaboran en el desarrollo de una aplicación nueva que estas pueden usar.
- Programas de formación y otros contenidos educativos que las empresas desean desarrollar o compartir.
- Reducción de los costos de los canales de distribución convencionales.

- Gestión de proyecto y control para empresas que forman parte de un mismo proyecto de trabajo.
- Intercambio de información actualizada sobre nuevos productos o servicios, acuerdos de directorio, etc.
- Colaboración de bases de datos y automatización de procedimientos administrativos comunes.
- Intercambio de información mediante formularios electrónicos de fácil manejo.

Uso de Extranets por otros supervisores bancarios

Algunos organismos supervisores bancarios de Estados Unidos, Reino Unido, Alemania y México han construido Extranets con sus empresas supervisadas haciendo uso intensivo de la tecnología e incorporando una amplia variedad de servicios y aplicaciones.

Entre los temas más significativos encontrados en estos sitios web se encuentran la remisión de información de reportes y anexos, seguimiento y verificación de la información contable y financiera, información de central de riesgos de crédito, actualización sobre información de accionistas, temas especializados, foros de diálogo, consultas y preguntas más frecuentes.

Además de la búsqueda de eficiencia en la captura de información, los organismos de control encuentran un lugar donde plantear temas claves para promover la supervisión y regulación tales como la difusión de las

mejores prácticas en los procesos de administración de riesgos, así como foros de discusión sobre temas de actualidad o proyectos de normatividad.

En Latinoamérica, los organismos supervisores bancarios tienen en su mayoría sólo algunos servicios aislados por Internet como la central de riesgos o módulos para el envío de información.

Consideraciones de seguridad

Debido a la confidencialidad de la información que se transmite por este medio, se requiere implementar mecanismos elevados de control, tales como: alto nivel de autenticación y encriptación, políticas de seguridad estrictas, auditoría y monitoreo permanente.

1.2 DISCUSIÓN DEL PROBLEMA

La Superintendencia de Banca y Seguros (SBS) es el organismo encargado de la regulación y supervisión del sistema financiero, seguros y AFP. No obstante el liderazgo reconocido de este ente supervisor, existen aspectos que requieren mejora:

- Falta de mecanismos eficientes para obtener y difundir información entre la Superintendencia de Banca y Seguros (SBS) y las entidades del sistema financiero.
- Deficiencias en seguridad para compartir información con las entidades del sistema financiero utilizando medios electrónicos.

- Costos ocasionados a las entidades del sistema financiero por utilizar medios convencionales más costosos que el canal de Internet para obtener información o enviar información de/a la SBS.
- Falta de mayores servicios de valor agregado para las entidades supervisadas.

Ante esta situación se propone construir un sitio web privado y seguro entre la SBS y las empresas del sistema financiero para brindar servicios e intercambiar información.

Al respecto, el presente informe tiene como objetivo elaborar el diseño funcional de alto nivel de los servicios a brindar en la Extranet, los requerimientos de seguridad y las estrategias necesarias para su implementación exitosa. El alcance del informe sólo contempla a las empresas supervisadas del sistema financiero sin considerar aún la relación con las empresas supervisadas de seguros y AFP.

1.3 DISPOSICIÓN DEL INFORME

Para proveer al lector de una rápida revisión del contenido del informe, se presenta a continuación una breve presentación de cada capítulo.

Capítulo 2. Antecedentes de la empresa; donde se presenta el diagnóstico estratégico y funcional de la SBS.

Capítulo 3. Descripción del problema; donde se describe la situación actual en la que opera la SBS para entregar y obtener información a/de las

entidades supervisadas, y las acciones que vienen desarrollando al respecto algunos supervisores bancarios de otros países.

Capítulo 4. Marco teórico; donde se describe la tecnología Extranet, sus ventajas y desventajas, los aspectos de seguridad requeridos y una metodología de desarrollo e implementación de sistemas de información.

Capítulo 5. Proceso de toma de decisiones; donde se plantea las alternativas disponibles, el análisis costo beneficio de la solución propuesta y los servicios, requerimientos de seguridad y estrategias a adoptar para su implementación.

Capítulo 6. Evaluación de resultados; donde se presenta los resultados que se prevén luego de finalizada la implementación de la solución propuesta.

Bibliografía; donde se puede encontrar toda la información fuente que ha sido utilizada para la elaboración del presente trabajo.

II. ANTECEDENTES DE LA EMPRESA

2.1 DIAGNÓSTICO ESTRATÉGICO

2.1.1 ¿Qué es la Superintendencia de Banca y Seguros?

La Superintendencia de Banca y Seguros (SBS) es el organismo encargado de la regulación y supervisión de los sistemas financiero, de seguros y del sistema privado de pensiones.

2.1.2 Misión y Visión de la SBS[1]

La misión de la SBS es proteger los intereses de los depositantes, asegurados y afiliados al sistema privado de pensiones, preservando la solidez e integridad de los sistemas financiero, de seguros y privado de pensiones.

Como institución reguladora la SBS propicia el desarrollo de un marco legal moderno sobre la base del funcionamiento de una economía de mercado. En cuanto a la tarea de supervisión, ésta consiste en velar, en forma permanente, por la solvencia e integridad de cada empresa que actúa en el mercado. De esta manera, la SBS contribuye a generar valor en los

[1] Tomado de la página Web de la SBS (www.sbs.gob.pe)

mercados financieros, de seguros y privado de pensiones, a través de la señal de credibilidad que brinda una supervisión eficaz.

2.1.3 Fortalezas y debilidades

Fortalezas

- Marco Regulatorio

  La SBS tiene experiencia en la elaboración de normas.

  Las normas son flexibles, adecuándose a las distintas coyunturas y necesidades de regulación.

  Las normas emitidas han permitido establecer un marco regulatorio que posibilita cumplir las funciones de supervisión y regulación de las empresas.

  La SBS cuenta con personal capacitado que le permite afrontar con éxito el reto de elaborar la mayor parte de las normas aplicables a los sistemas financiero, de seguros y AFP.

- Supervisión

  La SBS aplica un esquema de supervisión moderno, basado en la identificación, medición y seguimiento de los riesgos que enfrentan las entidades del sistema financiero. Este esquema enfatiza como riesgos principales el riesgo de crédito, de liquidez, de mercado y de operación. Para ello, la SBS realiza una supervisión *in situ* y *extra situ*.

  La supervisión *in situ* se efectúa mediante visitas de inspección de dos tipos a las empresas del sistema financiero: integrales y especiales. Las visitas integrales tienen lugar una vez al año. Las visitas especiales son

sorpresivas, y se realizan con un equipo más reducido, con el fin de evaluar un tema específico a partir de algún indicio detectado por las áreas de análisis.

La SBS cuenta con equipos especializados, capacitados en riesgo de crédito, de mercado, de liquidez y de operación, y con personal de alta experiencia en el manejo de problemas en el sector financiero.

La SBS cuenta con el apoyo de los auditores internos y externos y de las clasificadoras de riesgo.

La evaluación de los controles internos de los bancos se realiza con el apoyo de las unidades de auditoría a través de los planes e informes de auditoría interna de las empresas.

Los auditores externos emiten informes sobre la conformidad de los resultados y operaciones que realizan las empresas así como sobre sus sistemas de control interno.

Las empresas del sistema financiero deben contar por lo menos con dos clasificaciones al año de dos empresas clasificadoras de riesgo.

La Ley General del Sistema Financiero otorga amplias facultades a la SBS para sancionar a las empresas, a sus accionistas y funcionarios por infracciones a la Ley o a las normas dictadas por la Superintendencia.

La difusión de información no confidencial al público en general, se realiza mediante boletines, página Web y reportes estadísticos de manera precisa y oportuna.

- Recursos Humanos

El desarrollo de los recursos humanos se apoya en programas permanentes de capacitación.

- Recursos Financieros

  Los ingresos de la SBS son propios y relativamente estables, sustentados principalmente en las contribuciones percibidas de las instituciones bancarias, financieras, aseguradoras y AFPs.

Debilidades

- Cambios por motivos políticos a los que está sometido la SBS dificultan la ejecución de proyectos de mediano y largo plazo.
- Falta de mecanismos adecuados para la difusión de los objetivos de las normas al nivel de las áreas de línea y de las entidades del sistema financiero, lo cual origina desconocimiento, continuas consultas y aplicación heterogénea.
- Ejecución de tareas de carácter operativo en desmedro de las tareas de análisis.
- Validación manual de parte de la información que se recibe de las empresas supervisadas, que demora su disponibilidad para el análisis.
- Varios procesos internos son manuales y carecen del soporte de aplicaciones informáticas, ocasionando distracciones del personal en actividades operativas.
- No existe un plan de carrera para el personal de la SBS.

2.1.4 Oportunidades y Amenazas

Oportunidades

- La SBS cuenta con fuentes de financiamiento externo para la ejecución de diversos proyectos que mejoren el proceso de supervisión, como los créditos del BID coordinados a través de la Unidad de Coordinación de Préstamos Sectoriales del Ministerio de Economía y Finanzas.
- La SBS realiza su función de supervisión y regulación interactuando con otras entidades públicas y privadas, ya sea a través de convenios de intercambio de información o mediante coordinaciones con diversos organismos, con el objeto de desarrollar una regulación y supervisión financiera y de seguros efectivas.
- Coordinación e interacción con diversos organismos y entidades del ámbito nacional y extranjero: Ministerio de Economía y Finanzas, Banco Central de Reserva del Perú, Comisión Nacional Supervisora de Empresas y Valores, Corporación Financiera de Desarrollo, Superintendencia Nacional de Administración Tributaria, Órganos de Supervisión y Control Financieros de otros países, organismos internacionales como el *Bank of International Settlements* (BIS), a través del Comité de Basilea (entidad que elabora lineamientos de regulación prudencial a nivel mundial), entre otros.

Amenazas

- Entorno político y económico inestable.
- Distintos marcos de regulación y mecanismos de supervisión entre los organismos de supervisión.

- Problemas de Información. Los sistemas financiero, de seguros y AFP son sensibles a la difusión de información por una gran variedad de agentes.

2.1.5 Objetivos estratégicos 2003-2004

Después de cuatro años se llevó a cabo un proceso de Planeamiento Estratégico en la institución, definiendo objetivos, acciones y metas para el ejercicio 2003-2004[2].

Dentro del planeamiento se ha considerado el desarrollo e implementación de un Portal Web con las entidades supervisadas, la misma que se dará inicio a mediados del segundo semestre del presente año.

El contar con dicho portal contribuirá, entre otros objetivos, a comunicar oportunamente los riesgos identificados por la SBS a las entidades financieras supervisadas, que coadyuvará en mantener un sistema financiero sólido y seguro.

2.2 DIAGNÓSTICO FUNCIONAL

2.2.1 Funciones de la SBS[3]

La labor de la SBS comprende dos tareas básicas: regulación y supervisión. La regulación establece las reglas a las cuales se someten las empresas supervisadas desde su entrada al sistema, durante su operación y eventual salida del mercado. La supervisión consiste en verificar el

[2] Memoria SBS 2002 – Página 5 (publicada en www.sbs.gob.pe)
[3] Tomado de la página Web SBS (www.sbs.gob.pe)

cumplimiento de las normas y la aplicación de políticas y prácticas prudenciales por parte de las empresas supervisadas.

Las principales actividades de regulación y supervisión a las empresas del sistema financiero son:

Regulación

- Verificar que la dirección de las empresas supervisadas esté en manos de personas idóneas. El principal énfasis se encuentra en los requisitos de entrada al mercado.
- Respecto de la calidad de información y análisis empleado por las empresas supervisadas, la regulación de la SBS propicia una visión prospectiva de los riesgos que enfrentan las empresas supervisadas. El énfasis está puesto en la necesidad de aplicar sistemas que les permitan identificar, medir, controlar y monitorear sus riesgos de una manera eficiente. Las empresas tienen libertad para implementar los sistemas que crean más convenientes, pero la SBS establece los parámetros mínimos que deben cumplirse para garantizar un manejo prudente de los riesgos.
- La regulación busca crear incentivos y herramientas que garanticen la calidad y oportunidad de la información emitida por las empresas supervisadas.
- Se busca que las normas dictadas por la SBS sean de fácil comprensión, exigibles y que puedan ser supervisadas.

Supervisión

La estrategia de supervisión de la SBS se desarrolla en dos frentes. El primero consiste en la supervisión que ejerce directamente sobre las empresas y el segundo se basa en participación de los colaboradores externos, tales como los auditores, las empresas clasificadoras de riesgo, supervisores locales y de otros países.

- Con relación a la supervisión directa, ésta se desarrolla bajo dos modalidades: la *supervisión extra-situ* y la *supervisión in-situ*. La primera consiste en analizar en forma permanente la información brindada por las empresas supervisadas e identificar los temas que sean de preocupación y que merezcan un examen más profundo. La segunda se ocupa de verificar en la propia empresa supervisada los aspectos identificados previamente en la labor de análisis extra-situ.
- Respecto de la colaboración de agentes externos, desde su propia perspectiva estas entidades ejercen un cierto tipo de monitoreo de las empresas que se encuentran dentro del ámbito de la Superintendencia. La estrategia de la SBS es buscar que su participación sea permanente y consistente con la regulación. En el caso de los auditores y clasificadoras de riesgo se busca que, adicionalmente a las labores que realicen estos agentes, se pronuncien sobre la calidad de la administración de riesgos de las empresas. En el caso de los supervisores locales y de otros países, la estrategia se basa en propiciar la cooperación y el intercambio de información.

2.2.2 Macro procesos de la SBS

Figura Nº 1: Principales procesos de la SBS

Fuente: Propia

2.2.2.1 Procesos Críticos

Planeamiento

- Elaboración del Plan Estratégico de la SBS
- Evaluación del cumplimiento de los objetivos estratégicos de la SBS.

Gestión de Riesgos

- *Definición del Contexto*

- Identificación de los objetivos estratégicos de la SBS.
- Identificación de los grupos de interés y sus objetivos.
- Definición de los criterios de éxito de la SBS.
- Definición de las áreas de interés de la SBS.

- *Identificación de los Riesgos*

- Determinación de factores de riesgo y la forma como influyen.
- Identificación de temas nuevos / emergentes que pueden generar nuevos riesgos.

- *Análisis de los Riesgos*

  Revisión de los controles existentes para tratar el riesgo.

  Definición de medidas cualitativas/cuantitativas de la probabilidad e impacto del riesgo.

  Empleo de modelos de riesgos.

  Asignación de un nivel inicial de riesgo.

- *Evaluación de los Riesgos*

  Revisión de los resultados del análisis en comparación con los objetivos y prioridades de la SBS.

  Evaluación de los riesgos individuales.

  Elaboración de un ranking de riesgos y priorización de los riesgos.

- *Tratamiento de los Riesgos*

  Selección de las opciones para enfrentar los riesgos identificados.

  Establecimiento de medidas para tratar con los riesgos antes de que aparezcan.

  Elaboración de planes de contingencia o recuperación ante la aparición de los riesgos.

  Modificación de los planes de la SBS para evitar algunos riesgos o hacer menos vulnerable a la organización.

- *Monitoreo y Revisión*

  Monitoreo de los resultados de cada fase.

  Identificación de cambios en el entorno de la SBS u obtención de nueva información que torne desactualizados los resultados de las fases anteriores.

Monitoreo del desempeño de cada fase para asegurar su eficiencia y eficacia.

Las fases anteriormente descritas se desarrollan tanto a través de la supervisión (extra-situ e in-situ), la regulación y el empleo de la disciplina del mercado, entre otras herramientas a disposición de los supervisores.

2.2.2.2 Procesos de Apoyo

Gestión del Conocimiento

Capacitación del personal.

Desarrollo del conocimiento institucional.

Gestión de la Información

Comunicación interna y externa.

Administración de la documentación recibida / emitida.

Atención de consultas, pedidos y requerimientos de organismos externos.

Gestión de los Recursos

Administración de los recursos humanos.

Administración de los recursos logísticos.

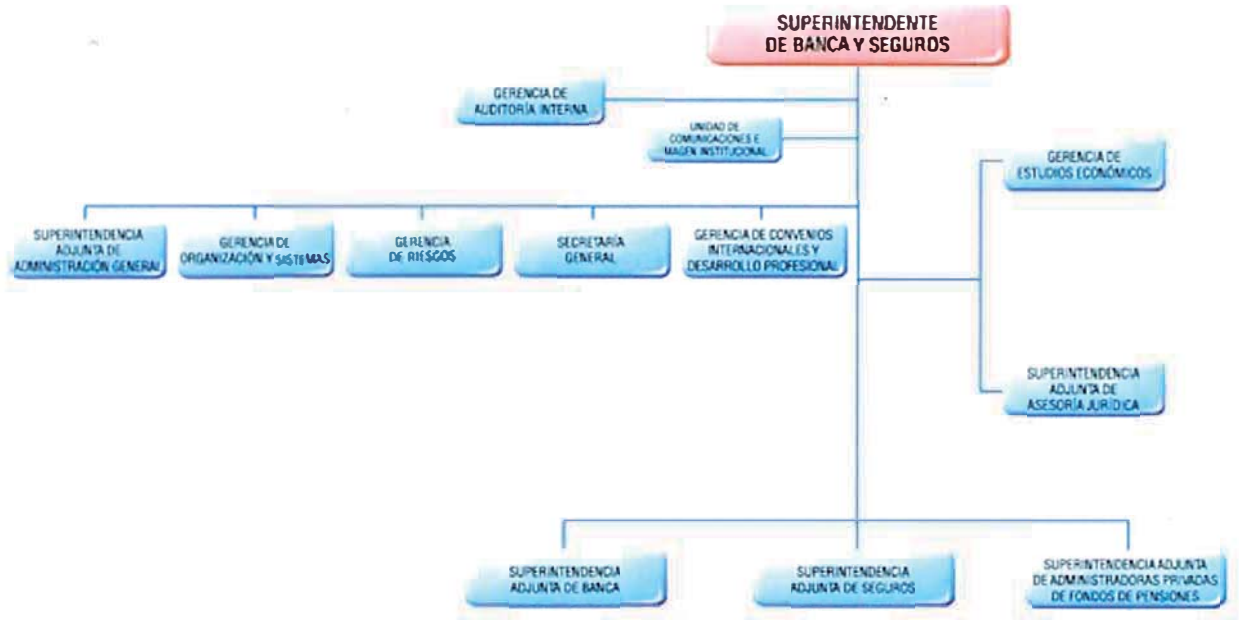
Administración de la tecnología de información.

2.2.3 Breve descripción de las principales áreas funcionales

- La **Superintendencia Adjunta de Banca** es el órgano encargado de realizar la evaluación e inspección permanente de las empresas del sistema financiero, de los conglomerados financieros a los que éstas pertenecen y demás empresas sometidas a su supervisión, para el

adecuado control de los riesgos que los supervisados asumen en sus operaciones.

Figura Nº 2: Organigrama SBS



Fuente: www.sbs.gob.pe, visitado el 03.05.2003

- La **Superintendencia Adjunta de Seguros** es el órgano encargado de realizar la evaluación e inspección permanente de las empresas de seguros y reaseguros, sus subsidiarias y los intermediarios y auxiliares de seguros, cajas de pensiones y derramas inscritas en el libro según Ley Nº 26516, para el adecuado control de los riesgos que los supervisados asumen en sus operaciones.
- La **Superintendencia Adjunta de AFP** es el órgano encargado de controlar el riesgo y velar por la adecuada rentabilidad de las inversiones que efectúen las AFP con los recursos del fondo de pensiones, realizar el control y la fiscalización de las actividades de las AFP en cumplimiento de

las disposiciones financieras, legales y administrativas que las rigen, así como resguardar el otorgamiento adecuado y oportuno de las prestaciones y los beneficios de los afiliados.

- La **Gerencia de Estudios Económicos** apoya la labor de regulación y supervisión del sistema financiero, sistema de seguros y sistema privado de administración de fondos de pensiones, a través de la producción de estadísticas y de la realización de estudios sobre temas económicos, financieros, de seguros y de pensiones.

- La **Superintendencia Adjunta de Asesoría Jurídica** brinda asesoría a los demás órganos de la institución y emite opinión como instancia superior, en materias de carácter legal bajo competencia de la Superintendencia, así como de elaborar las normas que corresponde emitir a la Superintendencia para el adecuado control de las empresas y personas naturales supervisadas.

- La **Gerencia de Auditoría Interna** es el órgano encargado de efectuar el control posterior, en forma sistemática y permanente, de la gestión operativa, económica, financiera y presupuestal de la Superintendencia de Banca y Seguros, de conformidad con las normas que rigen el Sistema Nacional de Control, los dispositivos legales vigentes sobre la materia y los objetivos y metas aprobados por el Superintendente.

2.3 LOGROS Y RECONOCIMIENTOS EN EL 2003

- Se tiene un sólido sistema financiero peruano, que ha recibido el reconocimiento de distintos organismos internacionales. Es por ello que

en la reciente reunión anual[4] de Gobernadores del Banco Interamericano de Desarrollo (BID) llevado a cabo en Italia, el sistema financiero peruano es ubicado en el segundo puesto junto a Chile, después de México para América Latina.

- Percepción e imagen de la SBS. Según el estudio de Actitudes hacia la Economía, el Estado e Imagen de Instituciones Estatales en la Opinión Pública, realizado por la empresa Apoyo, en abril del 2003, la Superintendencia de Banca y Seguros obtuvo a nivel nacional una identificación del 44 por ciento y al conocer al titular de la institución, la opinión favorable alcanzó el 60 por ciento. Dicha aprobación se incrementa conforme se eleva el nivel educativo y socio-económico de la población encuestada.
- Nueva Central de Riesgos Web. En su afán de mejorar la transparencia de la información del sistema financiero, la Superintendencia de Banca y Seguros está trabajando en la construcción de la Nueva Central de Riesgos Web. Este nuevo sistema permitirá a las empresas supervisadas contar con una importante herramienta de consulta, seguimiento y evaluación para el otorgamiento de créditos a sus clientes.
- Con el objeto de brindar al público información integral respecto a los tres sectores que supervisa y regula la SBS, a partir del 1 de abril la SBS amplió los temas a informar en los programas de CPN (Cadena Peruana de Noticias) y RPP (Radio Programas del Perú).

[4] Del 24 al 26 de marzo de 2003 en Milán. Se dieron cita los ministros de economía y finanzas, presidentes de bancos centrales y altos funcionarios gubernamentales de más de 46 países.

- Publicación de tasas de interés para MiVivienda. A partir del 19 de marzo de 2003, la SBS inició la publicación periódica de los costos asociados al crédito hipotecario del programa MiVivienda.
- Campaña Pánico Financiero. La Superintendencia llevó a cabo una campaña de difusión de la ley que sanciona el pánico financiero.

III. DESCRIPCIÓN DEL PROBLEMA

3.1 PLANTEAMIENTO DEL PROBLEMA

No obstante el reconocimiento a la labor de la SBS de distintos organismos nacionales e internacionales, existen actividades – como es natural en cualquier empresa – que requieren ser mejoradas:

- Falta de mecanismos eficientes para obtener y difundir información de y hacia a las entidades del sistema financiero.

Existe información útil para la labor de análisis de la SBS que no es obtenida en forma eficiente, tales como observaciones de las unidades de auditoría interna, observaciones de las unidades de riesgos, políticas, procedimientos, manuales, entre otros requerimientos de información.

De otro lado, se tiene información de utilidad para las empresas supervisadas que no se comunican eficientemente debido a la falta de definición de qué comunicar y/o los medios para hacerlo en forma rápida y segura.

- Deficiencias en seguridad para compartir información con las entidades del sistema financiero.

Algunos medios usados para compartir información con las entidades supervisadas no son seguros como el correo electrónico, FTP o la página Web SBS que es de dominio público.

- Costos ocasionados a las entidades del sistema financiero para obtener información, enviar información a la SBS o para hacer consultas (en tiempo y dinero)

Las entidades tienen que utilizar los medios tradicionales como el teléfono, correo postal o venir en forma presencial a la SBS para actividades rutinarias como obtener información de interés que está en poder la SBS, enviar información requerida por alguna resolución, circular o simplemente para efectuar consultas que podrían ser similares a consultas efectuadas por otras entidades.

Los costos de efectuar operaciones en forma presencial, por teléfono o correo postal son evidentemente mayores que hacerlos por Internet, cuyo uso es ya universal.

Los medios tradicionales siguen siendo útiles y necesarios, pero varias actividades, especialmente sin son repetitivas, podrían realizarse a través del canal más barato que existe en la actualidad: Internet.

- Falta de más servicios de valor agregado para las entidades supervisadas

Por ejemplo: Atención rápida a sus comunicaciones, personalización de información por cada empresa supervisada, servicios de normas actualizadas con los últimos cambios y herramientas de análisis en línea.

3.2 OBJETIVOS DEL INFORME

El principal objetivo de este informe es definir el contenido de un canal por Internet, privado y seguro (comúnmente llamado Extranet), entre la SBS y las empresas del sistema financiero para brindar servicios e intercambiar información.

3.3 ALCANCE

El alcance del trabajo está limitado a las empresas supervisadas del sistema financiero, sin considerar la relación con las empresas supervisadas de Seguros y AFP, ni otras instituciones como la Unidad de Inteligencia Financiera (UIF), Ministerios del Estado u otros supervisores nacionales o extranjeros.

3.4 VISIÓN DEL CANAL EXTRANET EN EL ROL SUPERVISOR SBS

Que los funcionarios del sistema financiero accedan en línea, en tiempo real y en forma segura a información de utilidad que contribuya a su gestión y que a la vez informen continuamente sus prácticas a la SBS. Asimismo, que los funcionarios de la SBS los encuentren en línea para explicarles las normas, políticas y contestar sus preguntas. Más aún, que todas las transacciones rutinarias entre la SBS y las empresas supervisadas sean efectuadas electrónicamente por este canal.

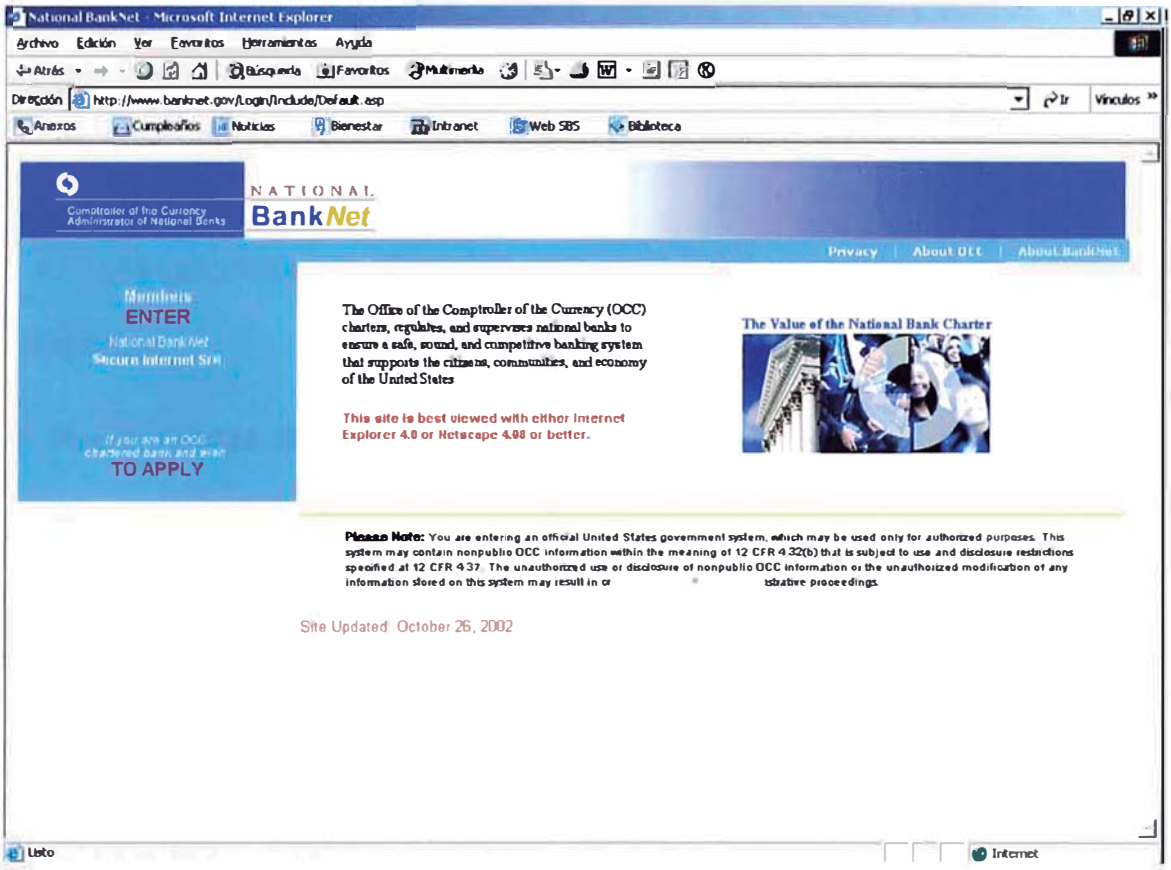
3.5 SITUACIÓN INTERNACIONAL

Varios supervisores bancarios de otros países han construido canales de comunicación con sus supervisados a través del Internet. A continuación los casos más destacados:

3.5.1 Estados Unidos de América

La *Office of the Comptroller of the Currency* (OCC) regula y supervisa a todos los bancos nacionales de los Estados Unidos. La OCC ha construido una Extranet con sus supervisados denominada **Nacional Banknet**.

Figura Nº 3: National Banknet (OCC)



Fuente: http://www.banknet.gov/ , visitado el 26 de octubre de 2002

El National BankNet es un exclusivo servicio Web para los bancos nacionales supervisados por la OCC. Este servicio va más allá que un servicio estándar en Internet.

El National BankNet está comenzando a revolucionar la forma en que la OCC se comunica con los bancos. En lugar de depender de documentos y

servicios postales o hasta del correo electrónico por Internet, se ha abierto una puerta a los bancos para una comunicación en tiempo real.

El National BankNet fue lanzado en noviembre de 1999 con el popular sistema de análisis comparativo (denominado CAR) que provee análisis comparativos entre los bancos. El sitio Web no tiene costo y provee a los bancos información precisa y adecuada en una plataforma segura que garantiza la seguridad de la información y la integridad de los datos.

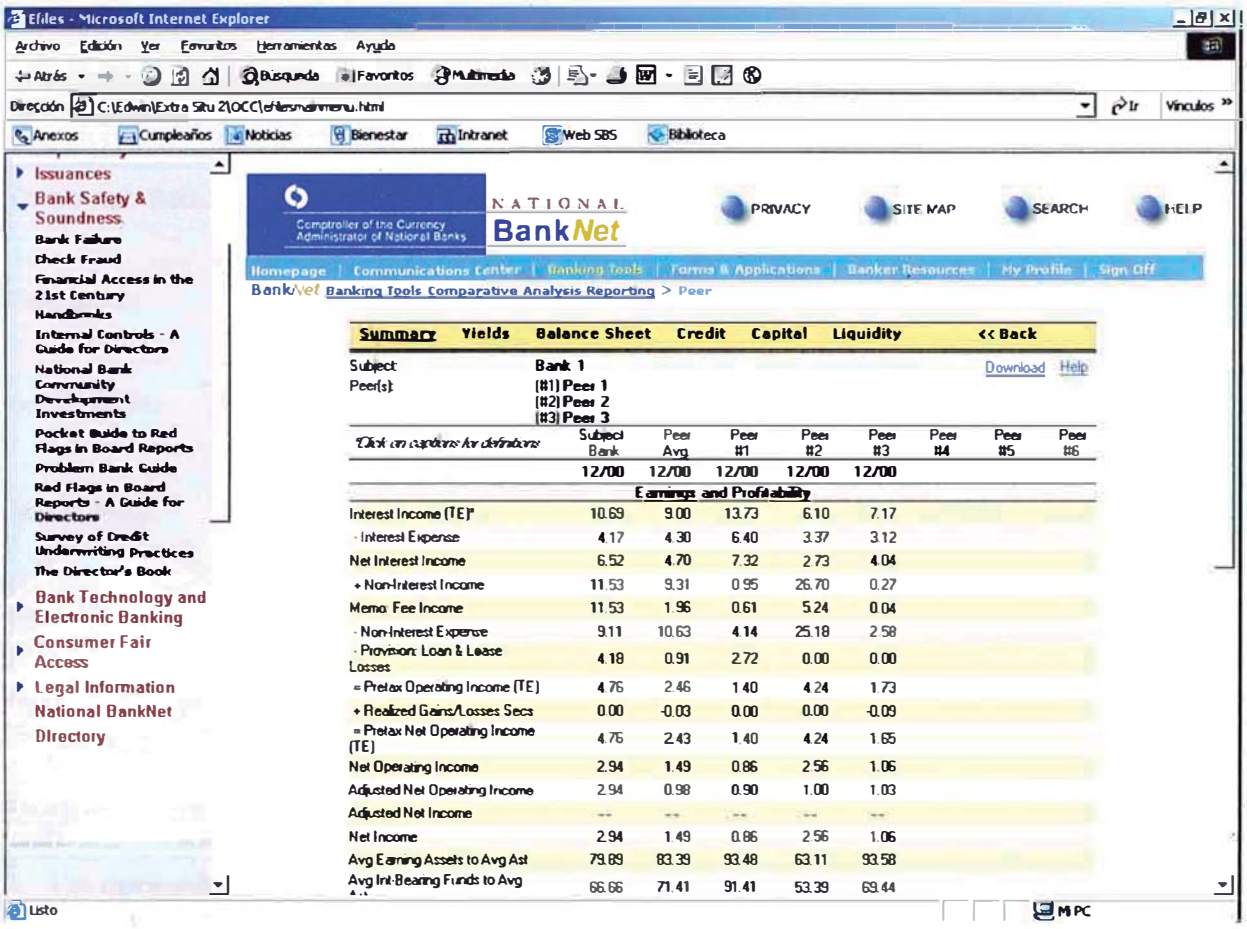
Los servicios de BankNet se encuentran organizados en cuatro categorías:

- **Herramientas de Análisis**

Una variedad de amigables modelos financieros están disponibles para ayudar a los bancos en sus labores diarias. Estos modelos sirven a los bancos para analizar su desempeño desde una perspectiva de competitividad, rentabilidad, riesgo y regulación.

Comparative Analysis Reporting (CAR).- Fue la primera aplicación disponible de la OCC. CAR permite a los bancos compararse con otros bancos comerciales desde competidores locales hasta instituciones de todo el país en más de 200 criterios financieros. Los criterios están agrupados en las categorías de ingresos, rentabilidad, tasa de interés, balance, créditos, capital y liquidez. Un banco puede compararse con otros seis bancos al mismo tiempo y ver su desempeño histórico.

Figura Nº 4: Comparative Analysis Reporting – CAR (OCC)



Canary.- Es un paquete de herramientas que la OCC viene usando para identificar los riesgos emergentes en cada banco. El componente más innovador es un sistema de *benchmarks* que sirve como alerta temprana.

El *benchmark* consiste de 15 ratios y medidas relacionadas al riesgo de crédito, de tasa de interés y de liquidez.

Figura Nº 5: Cómo se muestran los resultados del *benchmark*

Credit Risk	Type	Benchmark*	06/30/2001	03/31/2001	12/31/2000	09/30/2000	06/30/2000
Adjusted Reserve to Adjusted Loans	ROC	<-50bp	-1042bp	-619bp	-748bp	84bp	-17bp
	Static	<0%	-11.65%	-9.34%	-9.82%	-1.00%	-1.23%
Change in Portfolio Mix	ROC	>7%	2.56%	1.95%	2.84%	6.81%	4.19%
	Static	>7%	2.56%	1.95%	2.84%	6.81%	4.19%
Loan Growth	ROC	>15%	-22.85%	-7.77%	-10.09%	-6.60%	15.95%
	Static	>20%	-22.85%	-7.77%	-10.09%	-6.60%	15.95%
Loan to Assets	ROC	>15%	-17.03%	-7.57%	-12.28%	-1.39%	2.66%
	Static	>70%	74.40%	81.10%	78.01%	81.48%	89.67%
Loan to Equity	ROC	>15%	-26.61%	-14.36%	-19.65%	-18.70%	-1.01%
	Static	>8x	6.45	7.49	7.06	7.18	8.78
Loan Yield	ROC	>15%	-4.51%	-1.48%	-0.28%	1.04%	2.76%
	Static	>=9.7%	9.96%	9.98%	10.73%	10.65%	10.43%

Fuente: Early Warning Analysis & Stress Testing. May 2002. Association of Supervisors of Banks of the Americas. V Annual Assembly.

Recursos para los Bancos

Un conjunto de información actualizada que puede ayudar a los bancos a un manejo más eficiente.

Mejores prácticas.- La OCC recoge las mejores prácticas de un conjunto de actividades bancarias. Estas mejores prácticas están basadas en la perspectiva nacional de los 2300 bancos que supervisa. Esta información puede proveer a los bancos información útil para que desarrollen negocios efectivos.

Análisis económico y análisis de riesgos.- El Comité de Riesgos y el Departamento de Economía de la OCC producen un conjunto de análisis e información. El National Banknet permite a la OCC ofrecer los beneficios de su investigación a los bancos de una manera oportuna y útil.

Servicios y productos bancarios.- Los bancos pueden acceder a una lista de las descripciones de las actividades permitidas a los bancos públicos y sus subsidiarias en áreas específicas, tal como Banca Electrónica.

Regulación y Supervisión.- Una variedad de documentos actualizados de supervisión y regulación, e información de leyes, reglamentos y políticas, y su impacto en los bancos públicos.

E-Files.- *Examitanion handbooks*, alertas, cartas con consultas, boletines y otras publicaciones oficiales producidas por la OCC están disponibles en este medio y son actualizadas regularmente.

OCC Trainining.- Anuncios de entrenamiento de la OCC disponibles a los bancos son anunciados en este sitio. En el futuro, la OCC espera ofrecer cursos a distancia basados en este canal Web.

- **Reportes y Aplicaciones**

El Nacional Banknet es usado para reducir la carga que implica una solicitud o requerimiento de información. Mediante este sistema eficiente y seguro, la OCC reduce los papeles de trabajo.

Proceso de solicitudes electrónicas corporativas.- Este proceso provee archivamiento electrónico de solicitudes.

E-Corp.- Los bancos pueden completar y enviar electrónicamente la solicitud de apertura o cambio de ubicación de una agencia.

Esta herramienta permite en forma simple e interactiva el envío de solicitudes de autorización. Los aplicantes ven sólo algunas preguntas que completar. Una lista de opciones asiste a los aplicantes con información específica de la empresa tomada de la base de datos de la OCC. Los hipervínculos conectan a los usuarios rápida y fácilmente a todos los términos relevantes del licenciamiento, leyes y regulaciones, y consecuentemente reduciendo tiempos de investigación.

La herramienta ejecuta una revisión automática que asegura que la documentación esté completa antes de aceptar la solicitud. Los aplicantes son advertidos a no contestar respuestas erradas o incompletas para asegurar que el proceso de aplicación no sea indebidamente retrasado. En adición, la aplicación podría firmarse con una entidad certificadora de firmas digitales y enviarse a la OCC en línea y la herramienta proveería una inmediata aprobación.

- **Centro de Comunicación**

El centro de comunicación es un mecanismo amigable que puede ser usado por los bancos públicos para enviar y recibir mensajes seguros a y desde la OCC.

Centro de mensajes.- Mensajes y respuestas en tiempo real pueden ser comunicados.

Calendario de eventos.- Una lista de eventos de la OCC de interés de los supervisados.

Centro de Audio / Video.- La OCC ofrecerá transmisiones en vivo de seminarios, entrevistas al Contralor, medios informativos y otras presentaciones en línea.

3.5.2 Reino Unido

La *Financial Services Authority* (FSA) es la institución que regula los servicios de las entidades financieras en el Reino Unido. En su portal Web ha incluido servicios para las empresas reguladas.

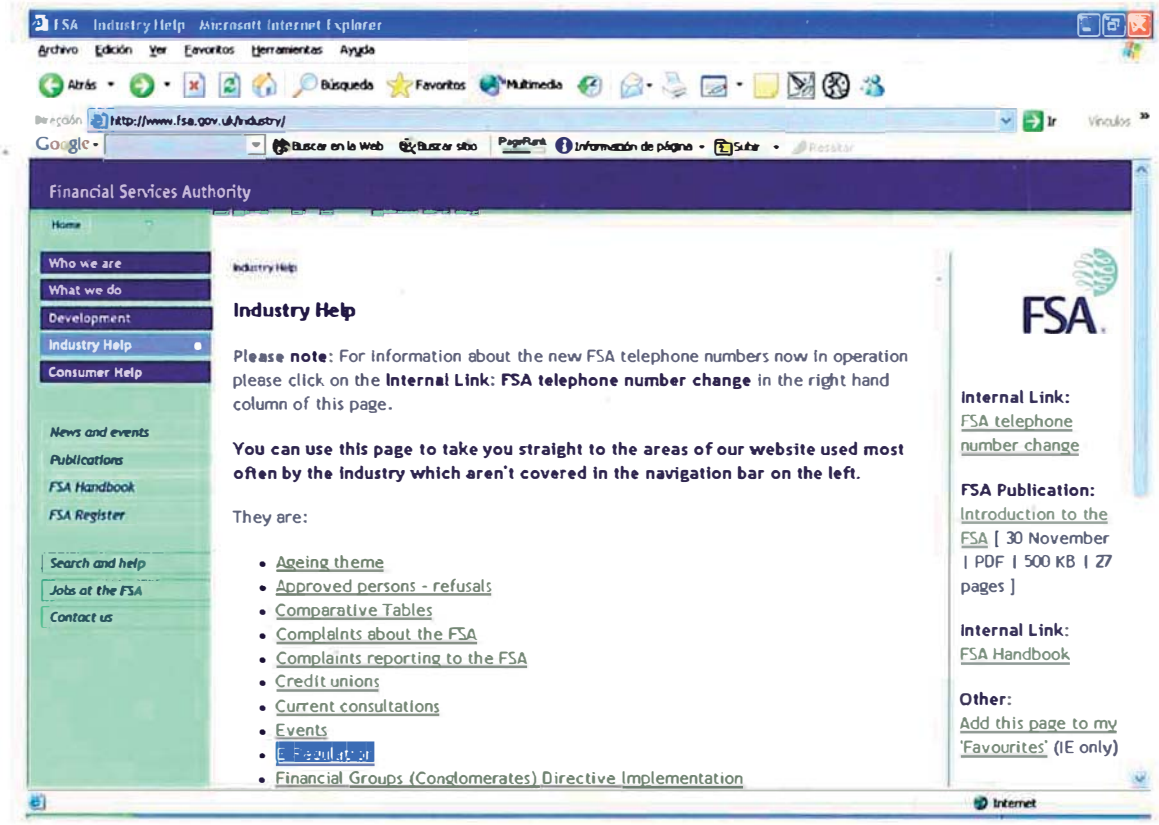
E-Regulation

La FSA está comprometida en tomar todas las ventajas que ofrece la tecnología para mejorar su eficiencia, analizar y entender mejor los mercados obteniendo alertas tempranas de los riesgos emergentes y dar información general a sus clientes.

El programa *E-Regulation* provee aplicaciones basadas en Web que permiten a las entidades enviar sus aplicaciones y recibir las respuestas electrónicamente. Estos servicios están abiertos a todas las entidades reguladas luego de un registro inicial.

La FSA indica que continuará ampliando el alcance de los reportes electrónicos, mejorando el tiempo de atención y reduciendo los costos para la industria y al regulador.

Figura Nº 6: E-Regulation (FSA)



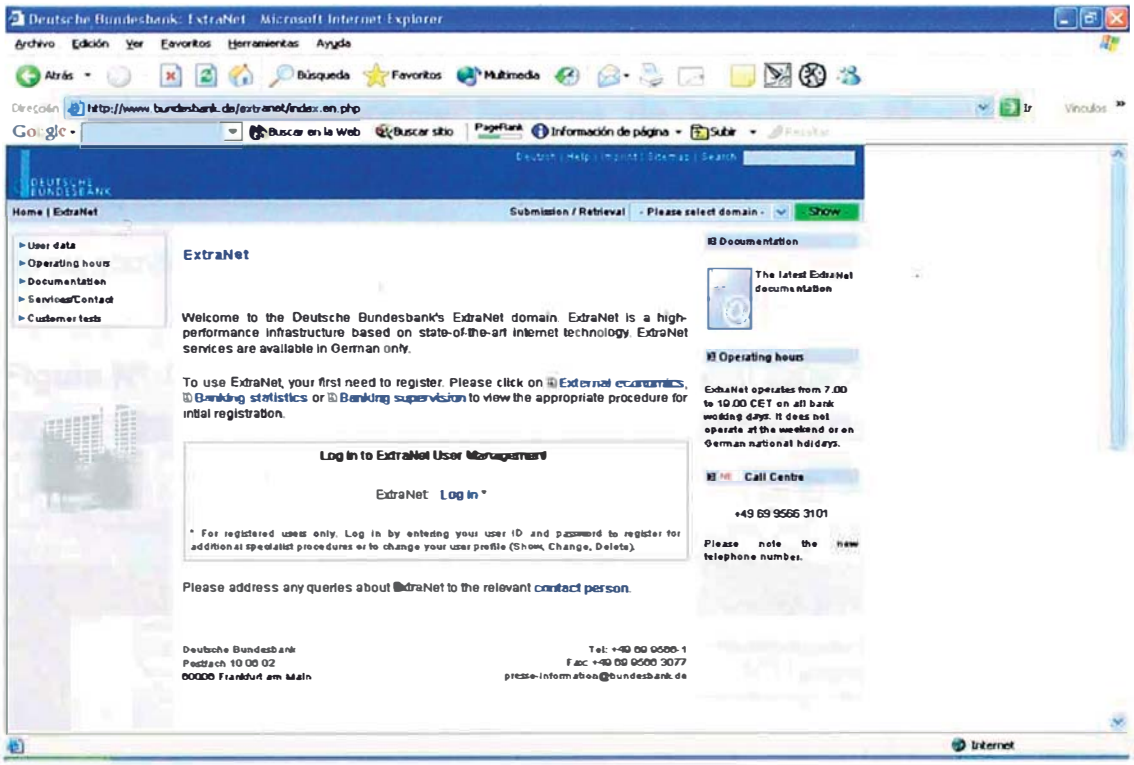
Fuente: http://www.fsa.gov.uk/, visitado el 03 de julio de 2003

3.5.3 Alemania

La *Deutsche Bundesbank* (DB) es el Banco Central de la República Federal de Alemania y forma parte del Sistema Europeo de Bancos Centrales (ESCB).

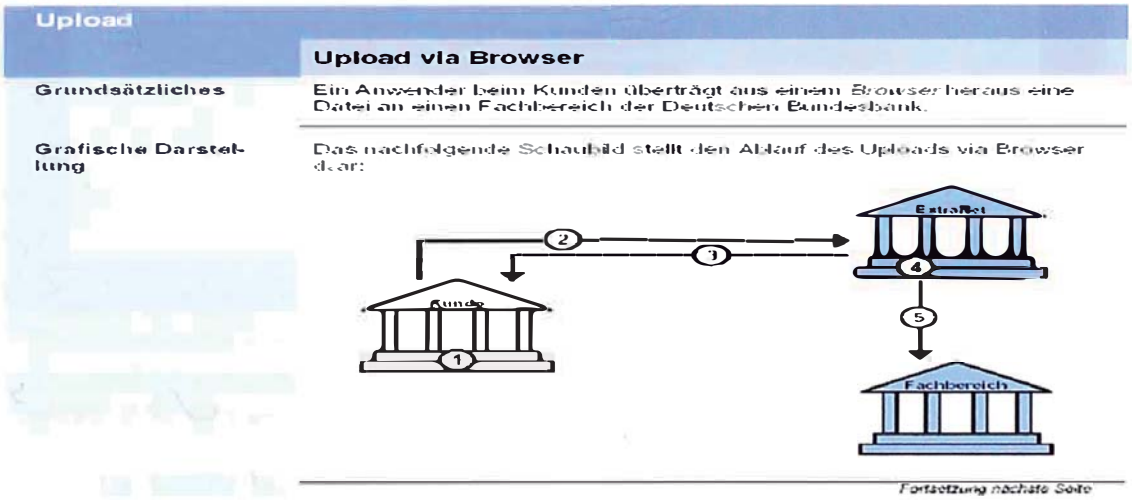
La DB ha construido una Extranet basada en la tecnología Internet que está disponible sólo en Alemania. Comenzó a operar el 2 de diciembre de 2002. Con este nuevo canal, la DB permite intercambiar datos e información con sus clientes de manera más rápida y segura.

Figura Nº 7: Extranet de Deutsche Bundesbank



Fuente: www.bundesbank.de/ , visitado el 03 de julio de 2003

Figura Nº 8: Esquema de operación Extranet Deutsche Bundesbank

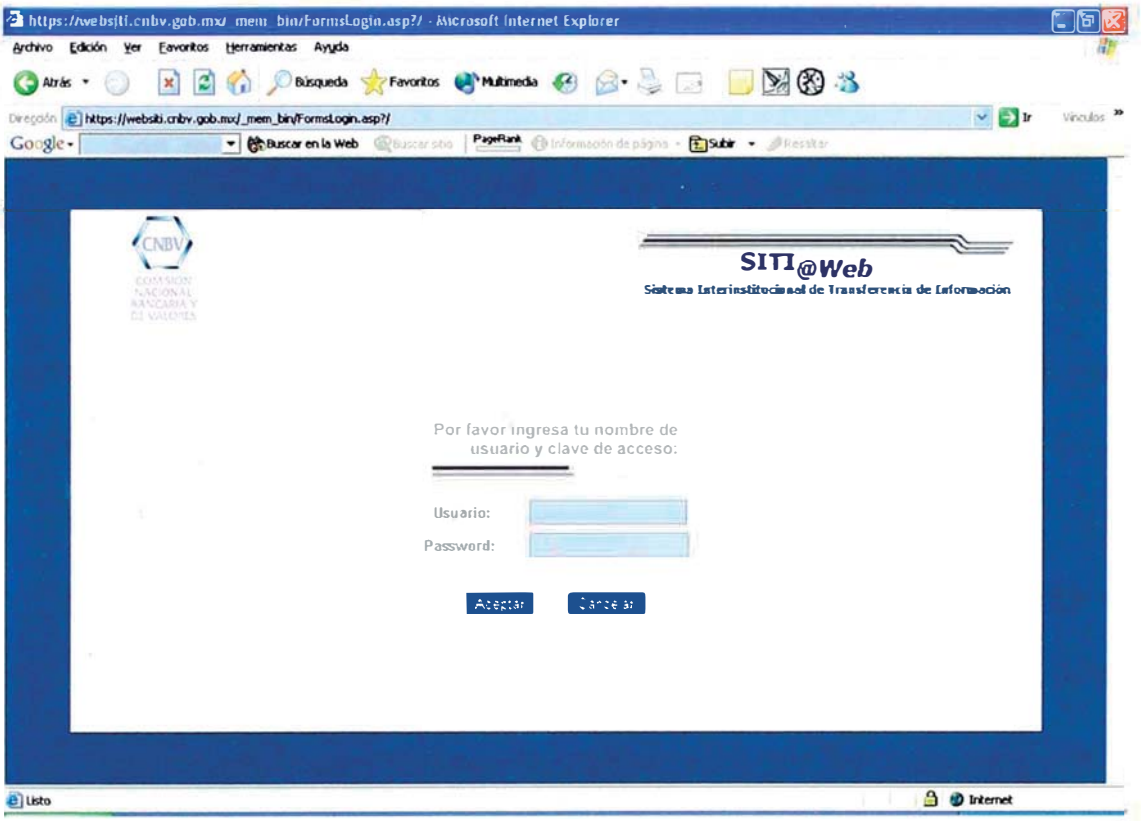


Fuente: Documentación Bundesbank Extranet

3.5.4 México

La Comisión Nacional Bancaria de Valores de México (CNBV) (http://www.cnbv.gob.mx/) tiene por objeto supervisar y regular, en el ámbito de su competencia, a las entidades financieras.

Figura Nº 9: SITI@Web de la Comisión Nacional Bancaria de México



https://websiti.cnbv.gob.mx/_mem_bin/FormsLogin.asp?/
visitado el 03 de Julio de 2003

La CNBV ha implementado el SITI@WEB, el cual es un sistema que usa la Internet para la recopilación de información de las instituciones del sistema financiero mexicano.

IV. MARCO TEÓRICO

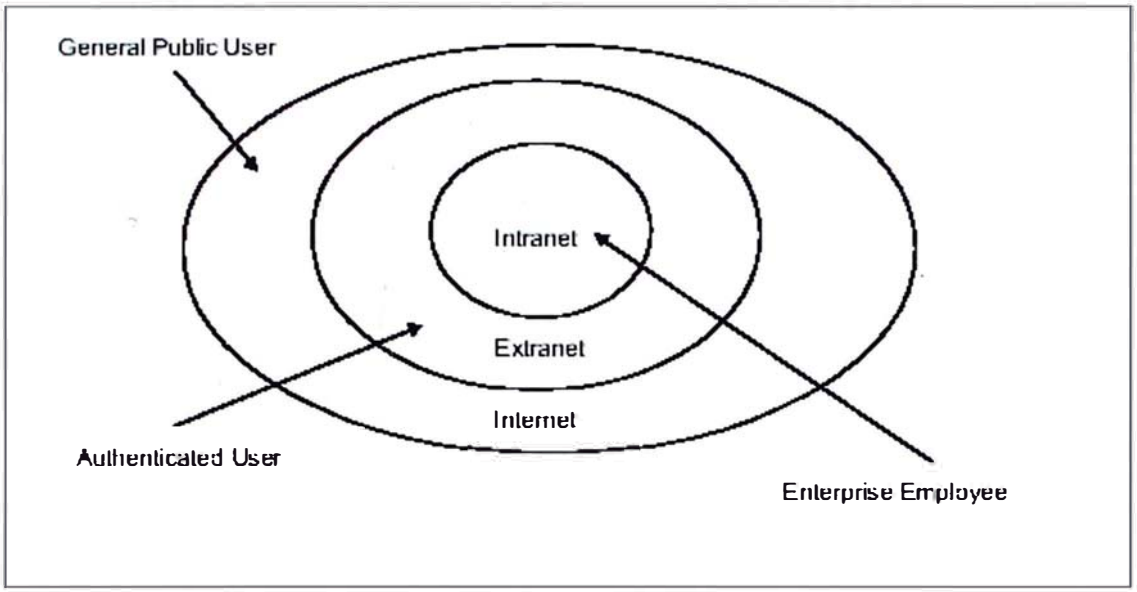
4.1 DEFINICIONES

4.1.1 Extranets

Son redes privadas que usan protocolos de Internet y la red pública de información para comunicarse con proveedores, vendedores, socios, clientes y otros negocios. Otra definición de una Extranet es: "La extensión de la Intranet de una empresa hacia fuera sobre la Internet, por ejemplo, para permitir a clientes seleccionados, proveedores y trabajadores móviles el acceder a datos privados de la empresa y aplicaciones vía la World Wide Web. Esto es en contraste, y usualmente en adición, al sitio Web de la empresa que es accesible a cualquier persona" (Ling and Yen, 2001, p. 40).

Las principales similitudes y diferencias entre Internet, Intranets y Extranets son presentadas en la Tabla Nº 1.

Figura Nº 10: Representación esquemática Internet, Intranet y Extranet



Fuente: The Ohio Department of Administrative Services

Tabla Nº 1: Similitudes y diferencias entre Internet, Intranets y Extranets

Características	Internet	Intranets	Extranets
¿Qué es?	Carretera de información	El uso de la tecnología Internet dentro de una organización	Una red que usa la Internet para mejorar las relaciones entre negocios
Acceso	Abierto	Privado	Sólo por acuerdo
Usuarios	Público	Miembros de la empresa	Socios de negocios
Información	General	Propietario	Selectivo

Fuente: Vlosky R, Blalock L, Fontenot R, p. 439, 2000

4.1.2 La Web (WWW)

La WWW (World Wide Web) es un sistema de documentos que contienen textos, gráficos y otros elementos multimedia accesibles mediante un visualizador.

4.1.3 Sitios Web

Son los lugares donde está la información que los interesados pueden acceder. Un sitio Web tiene tres componentes: Un programa Web Server que recibe pedidos de los clientes y les devuelve páginas, un conjunto de páginas Web, y programas para acceder a recursos que no son necesariamente de tecnología Web.

4.1.4 Visualizadores

También denominados navegadores o browsers, los cuales permiten a los usuarios ver documentos basados en Web. Los visualizadores son programas que leen archivos (normalmente de texto) y descifran las etiquetas de HTML.

Todos los navegadores recuperan información normalmente ubicada en computadoras remotas y descritas en forma semántica para luego componer y/o acomodar el texto, los gráficos y los elementos multimedia en la computadora del usuario. Los visualizadores comerciales más populares son *Netscape Navigator* e *Internet Explorer*.

4.1.5 URL (Uniform Resources Locator)

Es un sistema de direccionamiento en Web que define la ubicación exacta de un recurso en la red. La estructura básica de una URL es:

- Cómo (Protocolo. VB. http)
- //Quién (host)
- /Dónde (directorio)
- /Qué (recurso)

Ejemplo: http://www.sbs.gob.pe/capacitacion/mini_intro.es.htm

4.1.6 HTTP (HyperText Transfer Protocol)

Es un protocolo[5] a nivel de aplicación para sistemas de información distribuidos, colaborativos e hipermedios, que permite a un cliente enviar un requerimiento a un servidor y a su vez que el servidor envíe una respuesta.

4.2 VENTAJAS DE LAS EXTRANETS

4.2.1 Impacto en los negocios

Debido a las características de comunicación, las Extranets prometen tener un impacto significativo en construir, administrar y fortalecer las relaciones con los clientes (Ling and Yen, 2001).

La comunicación es un factor crítico en el entorno de la Extranet, que facilita la relación con otros negocios, intercambio de archivos y diferentes servicios.

Adicionalmente, la Extranet crea una oportunidad para personalizar la información disponible para cada persona que ingrese al sistema.

[5] Un protocolo es una serie de normas que definen cómo se remiten y reciben datos entre equipos.

El acceso global 24x7 permite una comunicación en tiempo real. Es de resaltar que desde que las Extranets son basadas en Web e interactivas, los clientes pueden buscar la información que desean y en el momento que la requieran.

4.2.2 Acceso disponible a la información

Acceso simplificado a muchos tipos de información. Una Extranet puede llegar a ser un vehículo ideal para la comunicación interna y externa. La información puede ser provista en una forma inmediata, efectiva, fácil de usar, rica en formato y versatilidad.

El intercambio de la información sobre la Extranet cuesta menos que intercambiarla a través de métodos antiguos como los faxes o correos de voz.

4.2.3 Libertad de elección

La tecnología Web está disponible a casi todas las plataformas de hardware y software.

4.2.4 Fácil de usar

El hipertexto (que permite buscar un sitio Web vía textos) es una de principales contribuciones que hace amigable el navegar por Internet.

4.2.5 Costo moderado

Dado que las Extranets usan la infraestructura de Internet existente, incluyendo servidores estándares, clientes e-mail y visualizadores Web, una

Extranet es más económica que crear y mantener una red propietaria, como por ejemplo la red tradicional de intercambios de datos (EDI).

4.2.6 Disminución de los costos al reemplazar medios tradicionales

El ahorro de costos es una principal motivación para la implementación de Extranets. El uso de esta herramienta haría disminuir la necesidad de utilizar otros medios más costosos como correo postal, teléfono, entre otros.

4.3 DESVENTAJAS DE LAS EXTRANETS

4.3.1 Falta de contacto personal

La Extranet no provee contacto personal (*face to face)*, aspecto que es considerado indispensable para algunas personas.

4.3.2 Problemas culturales

Los críticos argumentan que la Extranet es impersonal. Siempre en toda organización hay personas que resisten los cambios. Aún si el tiempo y el dinero son ahorrados, algunos empleados podrían tener una actitud diferente de la esperada.

4.3.3 Requerimiento de mayor seguridad

La seguridad es el principal asunto cuando se implementa una Extranet. Es difícil controlar quien accede al sistema, de donde y hacia donde. Las limitaciones de desempeño son la confiabilidad, escalabilidad y seguridad; es decir un mejor desempeño se va a ver limitado ante mayores mecanismos de seguridad y confiabilidad.

4.3.4 Costos de implementación (en caso no se disponga de una infraestructura Internet actual)

Si es que no se cuenta con infraestructura necesaria, como ocurre en empresas nuevas, se requerirá la adquisición de hardware, software, servicios de telecomunicaciones.

Los costos del hardware están asociados a la adquisición de servidores y computadoras, software y herramientas para integrar la Extranet con los sistemas existentes.

De otro lado, existen costos para cualquier empresa relacionados al entrenamiento de empleados para cambiar sus prácticas existentes del trabajo y entrenamiento de personal especializado para mantener la red. Asimismo, existen costos envueltos en el desarrollo y lanzamiento de la Extranet.

4.4 REQUERIMIENTOS DE SEGURIDAD EN EXTRANETS

4.4.1 ¿Por qué seguridad?

De acuerdo con una encuesta sobre seguridad y crimen informático efectuado por el CSI/FBI[6] en el año 2002, el 60% de las más grandes compañías y agencias de gobierno detectaron actividades no autorizadas en sus sistemas y muchas de ellas sufrieron pérdidas financieras, siendo los problemas más frecuentes virus de computadora (85%), abuso de acceso Internet (78%), robo de laptops (55%) y penetración del sistema (40%).

[6] Encuesta conducida por el *Computer Security Institute* (CSI) en asociación con el *San Francisco Computer Crime Squad* del *Federal Bureau of Investigation* (FBI)

Asimismo, dicho estudio revela que el 38% de las empresas encuestadas sufrió ataques en sus sitios Web en los últimos 12 meses (en algunos casos mientras efectuaba B2B o B2C), siendo los ataques más frecuentes: vandalismo (70%), *denial of service* (55%), robo de información (12%) y fraude financiero (6%).

4.4.2 Amenazas y Ataques

- Robo de claves.- El más fácil camino para entrar es por la puerta principal, por la ventana del *login*. Si lo usuarios establecen claves "pobres", éstas están expuestas a ser deducidas por los atacantes.
- Ingeniería social.- Técnicas para obtener claves con "engaño". Claves que pueden ser encontradas alrededor del terminal o escrita en documentos cerca del teclado y que pueden ser tomados por personas no autorizadas. Asimismo, personas no autorizadas a través del teléfono y con algo de "descaro" pueden conseguir las claves de acceso al sistema.
- Bugs and Back Doors.- Los *Back Doors* (puertas traseras) son programas o parte de programas que permiten el acceso no autorizado a un sistema. Algunas veces son insertados maliciosamente en los sistemas. Un *Bug* (insecto) es un defecto en un programa que causa algo inesperado (a menudo es destructivo).
- Fallas en la autenticación.
- Fallas en los protocolos de comunicación.

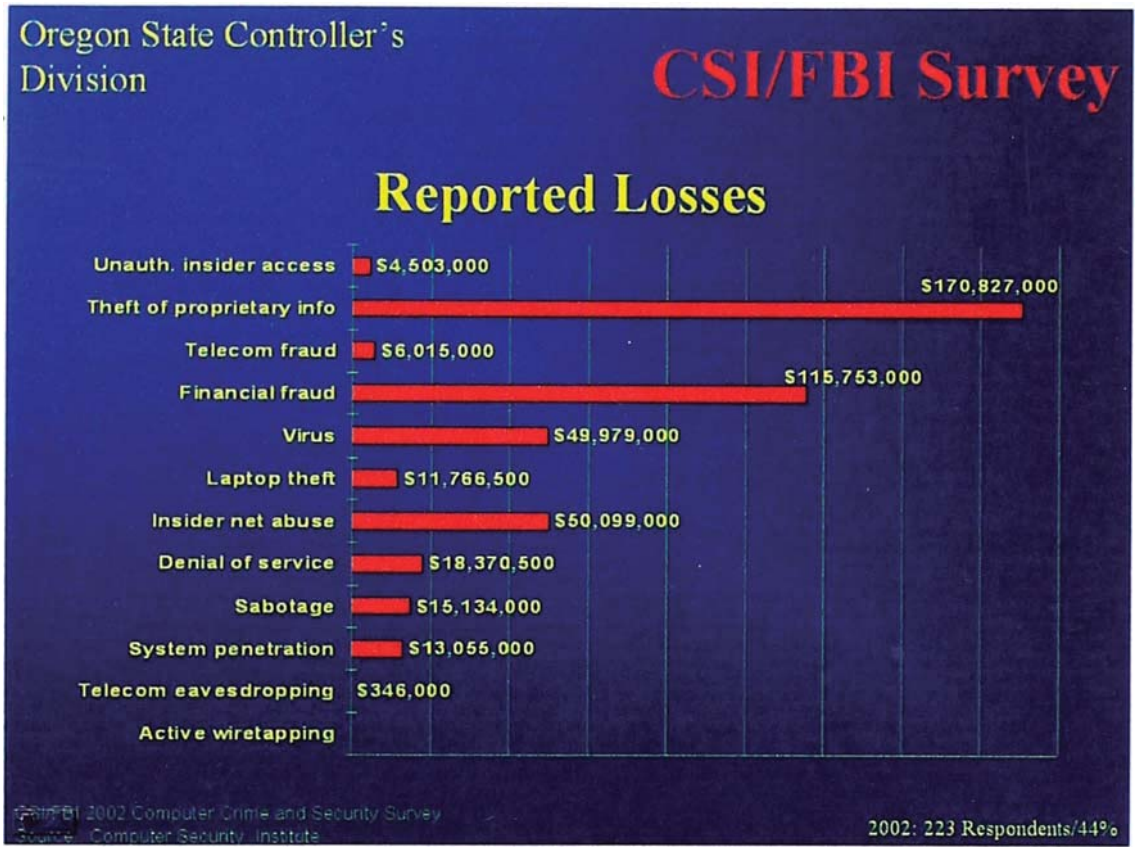
- Ataques exponenciales – *Virus y gusanos.*- Un virus es un programa destructivo que modifica otros programas insertando copias de sí mismo, en un esfuerzo por ocultar su existencia y propagarse en la red. Los gusanos son programas autoreplicables y autoiniciables, diseminables por ellos mismos de máquina en máquina a través de la red.
- Denial of Service.- Es el empleo excesivo de un servicio.
- Ataques activos.- En la literatura criptográfica existen dos tipos de atacantes. El primero es un adversario pasivo, quien puede escuchar a escondidas en toda la red de comunicaciones, con el objetivo de obtener la mayor información confidencial posible. El otro es el intruso activo, quien puede modificar mensajes, introducir paquetes en cada mensaje o borrar mensajes. El atacante puede también producir mensajes y enviarlo.

A modo referencial, se presenta en la Figura Nº 11, el promedio de pérdidas por ataques obtenido de una encuesta realizada en el año 2002 por el CSI/FBI.

4.4.3 Medidas para mitigar los riesgos en la implementación de las Extranets

Para mitigar estos riesgos, deben identificarse e implementarse las medidas de seguridad que protejan la conexión Extranet a través de todo su ciclo de vida. El ciclo de vida de la Extranet involucra el planeamiento, implementación y mantenimiento de la conexión.

Figura Nº 11: Promedio de pérdidas por varios tipos de ataques



Existe una variedad de técnicas disponibles para contrarrestar las amenazas y ataques a las Extranets. Antes de elegir una tecnología en particular, es importante entender el amplio rango de aspectos sobre la seguridad que debe tener cualquier sistema:

Tabla Nº 2: Características de un sistema seguro

Servicios de seguridad	Definición	Algunos mecanismos de control
Autenticación	Prueba o garantía de la identidad de quien envía la información	Usuario-Clave Tarjeta Inteligente Huella Digital
Control de Acceso	Permisos diferenciados de acceso a segmentos y necesidades especificas por cliente	Perfiles de usuario
Confidencialidad	Garantía de que el contenido de la información se mantiene	Algoritmos de encriptación

	oculto salvo para el destinatario	
Integridad	Garantía de que el contenido del mensaje no sufrió ninguna modificación	Algoritmos de encriptación
No repudiación	Inhabilidad de un individuo para desconocer una transacción una vez realizada	Algoritmos de encriptación

Fuente: La firma electrónica y las entidades de certificación por REYES Krafft.

La arquitectura técnica básica para asegurar una Extranet debe incluir las siguientes acciones:

4.4.3.1 Autenticación del usuario

La **autenticación** es el proceso de comprobar la identidad de alguien. Es distinta a la declaración de identidad (conocido y razonable: identificación) y distinta a decidir que privilegios dar a la identidad (autorización). Mientras que los tres son importantes, la autenticación es la más difícil desde la perspectiva de la seguridad de red.

La autenticación esta basada en uno, dos o tres factores:

- Algo que usted conoce
- Algo que usted tiene
- Algo que usted es

El primer factor incluye passwords, PINs y similares. El segundo incluye tarjetas bancarias y dispositivos de autenticación. El tercero se refiere a atributos biológicos del usuario. Las soluciones de autenticación pueden proveer uno, dos o los tres factores de autenticación. La mayoría de aplicaciones simples usa el más simple factor de autenticación. **Las más importantes requieren como mínimo dos.**

Tabla Nº 3: Tipos de autenticación y sus apropiados usos

Tipo de Autenticación	Uso apropiado
Passwords	Aplicaciones para toda la población
Passwords para cada sesión	Empleados o socios Extranet
Certificados digitales	Empleados, más un limitado número de socios de la Extranet
Personal identification number (PIN) tokens	Empleados más un muy limitado número de socios Extranet muy importantes
Smart Cards	Empleados más un muy limitado número de de socios Extranet muy importantes
Biometría	Un conjunto de empleados. Debería ser usado en conjunto con otro tipo de autenticación.

Fuente: Giga Information Group

En la Figura Nº 12 se puede apreciar la relación entre la confidencialidad que ofrece cada tipo de autenticación, costo de implementación y facilidad de uso.

4.4.3.2 Autorización del usuario

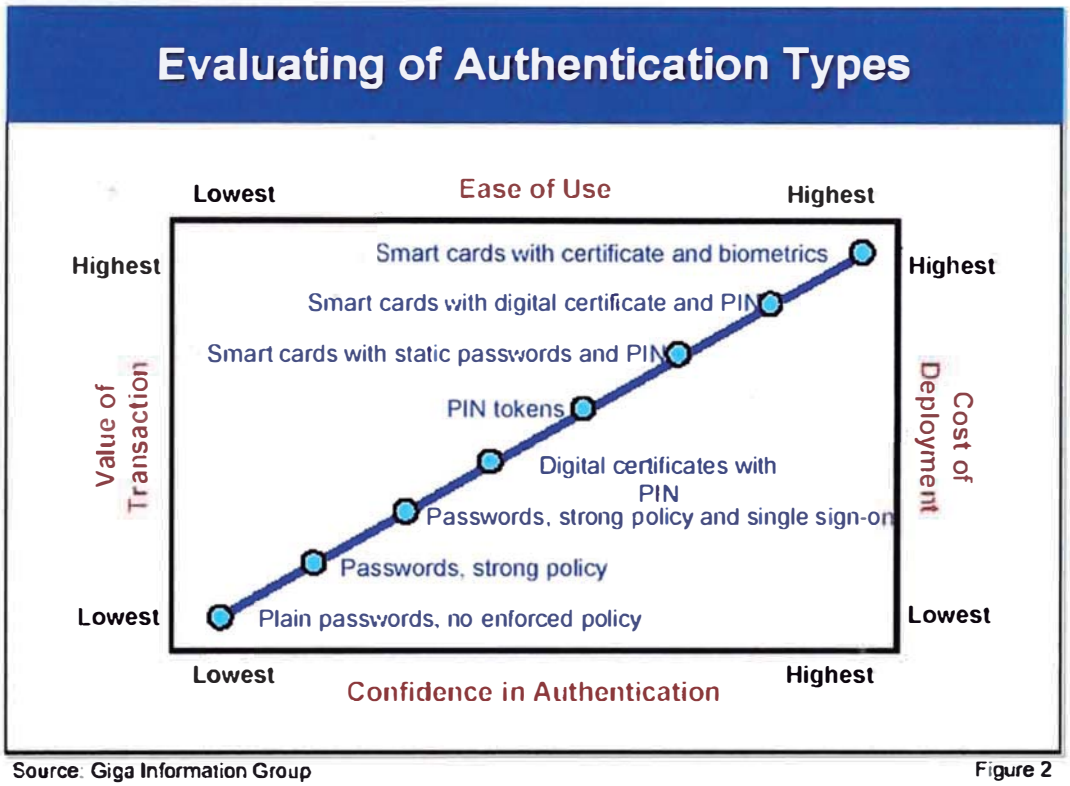
Asegurando la sesión

El SSL (*The Secure Socket Layer*) es el estándar para las transacciones seguras en la Web. La IETF[7] adoptó el protocolo y lo nombró el protocolo *Transport Layer Security* (TLS).

Existen dos propósitos para este protocolo. El primero es proveer un canal confidencial entre un *browser* y el servidor Web. El segundo es autenticar el servidor, y posiblemente al cliente. Ahora bien, autenticar al cliente no es muy común, pero esto debería cambiar en un futuro cercano, en particular para las aplicaciones de Intranet/Extranet.

[7] Internet Engineering Task Force

Figura Nº 12: Evaluación de los tipos de autenticación



Source: Giga Information Group Figure 2

Algunas transacciones podrían ser hechas sin controles de acceso adicionales. Existe información en la Web cuyo contenido no incluye información privada o sensitiva. Algunas transacciones incluyen datos con valor sólo por unos cuantos segundos, en cuyo caso, la necesidad de seguridad de sesión es mínima.

Para asegurar la confidencialidad de los datos como mínimo por algunos minutos o quizás unas horas, el estándar de implementación es de 48 bit SSL. El estándar SSL sólo requiere un certificado en el servidor Web.

Una forma más fuerte para implementar el SSL es distribuyendo certificados digitales a todos los usuarios para establecer mutuamente una

autenticación SSL. Asimismo, si se realiza transacciones monetarias o modificación de información se recomienda como mínimo 128 bit SSL.

Tabla Nº 4: Métodos apropiados de asegurar la sesión

Método	Uso apropiado
Sólo texto	Apropiado para información pública y de bajo riesgo
48-bit SSL	Apropiado para información privada de bajo valor
128-bit SSL	Transacciones financieras, datos de cuidado de salud, datos de algunos recursos humanos, contratos y documentos legales
Autenticación mutua (high bit SSL)	Moderado a alto valor de los datos compartidos entre dos partes con alguna frecuencia
Site-to-site VPNs	Recomendado para transferencias de datos de alto valor entre socios de negocios
Punto a punto VPNs	Recomendado para muy datos muy sensitivos que nunca deberían ser desencriptados durante el tránsito

Fuente: Giga Information Group

4.4.3.3 Proteger el contenido de las páginas [8]

Las aplicaciones Web tienen vulnerabilidades nativas, esto es, la naturaleza de los protocolos Web (HTTP) y los lenguajes de los browsers (HTML, CGI, Java).

Desarrollar código de aplicación con control de acceso es útil, pero no es completo. La integridad de los datos a ser vistos en el sitio Web sólo puede ser garantizada por un Proxy. Por ejemplo **Sanctum** tiene el producto AppShield, un *proxy* útil diseñado para eliminar todos los contenidos comunes que son *hackeados*. Otros vendedores en esta categoría incluyen a Gilian, ClickNet (ahora Entercept Security Technologies)

[8] Tomado del articulo *Optimal Extranet Security* de Giga Information Group (www.gigaWeb.com)

y Qiave (adquirido por WatchGuard en el 2000). Qiave es un útil método para limitar los datos a sólo lectura. Gilian y ClickNet tiene deficiencias de acuerdo con las recomendaciones del Giga Information Group.

4.4.3.4 Fortalecer(hardening) el sistema operativo del servidor Web

Después de proteger el contenido de la Web, asegurar el sistema operativo elimina riesgos innecesarios relacionados a la violación del sistema operativo. Por ejemplo, los *hackers* podrían instalar un software *Trojan Horse* y lanzar ataques a la red y a los datos mientras se oculta bajo el sistema operativo.

El Giga Information Group recomienda aplicar *hardening* y técnicas de separación para cada servidor de aplicación.

4.4.3.5 Asegurar la línea entre el Servidor Web y la base de datos

Durante una transacción Web podría requerirse una consulta a otro sistema interno, una base de datos, otro servidor, etc. Entonces se recomienda que la conexión cruce la red en forma limitada: desde una zona desmilitarizada (DMZ)[9] hasta la red destino. En este caso se deben requerir autorizaciones intermedias que permitan la conexión.

4.4.3.6 Implementar controles apropiados de acceso a la base de datos

Se debe trabajar con el equipo que soporta las aplicaciones para asegurar que las conexiones desde la zona desmilitarizada (DMZ) no excedan los privilegios apropiados.

---

[9] DMZ — Zona desmilitarizada. Una expresión de networking que implica segregación, red separada por firewalls donde usuarios externos tienen accesos limitados

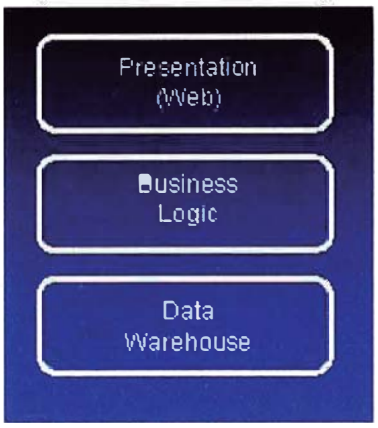
4.5 TECNOLOGÍAS PARA DESARROLLAR UNA EXTRANET

4.5.1 Arquitectura de desarrollo

Para desarrollar una Extranet se requiere como mínimo el uso de una arquitectura de tres niveles (modelo 3-tier). Este modelo separa y define claramente (1) Presentación Web, (2) Lógica de negocios, y (3) Almacén de datos.

4.5.1.1 Diagrama conceptual

Figura Nº 13: Modelo 3-tier



Primer nivel.- La capa de presentación Web (*Web Presentation*) soporta sólo las aplicaciones Web puras. Esto provee un valor añadido de reducir el entrenamiento para la integración rápida de nuevas aplicaciones y capacidad de proveer servicios a través de la Internet.

Segundo nivel.- La capa de la lógica de negocios (*Business Logic*) es un cambio de proveer aplicaciones individuales de software a proveer negocios automatizados. Un buen ejemplo es la automatización del ruteo y aprobación de documentos (lógica de negocios) que puede ser presentada a

los empleados como un sistema de requerimientos, sistema de vouchers de viajes o un sistema de requerimientos de control.

Tercer nivel.- La capa de almacén de datos (*Data Warehouse*) cambia la aproximación de usar múltiples bases de datos de la organización (empleados, activos, base de datos de proyectos financieros) a una arquitectura de un almacén central de datos.

4.5.2 Software estándar de desarrollo

Tabla Nº 5: Arquitectura estándar de desarrollo

	Estándares	**Herramientas**	**Uso**
Presentación	HTML XML	HomeSite Dreamweaver	Web page prototyping
Lógica negocios	EJB 1.1 Java 2 EE JDBC 2.0 JSP 1.2 Servlet 2.3	Orion	Integrated Web server, Servlet server, and EJB server
Desarrollo		CVS Kawa	Version Control IDE/Code Editor
Diseño	UML	StructureBuilder TogetherJ	Object modeling Object model prototyping
Almacén datos	SQL-92	PostgreSQL, Interbase, Oracle	Relational database server

4.6 EL GOBIERNO Y EL COMERCIO ELECTRÓNICO

4.6.1 E-Goverment (e-Gov)

E-Goverment se puede definir como el gobierno interconectado entre sus sistemas de información, que integra la tecnología de información y las

comunicaciones más recientes que han evolucionado de la mano de Internet, que abre sus procesos y servicios a todos los ciudadanos vía la World Wide Web.

Me refiero a la puesta en Internet de la información, y todos los procesos o gestiones posibles que se realizan día a día en las oficinas del gobierno, de manera que estas se puedan solventar desde una computadora en cualquier parte que tengamos acceso a la Internet

Cabe indicar que los gobiernos de los países más innovadores como los que conforman el G-8, están introduciendo todas las facilidades que proporcionan estos avances acelerados de la tecnología de la información propiciada por la Internet, como una iniciativa más para incrementar el acceso de los ciudadanos a los servicios del gobierno, esta iniciativa la desarrollan como uno de los programas estratégicos de Gobierno. Lo que pretenden es que los ciudadanos puedan acceder a los sistemas del gobierno desde su casa u oficina, sin mayores esfuerzos para obtener la información o realizar sus trámites, por supuesto, sin tener que esperar en largas y lentas filas, en las oficinas de gobierno rebalsadas. Para facilitar estos nuevos servicios, el gobierno debe establecer toda una estrategia impulsada desde los niveles más altos, clara y bien definida, con sus propósitos, estructura organizacional y fondos para su desarrollo.

El gobierno digital representa una alternativa real para **reducir la burocracia**, **incrementar la efectividad**, **ahorrar los gastos estatales**,

reducir los tiempos y para **obtener la información vital** para el desarrollo del país.

4.6.2 Goverment to Business (G2B)

El G2B es una categoría de comercio electrónico en la que se encuentran todas las transacciones que se realizan entre las compañías y las diferentes organizaciones gubernamentales.

En esta categoría podríamos ubicar la Extranet entre un organismo público como la SBS y las empresas del sistema financiero.

Figura Nº 14: e-Gov y G2B

e-Gov	Ciudadanos	Organismo Estatal	Negocios	Organización Sin fin lucro
Ciudadanos	C2C	C2G	C2B	C2N
Organismo Estatal	G2C	G2G	G2B	G2N
Negocios	B2C	B2G	B2B	B2N
Organización Sin fin lucro	N2C	N2G	N2B	N2N

4.7 METODOLOGÍA DE DESARROLLO DE SOLUCIONES DEL *DOE*

El Departamento de Energía de los Estados Unidos (DOE) ha emitido la versión 3 de su Metodología de Ingeniería de Sistemas (SEM en sus siglas en inglés) en Setiembre 2002. Esta guía ayuda a implementar

sistemas de información, administrar proyectos y asegurar la calidad de las prácticas y procedimientos utilizados.

Su propósito principal es promover el desarrollo confiable y a un costo efectivo de soluciones basadas en computadoras mientras se hace un uso eficiente de los recursos. Asimismo, la metodología ayuda al seguimiento, control y documentación del proyecto.

El SEM ha considerado los principios y estándares de los líderes de la industria en sistemas de información, como *The Institute of Electrical and Electronics Engineers* (IEEE) y *The Carnegie Mellon Software Engineering Institute* (SEI).

El aseguramiento de calidad está integrado en esta metodología, haciendo responsable de la calidad a todos los miembros del proyecto. Para asegurar el desarrollo de productos de calidad, la metodología prescribe revisiones, inspecciones y auditorías durante el ciclo de vida del proyecto. Para proteger la integridad de los sistemas de información, la metodología también prescribe controles sobre los componentes del sistema, datos y documentación técnica.

La metodología circunscribe todos los aspectos del ciclo de vida de un proyecto de sistemas de información, desde el planeamiento del proyecto hasta la puesta en producción y mantenimiento.

Figura Nº 15: Ciclo de vida de los sistemas de información

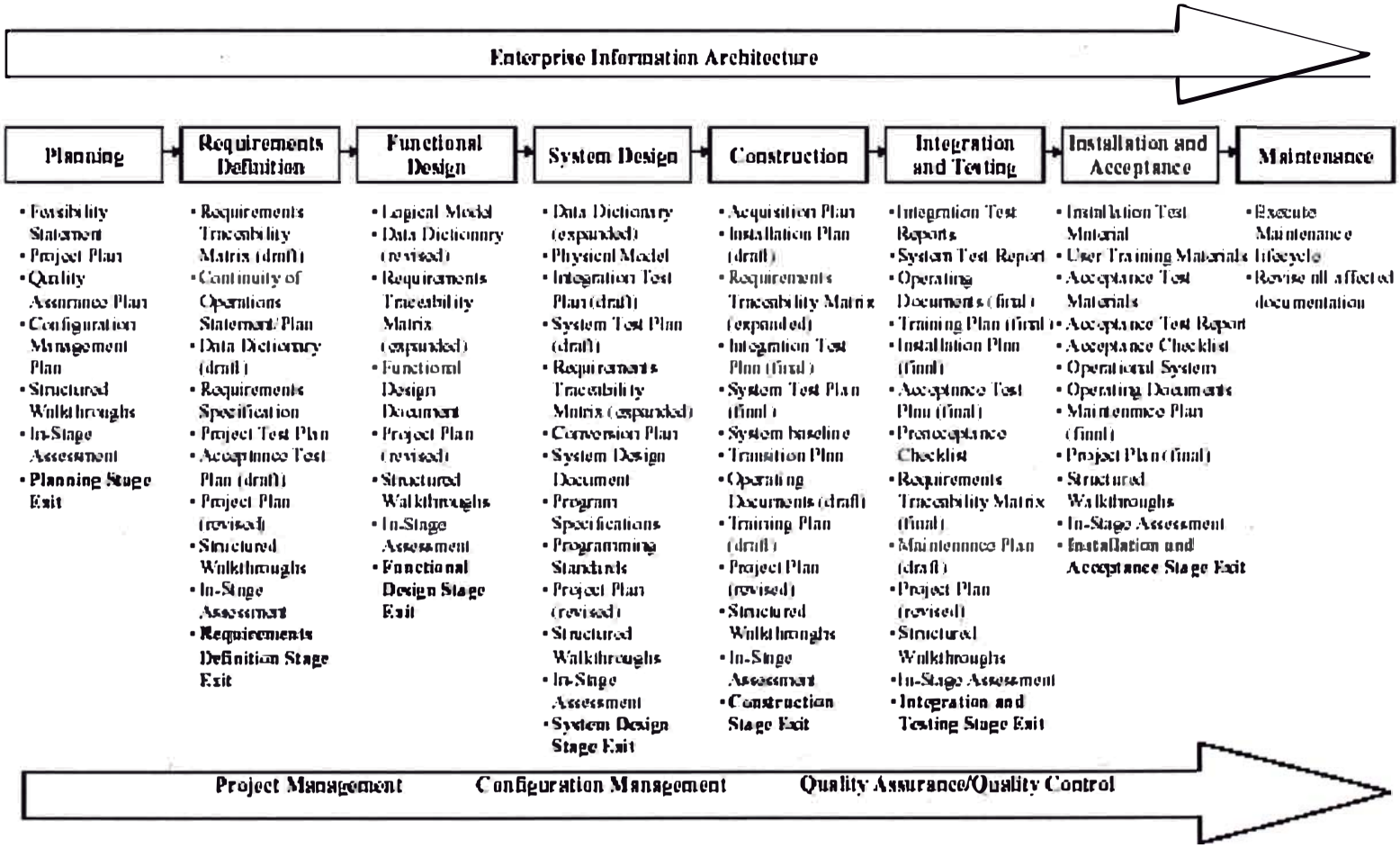
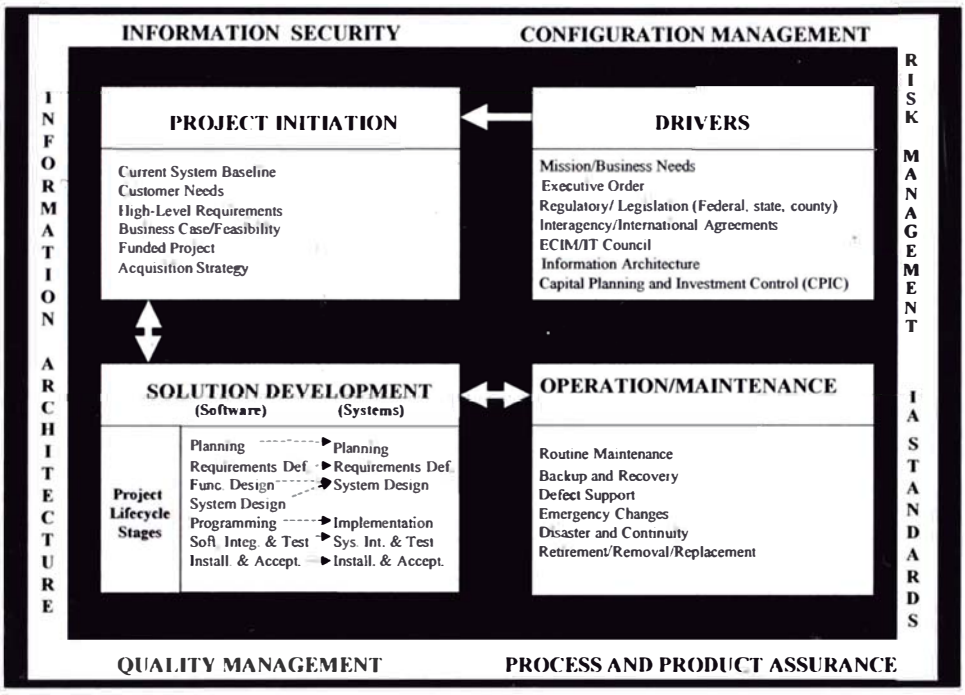


Figura Nº 16: Ciclo de vida para la solución de sistemas información



Fuente: http://cio.doe.gov/ITReform/sqse/

V. PROCESO DE TOMA DE DECISIONES

5.1 ALTERNATIVAS DE SOLUCIÓN

Dada la problemática descrita en el capítulo 3 (descripción del problema) se tienen las siguientes alternativas: Mantener la operatividad actual o desarrollar una Extranet que utilice el canal de Internet.

Cabe indicar que la alternativa de desarrollar un canal con una red propietaria (sin usar la Internet) ha sido descartada por su alto costo y su inviabilidad de ser implementarla en la gran diversidad de empresas que supervisa la SBS.

De otro lado no se ha efectuado un análisis de alternativas referidas a personalizar una solución existente, desarrollo con terceros o con recursos propios, dado que ya se han iniciado trabajos con personal de la SBS en la construcción de la infraestructura de la Extranet. De acuerdo con la información brindada por el Área de Sistemas de la SBS, se ha previsto iniciar el desarrollo de los servicios a mediados del segundo semestre de este año.

5.1.1 Mantener la situación actual (Status Quo)

Mantener la operatividad tal como se encuentra ahora. Los nuevos requerimientos serán efectuados progresivamente en forma manual, semiautomática o con el uso de la tecnología existente.

5.1.2 Desarrollar una Extranet

Crear un sitio Web privado y seguro (comúnmente llamado Extranet) entre la SBS y las empresas del sistema financiero con el objetivo de brindar servicios e intercambiar información.

Esta alternativa no considera aún la relación con las empresas supervisadas de seguros y AFPs, supervisores nacionales o extranjeros o instituciones públicas.

5.1.2.1 Algunos servicios a brindar por este canal a las empresas del sistema financiero

- Herramientas de análisis para que las empresas analicen su desempeño desde una perspectiva de competitividad y rentabilidad.
- Regulación (nuevas normas emitidas, proyectos de normas SBS con su informe de sustento correspondiente, foro de consultas)
- Directorio de la SBS para ayudar a identificar a los responsables específicos por cada área.
- Estudios económicos.
- Información sobre la administración de riesgos (Riesgo de crédito, Riesgo de mercado, Riesgo de liquidez, Riesgo de Operación).

- Comunicaciones para enviar y recibir mensajes seguros a / desde la Superintendencia, para que puedan formular consultas y, apreciar consultas realizadas y consultas frecuentes; asimismo, podrán incluirse presentaciones en línea, chats en línea y video conferencias.
- Estado de los documentos enviados a la SBS (usando como proveedor el sistema de trámite documentario).
- Estadísticas de cumplimiento de envío de reportes y anexos del manual de contabilidad.
- Envío de solicitudes para abrir nuevas agencias o reubicar otras agencias electrónicamente.

5.1.2.2 Obtención de información por medio de este canal

- Información de las observaciones de auditoría y unidades de riesgo.
- Información de accionistas, directores y gerentes.
- Información de manuales de la empresa supervisada, evaluaciones, y otros documentos que interesa analizar.
- Anexos y reportes del manual de contabilidad en reemplazo del Sucave[10].
- Información requerida por alguna circular, oficio múltiple, oficio, etc.

5.2 METODOLOGÍA DE SOLUCIÓN

El presente trabajo utiliza la metodología de desarrollo e implementación de soluciones del DOE[11] para definir los requerimientos y

[10] Submódulo de Captura y Validación externa para el envío de anexos y reportes del manual de contabilidad de las empresas supervisadas a la SBS.

elaborar el diseño funcional de la solución propuesta. Asimismo, presenta más adelante un cronograma estimado de las actividades para la implementación de la solución de acuerdo a la metodología señalada.

5.3 TOMA DE DECISIONES

A continuación se presenta el análisis costo de beneficio (ABC)[12] de la solución propuesta:

5.3.1 Objetivos y supuestos

Objetivos

- Brindar servicios e información de utilidad a las empresas supervisadas en forma rápida, oportuna y segura.
- Obtener información para las labores de supervisión en forma segura y rápida.

Suposiciones

- El ciclo de vida de la solución propuesta es 5 años. En dicho punto se evaluaría otros mecanismos de comunicación.
- El período de comparación es el mismo que el ciclo de vida asumido (5 años) comenzando en el 2004 (año 0).
- El sistema estará en producción en el segundo semestre del año 2004. Luego se efectuará un piloto por 3 meses con algunas entidades supervisadas.

---

[11] *Department of Energy USA*
[12] Se ha utilizado el *Analysis of Benefits and Costs (ABC's) Guideline* del *U.S. Department of Energy*

- Los beneficios y los costos recurrentes estimados serán constantes durante el período de comparación.

5.3.2 Análisis de beneficios

Pueden ser organizados en dos categorías: cuantificables y no-cuantificables. Los beneficios cuantificables representan ahorros monetarios a través de evitar o reducir costos. Los beneficios no cuantificables podrían agruparse por ejemplo en mejorar la imagen de la empresa ante sus clientes, mejorar la eficiencia de las operaciones, mejorar el estado emocional de sus empleados o incrementar su eficiencia.

Beneficios cuantificables

- Reducción de costos en el uso del teléfono y costos de personal ya que algunas actividades se automatizarán.
- Reducción de costos en correo postal, uso de papel e impresión.
- Reducción del tiempo dedicado a actividades operativas y repetitivas por parte de los analistas encargados de la supervisión, para dedicar más tiempo a labores de análisis.

Beneficios no cuantificables

- Mejora de la imagen de la SBS ante el sistema financiero supervisado.
- Mejora de la eficiencia de las operaciones.
- Simplificación de los procesos administrativos.
- Mejora de las comunicaciones entre SBS y supervisados.

Estimación de beneficios cuantificables

- **Datos preliminares**

Sistema financiero

A mediados del año 2003, el sistema financiero peruano estaba compuesto de la siguiente manera:

Tabla Nº 6: Sistema financiero peruano

	Número de empresas
Empresas bancarias	**17**
Empresas financieras	**6**
Empresas de arrendamiento financiero	**6**
Instituciones microfinancieras no bancarias	**40**
Cajas municipales (CM)	14
Cajas rurales de ahorro y crédito (CRAC)	12
Entidades de desarrollo de la pequeña y microempresa (EDPYME)	14
Almacenes generales de depósito	**6**
Cooperativas (Fenacrep)	**1**
Empresas de transporte, custodia y admin. Numerario	**2**
Empresas de transferencia de fondos	**14**
Empresas afianzadoras y de garantías	**1**
SISTEMA FINANCIERO	**93**

Fuente: www.sbs.gob.pe visitado el 29.06.2003

Adicionalmente, la Superintendencia tiene a su cargo las empresas en liquidación, las cuales también son sometidas a supervisión.

Tabla Nº 7: Empresas en liquidación

	Número de empresas
Liquidaciones bajo supervisión directa de la SBS	**9**
Supervisión delegada a la comisión administradora de carteras	**18**
Liquidaciones judiciales	**1**
EMPRESAS EN LIQUIDACIÓN	**28**

Fuente: www.sbs.gob.pe visitado el 29.06.2003

Se puede concluir, de la información de las Tablas Nº 6 y 7, que las empresas bajo supervisión directa de la SBS son 102 (93 activas y 9 liquidaciones)

Personal de la SBS

La Superintendencia Adjunta de Banca (SAB) contaba al 31.12 2002 con 98 analistas encargados de la supervisión del sistema financiero.

Para fines de la estimación y tomando como referencia la información de la Tabla Nº 8, se asumirá que el sueldo bruto en promedio que percibe cada analista de la SAB es S/. 8 815.23.

Tabla Nº 8: Sueldo bruto por categorías

Categoría	N°	Monto (S/.)
P1	37	13 077.62
P2	51	10 297.17
P3	90	8 161.65
P4	71	6 357.97
	249	
PROMEDIO	**8,815.23**	

Fuente: www.sbs.gob.pe visitado el 29.06.2003

- **Estimación de beneficios**

  Reducción del tiempo que dedican los analistas a labores operativas y/o rutinarias

  98 analistas para 102 empresas. Actualmente, los analistas dedican tiempo en pedir información, efectuar análisis que tal vez ya han sido hechos por otros analistas, atender consultas repetitivas de las empresas supervisadas, entre otras tareas.

Considerando el sueldo bruto mensual que percibe cada analista (S/. 8815.23) y que su jornada diaria efectiva es de 8 ¼ horas diarias (8:30 a.m. 5:30 p.m. con 45 minutos de refrigerio), se deduce que diariamente percibe S/. 419.77 (de 21 días efectivos en un mes) y por hora efectiva S/. 50.88.

Asumiendo que con la ayuda de la Extranet se **reduzca 20 minutos** diarios de los analistas en labores operativas (para destinarlas a labores de análisis), los minutos "ahorrados" en relación con sus ingresos representarán anualmente:

S/.25.44 x 21dias x 98 analistas x 12 = S/. 418 844.16 por cada año (1)

(1) Solo para efectos de cuantificar potencial beneficio de la Extranet y que ello redunde en que los analistas puedan dedicar mayor tiempo a las labores de análisis de las empresas supervisadas.

Reducción costo llamadas

Ahorro de una llamada mensual de 5 minutos (S/.0.50) a cada empresa supervisada por usar mecanismo de comunicaciones de Extranet. Mensualmente S/. 51, al año S/.612.

Ahorro de una llamada cada trimestre de 5 minutos por empresa para actualizar información de accionistas y directores. Al año S/. 204.

Ahorro de una llamada cada trimestre de 5 minutos por empresa para actualizar información de conglomerados financieros. Al año S/. 204.

Reducción costos correo Postal

Ahorro de un oficio de respuesta a consultas de una empresa cada tres meses. Cuatro oficios por año por cada empresa, 408 oficios por año. Aproximadamente S/. 1600 (Fuente: SERPOST).

Reducción costos personal

- Reducción de la carga de personal dedicado a mantener y preparar nuevas versiones de instalación del Sucave. Una persona con sueldo mensual de S/. 3 500, al año S/. 42 000.
- Ahorro de carga personal para organizar manuales. Una persona con un sueldo mensual de S/. 1500 mensual, S/. 18 000 anual.
- Reducción carga laboral en trámite documentario. Una persona con un sueldo mensual de S/. 1 500 mensual, S/. 18000 anual.

Tabla Nº 9: Resumen de beneficios cuantificables

Beneficios	Monto referencial
Reducción del tiempo de los analistas que dedican a labores operativas y/o rutinarias	S/. 418 844.16
Reducción costo de llamadas	S/. 1 020.00
Reducción correo postal	S/. 1 600.00
Reducción costos recursos humanos	S/. 78 000.00
TOTAL	**S/. 499 464.16**

Asignando valores a los beneficios no cuantificables

Paso 1 Definiendo Beneficios

Reducción costos teléfono, personal	- Cuantificable
Reducción costos correo postal, papel	- Cuantificable
Reducción tiempo de analistas en labores rut.	- Cuantificable
Mejora imagen SBS	- No-cuantificable
Simplificar procesos administrativos	- No- cuantificable
Mejorar eficiencia operaciones	- No- cuantificable

Mejorar comunicación SBS y supervisados - No- cuantificable

Paso 2 Rango de beneficios

1. Mejora imagen y servicio de la SBS
2. Mejorar comunicación entre SBS y supervisados
3. Reducción tiempo de analistas en labores rutinarias para hacer más labores de análisis
4. Reducción costos teléfono, personal, simplificación tramites
5. Reducción costos correo postal, papel
6. Mejorar eficiencia operaciones

Paso 3 Beneficios cuantitativos (anual)

Reducción tiempo de analistas en labores rutinaria	S/. 418 844.16
Reducción costos personal	S/. 78 000.00
Reducción costos correo postal	S/. 1 600.00
Reducción costos teléfono	S/. 1 200.00

Paso 4 Asignando valores a beneficios no-cuantificables (anual)

Mejora imagen y servicio de la SBS y comunicación entre SBS y supervisado[13]	S/. 418 844.16
Reducción tiempo de analistas en labores rutinaria	S/. 418 844.16
Reducción costos personal	S/. 78 000.00
Reducción costos correo postal	S/. 1 600.00
Reducción costos teléfono	S/. 1 200.00
Total x año	S/. 918 488.32

[13] Como parte de una de las técnicas del ABC y considerando que la mejora de imagen y otros intangibles son tan importantes como reducción de tiempo dedicado a labores operativas se asigna el mismo monto estimado.

5.3.3 Análisis de costos

Costos hundidos

Costos que no se incluyen en el análisis ABC, tales como los costos de la infraestructura tecnológica: servidores, firewall, software de desarrollo, herramientas para proteger a la red de ataques - adquiridos o en proceso de implementación en la SBS.

Costos no recurrentes

Son los gastos que se hacen por única vez para el diseño, programación e implementación del nuevo sistema, entrenamiento inicial a los usuarios, entre otros.

Proyecto mediano de seis meses

- 1 Jefe de proyecto (S/.10 000 mensual)
- 3 personas especialistas en sistemas (3 x 7 000 = S/.21 000 mensual)
- 2 analistas funcionales (2 x 8 000 = S/. 16 000 mensual)
- 1 analista de control calidad (1 x 7 000 = S/. 7 000 mensual)

Total costo mensual = S/. 54 000.

Total costo por la duración del proyecto = S/. 324 000 (6 meses)

Entrenamiento inicial

- 109 usuarios en la Superintendencia Adjunta de Banca (98 analistas y 11 intendentes). Costo de entrenamiento por cada participante de S/. 500. Un costo total de S/. 54 500.
- 102 empresas supervisadas. Costo estimado de S/. 500 por cada empresa supervisada. Un costo total de S/. 51 000.

Conducir una evaluación de riesgos a la arquitectura soporta de la Extranet

- Contratar una consultoría. Costo estimado de S/. 17 500 (US$5000).

Auditoría a la Extranet

- Contratar una consultoría. Costo estimado de S/. 17 500 (US$5000).

Costos Recurrentes

Son los gastos corrientes de operación del sistema. Estos costos son incurridos a través del ciclo de comparación. Se ha identificado los siguientes costos recurrentes:

- Entrenamiento de personal nuevo

20 usuarios por año a S/. 500 cada uno. Un total de S/. 10 000 por año.

- Entrenamiento de nuevas empresas

5 empresas nuevas cada año a S/. 500 cada una. Un total de S/. 2 500 por año.

- Soporte del sistema

Mantenimiento y operación del sistema. Dos personas encargadas de soportar plataforma Web permanentemente. Un total S/.5 000 mensual cada uno y en total S/. 120 000 por año.

5.3.4 Comparación de alternativas

Total beneficios al año = S/. 918 488.32

Total costos recurrentes al año = S/. 132 500

Tota costos no recurrentes (una vez) = S/. 464 500

Tabla Nº 10: Valor Presente Neto (En miles de nuevos S/.)

	Años					Tasa Descuento 15%	
	0	1	2	3	4	Total	Valor Presente
Costos	465.0	132.5	132.5	132.5	132.5	995	843
Beneficios	0.0	918.5	918.5	918.5	918.5	3 674	2 622
						Valor Presente Neto	**1 779**
						Tasa Interna Retorno (TIR)	**165.6%**

Fuente: Propia

5.4 ESTRATEGIAS ADOPTADAS

5.4.1 Servicios

Las herramientas a incorporar en este portal ampliarán y no remplazarán el trabajo altamente experto que realiza la SBS día a día en la supervisión de las empresas del sistema financiero.

Las funciones que incorporaría esta solución se describen a continuación (en la Figura Nº 17 se presenta un esquema resumen):

Herramientas

- Herramientas de análisis para que las empresas analicen su desempeño desde una perspectiva de competitividad y rentabilidad. Por ejemplo, podrían compararse en línea con otras instituciones en criterios de ingresos, liquidez, rentabilidad, etc., o poder revisar su desempeño histórico en línea. Actualmente, la Superintendencia cuenta con un sistema que genera diversos reportes históricos y de comparación basados en la información que se remite en los anexos y reportes del manual de contabilidad.

- Herramientas de alertas tempranas para apoyar a las empresas en la identificación de riesgos emergentes. *Para una siguiente etapa.*

Comunicaciones

- Coordinar permanentemente con los responsables de las entidades supervisadas.
- Consultas y respuestas a las consultas de las empresas supervisadas.
- Directorio actualizado de los funcionarios de la SBS para ayudarlos a identificar a los responsables específicos por cada área concerniente.
- Comunicaciones: Presentaciones en línea, chats en línea y video conferencias preparadas por la Superintendencia. *Para una siguiente etapa*.

Normativa

- Proyectos normas y foros de discusión a través de la Extranet.
- Servicio de normas actualizada con las modificaciones posteriores.
- Panel con las normas emitidas personalizadas por cada empresa. Se incluirá resoluciones, circulares, oficios múltiples, oficios, etc.

Informes SBS

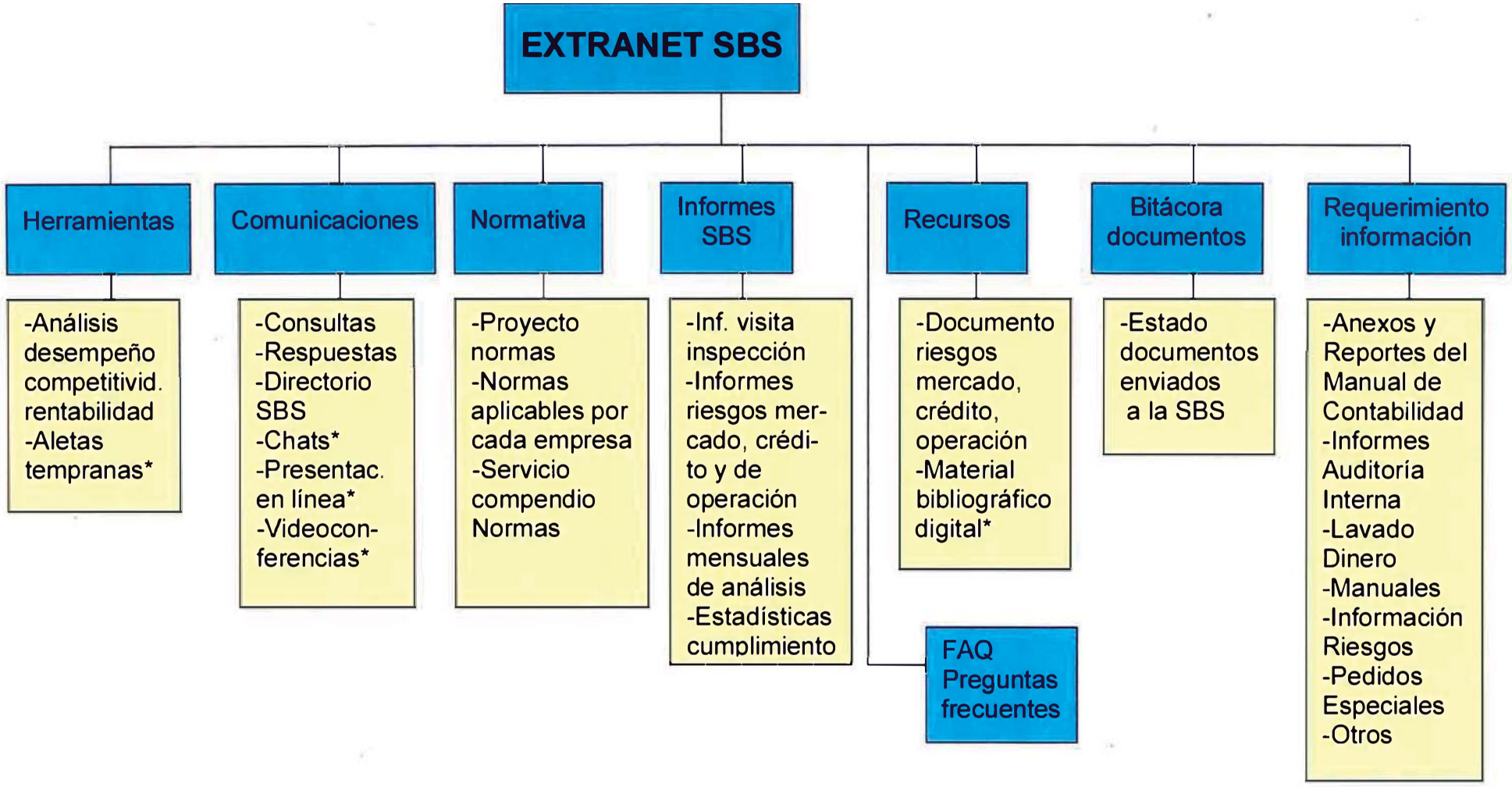
- Informes de visita por cada empresa supervisada.
- Información sobre la administración de riesgos de cada empresa (riesgos de crédito, mercado, liquidez y de operación).
- Informes mensuales de análisis de cada empresa.

- Estadísticas de cumplimiento de envío de reportes y anexos del manual de contabilidad.

Recursos disponibles

- Documentos sobre riesgo de crédito, riesgo de mercado, riesgo de liquidez y riesgo de operación, organizados por sector (bancos, financieras, cajas municipales, rurales y edpymes).
- Material bibliográfico digital. *Para una siguiente etapa.*

Figura Nº 17: Esquema funciones



Fuente: Propia

** Para una siguiente etapa*

Bitácora de documentos enviados

- Estados de los documentos enviados por las instituciones financieras (no recibido, recibido, a quién se derivó, acción tomada, etc.).

Requerimientos de información

- Informe y observaciones de auditoria interna y unidades de riesgos.
- Reemplazar el Submódulo de Captura y Validación Externa (SUCAVE)[14] para el envío de los anexos y reportes del Manual de Contabilidad.
- Centralizar, procesar y mantener la información referente a los accionistas, directores y funcionarios de las empresas del sistema financiero.
- Centralizar, procesar y mantener la información referente a los conglomerados financieros y mixtos a los que pertenecen las empresas del sistema financiero y de los principales grupos económicos con los que el sistema financiero mantiene exposición al riesgo crediticio.
- Coordinar con las áreas internas de la Superintendencia y con las empresas supervisadas, la definición de los formatos de requerimiento de información a las entidades supervisadas para que se cuente oportunamente con la información requerida para el análisis.
- Informes de Oficiales de Cumplimiento (semestral) e Informes de riesgo de operación (anual).
- Información de manuales de la empresa supervisada, evaluaciones, y otros documentos que interesa analizar. Entre algunos manuales se

[14] Azañedo Marcos, propuesta presentada en Informe Suficiencia de 2002

tienen: Manual de Riesgos, Manual de Procedimientos y Manual de Organización y Métodos.

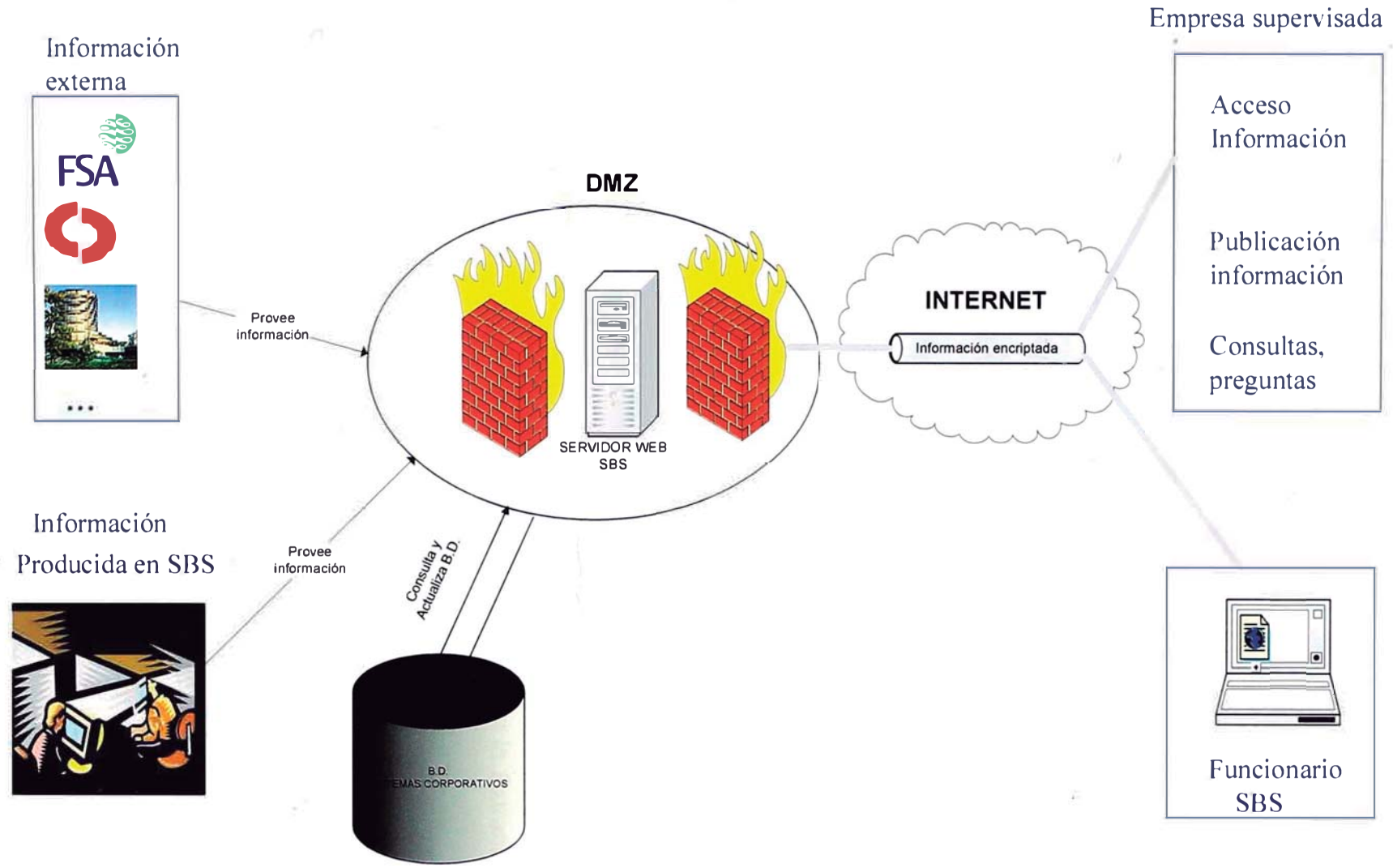
- Anexos y reportes del manual de contabilidad que no se envían por Sucave.
- Información requerida por alguna circular, oficio múltiple, oficio, etc.
- Canal para que la empresa actualice información de su arquitectura tecnológica.
- Envío de documentos oficiales con el uso de certificados digitales (con valor legal). *Para una siguiente etapa*.
- Permitir a las empresas del sistema financiero enviar sus solicitudes de autorización –en forma electrónicas- para abrir nuevas agencias o reubicar las existentes. *Para una siguiente etapa.*

FAQ: Preguntas más frecuentes

- Preguntas frecuentes por temas (riesgo de crédito, riesgo de mercado, riesgo de operación, Manual de Contabilidad, etc.)

5.4.2 Seguridad

EXTRANET CON SUPERVISADOS



Acciones conjuntas con los supervisados para mitigar los riesgos asociados a la seguridad de la Extranet

- Establecer un fórum para el planeamiento, implementación y mantenimiento de la Extranet. Para asegurar que la interconexión vía la Extranet esté tan protegida como sea posible durante su ciclo de vida, la SBS y sus clientes deberán trabajar juntos para desarrollar un acercamiento coordinado y comprensivo para el planeamiento, implementación y mantenimiento de una conexión segura. Las responsabilidades del fórum deben incluir la identificación de controles de seguridad que deberían ser implementados por cada organización para proteger la interconexión y los activos de información relacionados, el desarrollo de una política de seguridad de la Extranet, y el establecimiento e implementación de un acuerdo de seguridad de la Extranet. El establecimiento de un fórum puede proveer un canal de comunicaciones regular entre las partes envueltas en la Extranet. Tanto el personal directivo y técnico deberían ser miembros del fórum.

- Desarrollar e implementar una Política de Seguridad de la Extranet. El fórum establecido debe desarrollar la política de seguridad de la Extranet. La política proveerá un común entendimiento y un conjunto de estándares para administrar los riesgos asociados al establecimiento y mantenimiento de la Extranet. La política no solo identifica los requerimientos de seguridad para la Extranet, también asigna responsabilidades para la implementación de las medidas de seguridad. La política de seguridad debe ser un documento activo que se actualice

con los cambios en la tecnología y seguridad. La política de seguridad debe ser acordada y aprobada por todas las partes. Las siguientes declaraciones deberían ser incluidas en la política:

- Asegurar que la Extranet esté separada de la Intranet de la empresa.
- Proveer de conectividad segura en la red encriptando los datos o usando una red privada virtual.
- Los usuarios de la Extranet deben ser identificados únicamente usando adecuadas técnicas de autenticación.
- La autorización debe adherirse al principio del menor privilegio.
- Los administradores de Extranet recibirán mensualmente reportes de acceso para que verifiquen el apropiado uso de la red.
- Monitoreo en tiempo real, auditoría, y dispositivos de alerta deben ser empleados para detectar fraudes y abusos.

Adicionalmente, la política debería declarar que todas las entidades que acceden a la Extranet son responsables de asegurar el acceso sólo a usuarios autorizados y que estos usuarios cumplan con la política de seguridad de la Extranet.

- Establecer e implementar un acuerdo de seguridad de la Extranet. El fórum creado debe desarrollar también un acuerdo de seguridad. Este acuerdo es un documento que especifica los requerimientos técnicos y de seguridad a través del ciclo de vida de la Extranet. El acuerdo debe documentar los requerimientos de seguridad para acceder a los sistemas

de información e identificar los controles de seguridad que serán usados para proteger los datos y sistemas:

- Proveer un claro entendimiento de los estándares a ser seguidos.
- Proveer una descripción de las aplicaciones e/o información que serán accedidos por los usuarios.
- Ser revisado y aprobados por los consejeros legales.
- Asegurarse que las empresas usuarias cumplan con las políticas de seguridad mínimas.
- Estipular que las intrusiones serán investigadas, reportadas y se implementarán medidas correctivas.
- Asegurar que cada empresa que se conecte, audite su red e informe de cualquier situación que afecta la seguridad mutua.
- Estipular la fecha que empieza el servicio y la declaración de finalización en caso no se adhieran al acuerdo.

- Conducir una evaluación de riesgos. Es crítico que todas las partes de la conexión Extranet entiendan los riesgos que existen en la interconexión, y tengan un común entendimiento y acuerdo en los controles de seguridad requeridos para mitigar estos riesgos. Entendiendo la red e investigando las amenazas y vulnerabilidades asociadas con la interconexión, se puede determinar el nivel de riesgos asociados con la interconexión a otros sistemas. Conducir una evaluación de riesgos de la red y los sistemas es una buena forma de determinar cuan segura es la red. La evaluación de riesgos puede ser llevada por un tercero que examine las políticas y arquitectura de seguridad.

- Proveer controles de acceso físico a las redes de la empresa. De acuerdo con The *Computer Security Journal (CSJ)*, una compañía debe centralizar los puntos de conexión de su red en lugares seguros. Estos lugares deben proveer protección a los activos de la red contra daños, pérdidas, robos o accesos físicos no autorizados. Adicionalmente, debe protegerse los activos contra desastres naturales y peligros tales como fuego, humedad excesiva e inundaciones.

- Aseguramiento de la red. Asegurar todos los componentes de la red de la empresa. Una común práctica cuando se conecta la red interna a una red externa, como una Extranet, es instalar una zona desmilitarizada (DMZ). Una DMZ provee mecanismos de protección entre la red interna y externa.

El aseguramiento de la red también incluye el uso de software y hardware de seguridad que provee capacidades de detección de intrusos, *virus scanning*, identificación y autenticación y encriptación. La encriptación consiste en ocultar un mensaje por medio de algoritmos de criptografía. Los objetivos de la criptografía son: Privacidad (un intruso que "escuche" la comunicación no puede obtener ninguna información acerca del contenido), autenticidad (se le da al destinatario la certeza de que la comunicación proviene del origen supuesto), verificabilidad (el destinatario sabe que la comunicación es auténtica y se le da la capacidad de demostrarlo ante terceros).

Asimismo, el sistema de detección de intrusos provee la capacidad de detectar violaciones a la seguridad de la red. El software *virus scanning* busca la información que es transmitida desde un sistema de información a otro y elimina código malicioso antes que cause daños al sistema.

También se debe usar el *Secure Sockets Layer* (SSL) o similar que viene a ser un protocolo de seguridad para proporcionar confidencialidad, integridad y autenticación del sitio Web. Y tratándose del alto valor de la información que se transmitirá se recomienda extender el uso del SSL para autenticar al cliente, es decir, efectuar autenticaciones mutuamente con el SSL tanto al servidor Web SBS como al cliente.

- Conducir Auditorías a la Extranet. Para ayudar a controlar los riesgos, las partes involucradas deben implementar mecanismos de auditoría para registrar las actividades que ocurren a través de la interconexión. Para que sea efectiva, la auditoría debe ser minuciosa en la revisión de posibles vulnerabilidades de la red y deben ser repetibles para proveer una consistente perspectiva de las prácticas de seguridad de la empresa. Los tipos de actividades a ser auditadas deben incluir: tipo de evento/transacción, fecha y hora del evento, identificación de usuario, el éxito o fracaso del intento de acceso, las acciones de seguridad tomadas por el administrador del sistema, entre otros. Los *logs* de auditoría deben ser analizados en forma regular.

5.4.3 Estrategias de implementación

Consideraciones

En la conformación de equipos se debe considerar la participación de funcionarios del sistema financiero en las etapas de diseño de la interfaz usuaria, pruebas del sistema y proceso de aceptación. Así como para conformar el fórum de seguridad de la Extranet que desarrolle políticas y procedimientos de seguridad para todo el sistema financiero.

Se recomienda invitar a tres bancos (un banco grande, un banco mediano, un banco pequeño) que designen por lo menos dos personas (un funcional y un técnico) para que participen en las fases indicadas en el párrafo anterior.

Asimismo, luego de culminada la implementación se recomienda efectuar un piloto "real" por un período de tres meses con las empresas invitadas anteriormente, con el objetivo de corregir o mejorar cualquier aspecto que sea necesario. Luego del piloto, se procedería a la apertura del canal a cualquier empresa del sistema financiero que lo solicite.

Diagrama Gantt

En la Tabla Nº 11 se presenta las actividades necesarias para la puesta en marcha de la Extranet. Se divide en tres grandes fases: Desarrollo e implementación (138 días útiles), piloto (60 días útiles) y puesta en producción a todo el sistema financiero (12 días útiles).

Tabla Nº 11: Diagrama gantt Proyecto Extranet

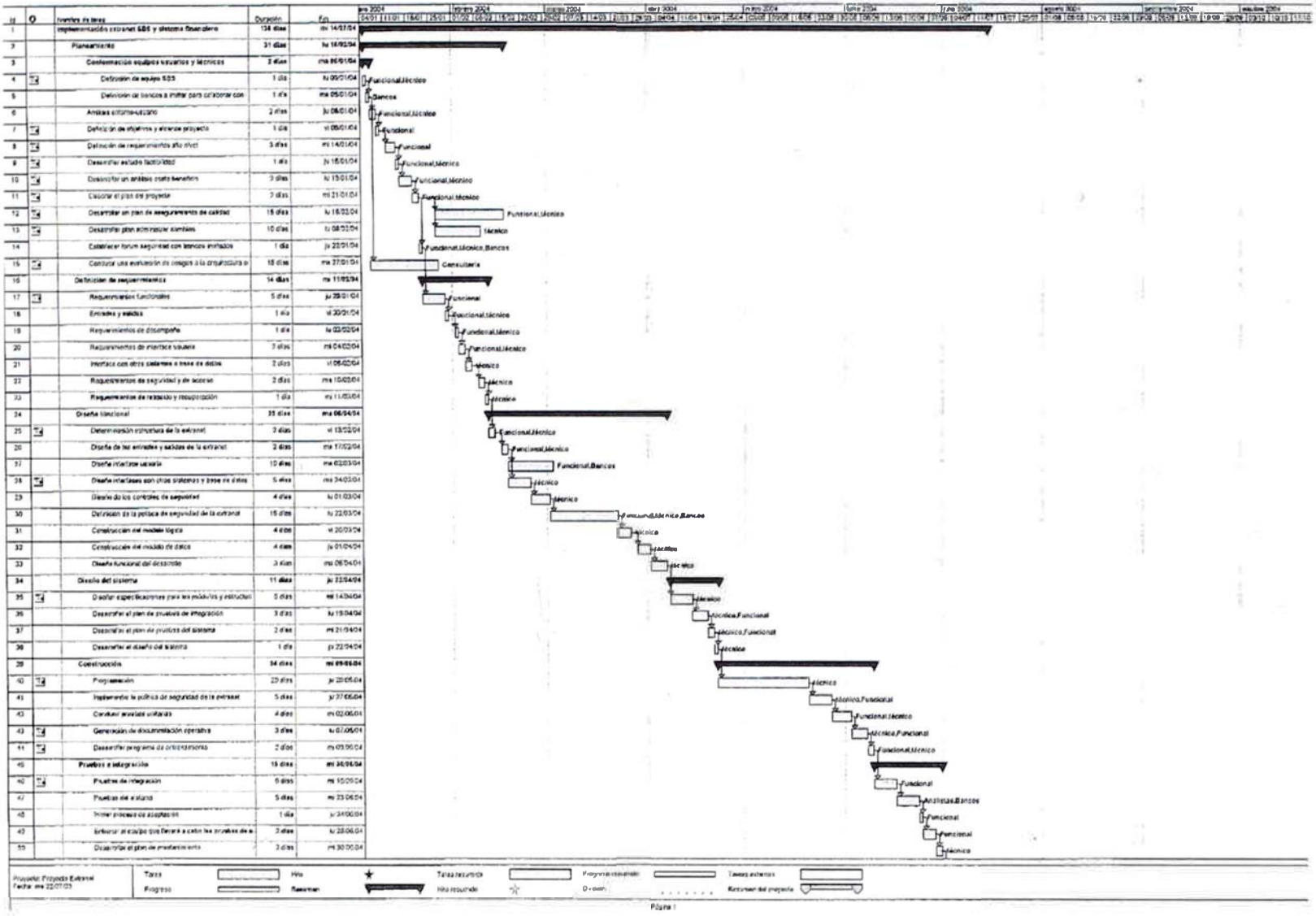
Fecha de comienzo del proyecto: lu 05/01/04
Fecha de fin del proyecto: vi 22/10/04

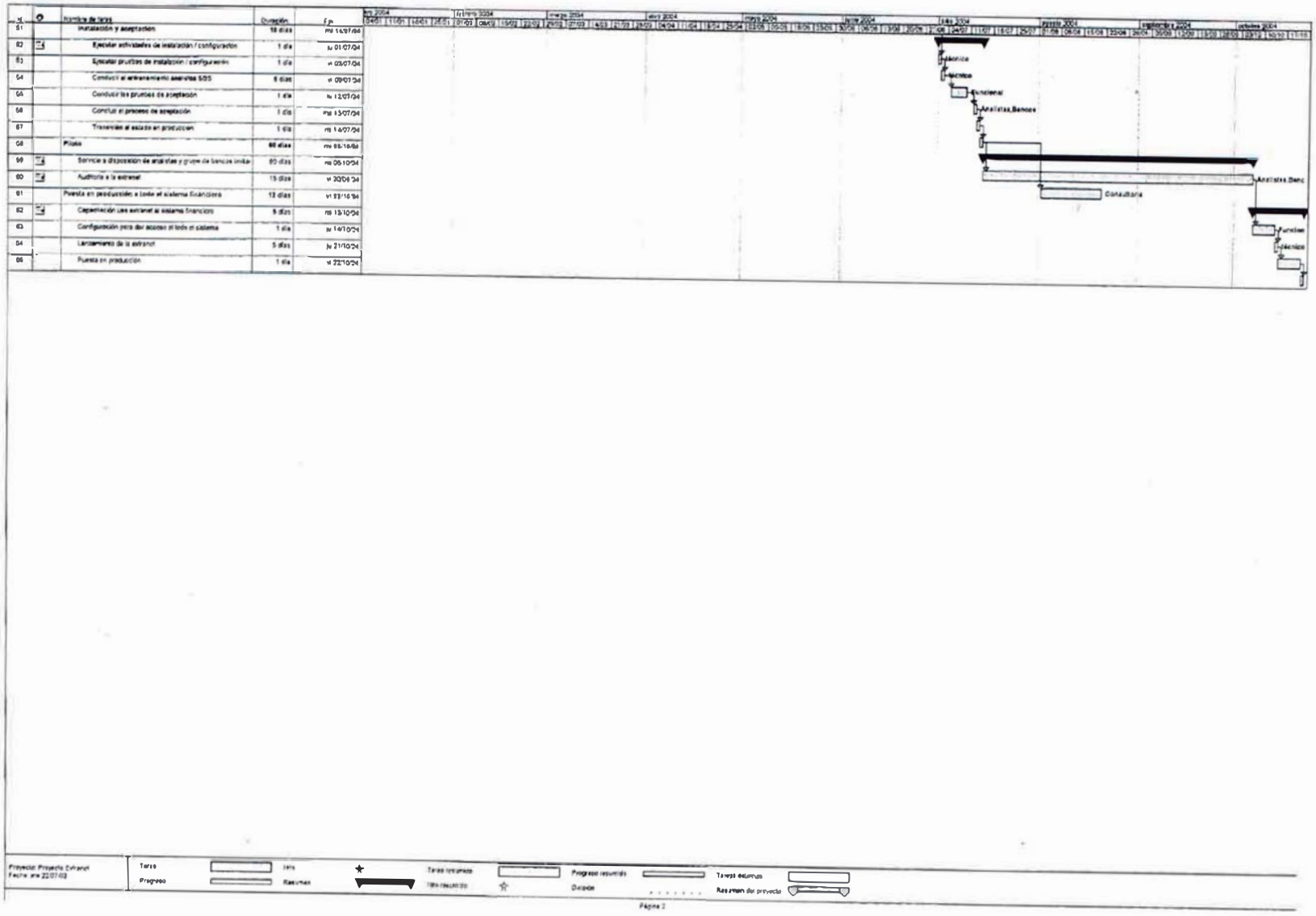
Id	Nombre Tarea	Duración	Fecha Comienzo	Fecha Fin	Predecesoras	Nombres Recursos
1	**Implementación Extranet SBS y sistema financiero**	138 días	lu 05/01/04	mi 14/07/04		
2	**Planeamiento**	31 días	lu 05/01/04	lu 16/02/04		
3	**Conformación equipos usuarios y técnicos**	2 días	lu 05/01/04	ma 06/01/04		
4	Definición de equipo SBS	1 día	lu 05/01/04	lu 05/01/04		Funcional, técnico
5	Definición de bancos a invitar para colaborar con la implementación	1 día	ma 06/01/04	ma 06/01/04	4	Bancos
6	Análisis entorno-usuario	2 días	mi 07/01/04	ju 08/01/04	5	Funcional, técnico
7	Definición de objetivos y alcance proyecto	1 día	vi 09/01/04	vi 09/01/04	6	Funcional
8	Definición de requerimientos alto nivel	3 días	lu 12/01/04	mi 14/01/04	7	Funcional
9	Desarrollar estudio factibilidad	1 día	ju 15/01/04	ju 15/01/04	8	Funcional, técnico
10	Desarrollar un análisis costo beneficio	2 días	vi 16/01/04	lu 19/01/04	9	Funcional, técnico
11	Elaborar el plan del proyecto	2 días	ma 20/01/04	mi 21/01/04	10	Funcional, técnico
12	Desarrollar un plan de aseguramiento de calidad	15 días	ma 27/01/04	lu 16/02/04	11	Funcional, técnico
13	Desarrollar plan administrar cambios	10 días	ma 27/01/04	lu 09/02/04	11	técnico
14	Establecer fórum seguridad con bancos invitados	1 día	ju 22/01/04	ju 22/01/04	11	Funcional, técnico, bancos
15	Conducir una evaluación de riesgos a la	15 días	mi 07/01/04	ma 27/01/04	5	Consultoría

	arquitectura soporta de la Extranet					
16	**Definición de requerimientos**	14 días	vi 23/01/04	mi 11/02/04		
17	Requerimientos funcionales	5 días	vi 23/01/04	ju 29/01/04	14	Funcional
18	Entradas y salidas	1 día	vi 30/01/04	vi 30/01/04	17	Funcional, técnico
19	Requerimientos de desempeño	1 día	lu 02/02/04	lu 02/02/04	18	Funcional, técnico
20	Requerimientos de interfaz usuaria	2 días	ma 03/02/04	mi 04/02/04	19	Funcional, técnico
21	Interfaz con otros sistemas o base de datos	2 días	ju 05/02/04	vi 06/02/04	20	técnico
22	Requerimientos de seguridad y de acceso	2 días	lu 09/02/04	ma 10/02/04	21	técnico
23	Requerimientos de respaldo y recuperación	1 día	mi 11/02/04	mi 11/02/04	22	técnico
24	**Diseño funcional**	39 días	ju 12/02/04	ma 06/04/04		
25	Determinación estructura de la Extranet	2 días	ju 12/02/04	vi 13/02/04	23	Funcional, técnico
26	Diseño de las entradas y salidas de la Extranet	2 días	lu 16/02/04	ma 17/02/04	25	Funcional, técnico
27	Diseño interfaz usuaria	10 días	mi 18/02/04	ma 02/03/04	26	Funcional, Bancos
28	Diseño interfaces con otros sistemas y base de datos	5 días	mi 18/02/04	ma 24/02/04	26	técnico
29	Diseño de los controles de seguridad	4 días	mi 25/02/04	lu 01/03/04	28	técnico
30	Definición de la política de seguridad de la Extranet	15 días	ma 02/03/04	lu 22/03/04	29	Funcional, técnico, bancos
31	Construcción del modelo lógico	4 días	ma 23/03/04	vi 26/03/04	30	técnico
32	Construcción del modelo de datos	4 días	lu 29/03/04	ju 01/04/04	31	técnico
33	Diseño funcional del desarrollo	3 días	vi 02/04/04	ma 06/04/04	32	técnico

34	**Diseño del sistema**	11 días	ju 08/04/04	ju 22/04/04		
35	Diseñar especificaciones para los módulos y estructura base datos	5 días	ju 08/04/04	mi 14/04/04	33	técnico
36	Desarrollar el plan de pruebas de integración	3 días	ju 15/04/04	lu 19/04/04	35	técnico, Funcional
37	Desarrollar el plan de pruebas del sistema	2 días	ma 20/04/04	mi 21/04/04	36	técnico, Funcional
38	Desarrollar el diseño del sistema	1 día	ju 22/04/04	ju 22/04/04	37	técnico
39	**Construcción**	34 días	vi 23/04/04	mi 09/06/04		
40	Programación	20 días	vi 23/04/04	ju 20/05/04	38	técnico
41	Implementar la política de seguridad de la Extranet	5 días	vi 21/05/04	ju 27/05/04	40	técnico, Funcional
42	Conducir pruebas unitarias	4 días	vi 28/05/04	mi 02/06/04	41	Funcional, técnico
43	Generación de documentación operativa	3 días	ju 03/06/04	lu 07/06/04	42	técnico, Funcional
44	Desarrollar programa de entrenamiento	2 días	ma 08/06/04	mi 09/06/04	43	Funcional, técnico
45	**Pruebas e integración**	15 días	ju 10/06/04	mi 30/06/04		
46	Pruebas de integración	5 días	ju 10/06/04	mi 16/06/04	44	Funcional
47	Pruebas del sistema	5 días	ju 17/06/04	mi 23/06/04	46	Analistas, Bancos
48	Iniciar proceso de aceptación	1 día	ju 24/06/04	ju 24/06/04	47	Funcional
49	Entrenar al equipo que llevará a cabo las pruebas de aceptación	2 días	vi 25/06/04	lu 28/06/04	48	Funcional
50	Desarrollar el plan de mantenimiento	2 días	ma 29/06/04	mi 30/06/04	49	técnico
51	**Instalación y aceptación**	10 días	ju 01/07/04	mi 14/07/04		
52	Ejecutar actividades de instalación / configuración	1 día	ju 01/07/04	ju 01/07/04	50	técnico
53	Ejecutar pruebas de instalación /	1 día	Vi 02/07/04	vi 02/07/04	52	técnico

	configuración					
54	Conducir el entrenamiento analistas SBS	5 días	lu 05/07/04	vi 09/07/04	53	Funcional
55	Conducir las pruebas de aceptación	1 día	lu 12/07/04	lu 12/07/04	54	Analistas, Bancos
56	Concluir el proceso de aceptación	1 día	ma 13/07/04	ma 13/07/04	55	
57	Transición al estado en producción	1 día	mi 14/07/04	mi 14/07/04	56	
58	**Piloto**	60 días	ju 15/07/04	mi 06/10/04		
59	Servicio a disposición de analistas y grupo de bancos invitados	60 días	ju 15/07/04	mi 06/10/04	57	Analistas, bancos
60	Auditoría a la Extranet	15 días	lu 02/08/04	vi 20/08/04	57	Consultoría
61	**Puesta en producción a todo el sistema financiero**	12 días	ju 07/10/04	vi 22/10/04		
62	Capacitación uso Extranet al sistema financiero	5 días	ju 07/10/04	mi 13/10/04	59	Funcional
63	Configuración para dar acceso al todo el sistema	1 día	ju 14/10/04	ju 14/10/04	62	técnico
64	Lanzamiento de la Extranet	5 días	vi 15/10/04	ju 21/10/04	63	Comunicaciones SBS
65	Puesta en producción	1 día	vi 22/10/04	vi 22/10/04	64	técnico


Nombre de tarea
Duración
Fin
Implementación extranet SIG y sistema financiero
Planeamiento
Conformación equipos usuarios y técnicos
Definición de equipo SIG
Definición de bancos a invitar para colaborar con
Análisis externo-interno
Definición de objetivos y alcance proyecto
Definición de requerimientos alto nivel
Desarrollar estudio factibilidad
Desarrollar un análisis costo beneficio
Elaborar el plan de proyecto
Desarrollar un plan de aseguramiento de calidad
Desarrollar plan administrar cambios
Establecer forum seguridad con bancos invitados
Contratar una evaluación de riesgos a la infraestructura
Definición de requerimientos
Requerimientos funcionales
Entradas y salidas
Requerimientos de desempeño
Requerimientos de interface usuario
Interface con otros sistemas o base de datos
Requerimientos de seguridad y de acceso
Requerimientos de respaldo y recuperación
Diseño funcional
Determinación estructura de la extranet
Diseño de las entradas y salidas de la extranet
Diseño interface usuario
Diseño interfases con otros sistemas y base de datos
Diseño de los controles de seguridad
Definición de la política de seguridad de la extranet
Construcción del modelo lógico
Construcción del modelo de datos
Diseño funcional del desarrollo
Diseño del sistema
Diseñar especificaciones para los módulos y estructur
Desarrollar el plan de pruebas de integración
Desarrollar el plan de pruebas del sistema
Desarrollar el diseño del sistema
Construcción
Programación
Implementar la política de seguridad de la extranet
Conducir pruebas unitarias
Generación de documentación operativa
Desarrollar programa de entrenamiento
Pruebas e integración
Pruebas de integración
Pruebas de volumen
Iniciar proceso de aceptación
Entrenar al equipo que llevará a cabo las pruebas de a
Desarrollar el plan de implantación
Proyecto: Proyecto Extranet
Fecha: mié 22/07/03
Tarea
Progreso
Hito
Resumen
Tarea resumida
Hito resumido
Proyecto resumido
División
Tareas externas
Resumen del proyecto
Página 1


Técnico
Técnico
Funcional
Analistas_Bancos
Consultoria
Analistas_Banc
Funcion
Técnico
Proyecto: Proyecto Extranet
Fecha: mie 22/07/03
Tarea
Progreso
Hito
Resumen
Tareas resumen
Hito resumen
Progreso resumido
División
Tareas externas
Resumen del proyecto
Página 2

5.4.4 Avances alcanzados a mayo 2003

Una de las áreas responsables de la supervisión de las entidades financieras (unidad donde el autor desempeña sus labores), ha definido un grupo de servicios que desde el punto de vista usuario debe tener este nuevo canal. Dicha definición ha sido comunicada a otras áreas, entre ellas Sistemas, con el objetivo de iniciar la definición y desarrollo de la solución.

Asimismo, el Área de Sistemas ha empezado las siguientes actividades de base para la futura Extranet: Implementación de la infraestructura tecnológica de comunicaciones y sistemas, y la implementación de esquemas de seguridad, privacidad y confianza.

El desarrollo del portal Web con las empresas supervisadas está programado para comenzar a mediados del segundo semestre del presente año.

VI. EVALUACIÓN DE RESULTADOS

Se estima que el proyecto estará culminado para el segundo semestre de 2004 y se prevé que la solución generará los siguientes resultados:

6.1 SUPERINTENDENCIA DE BANCA Y SEGUROS

- Cambios importantes en la cultura de trabajo de la SBS.
- Acceso, en línea, a información útil para la labor de análisis.
- Mejora de la calidad de servicio a las entidades supervisadas.
- Reducción de costos al brindar servicios por el canal Internet.
- Mejora de la imagen de la SBS.
- Reducción de papeles físicos en un mediano plazo.
- Liderazgo tecnológico en Latinoamérica: la SBS sería uno de los primeros supervisores bancarios en implementar una Extranet de esta magnitud.

6.2 SISTEMA FINANCIERO

Servicios e información que contribuirán a un mejor manejo de las empresas

- En especial para las pequeñas empresas que no tienen muchos recursos. Este canal será útil para informar, educar y prevenir a las empresas supervisadas.

Reducción de algunos costos a las empresas supervisadas

- Ahorro de llamadas telefónicas a la SBS para conocer estado de documentos.
- Ahorro de llamadas telefónicas para que funcionarios SBS puedan atenderlos.
- Reducción de costos de personal que compendia normas.
- Ahorro de llamadas telefónicas por consultas comunes que ya han sido respondidas por la SBS.
- Ahorro de costos por no enviar por correo postal los siguientes informes: oficiales de cumplimiento, riesgos de operación, entre otros, los cuales se ingresarían directamente en la Extranet.
- Ahorro de costos por no enviar documentos físicos requeridos por oficios o circulares.

Suscripción al canal

- Se espera que todos los bancos se suscriban al servicio durante el primer trimestre de 2005.
- Se espera que las financieras, empresas de leasing y cajas municipales se suscriban durante el primer semestre de 2005.
- Se espera que las cajas rurales y edpymes se suscriban a la Extranet a más tardar a fines de 2005.

VII. CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

Servicios

- Como resultado de este trabajo, se concluye que es altamente necesario implementar los servicios de este canal en beneficio de las empresas supervisadas y la SBS.

Seguridad

- Es imposible obtener 100% de seguridad en la Extranet. La evolución de herramientas y técnicas proveen nuevas oportunidades de ataques.
- Sin embargo, existe una diversidad de técnicas y herramientas expuestas en este trabajo para lograr un alto grado de seguridad de la Extranet.

  En la SBS se debe implementar mecanismos fuertes de autenticación, autorización, identificación del usuario, así como los mecanismos de encriptación y servicios de defensa del canal y la red.

  Asimismo, el uso de estas técnicas y herramientas en las empresas supervisadas dependerá exclusivamente de la decisión e implementación de aquellas que se suscriban a este servicio. Por lo tanto la SBS deberá

establecer acuerdos de seguridad con cada empresa que se suscriba a la Extranet.

Implementación

- Se requiere la participación de algunas empresas supervisadas en el diseño de la interfaz usuaria, pruebas, aceptación y definición de las políticas y procedimientos de seguridad.
- Una vez finalizada la implementación se requiere efectuar un piloto de la solución con algunas empresas supervisadas por alrededor de tres meses antes de ofrecer el servicio a todo el sistema financiero.
- Para asegurar el uso efectivo de este nuevo servicio en la SBS, se requiere contar con el apoyo de la Alta Dirección, debido a que involucrará un cambio importante en las labores diarias de supervisión.

7.2 RECOMENDACIONES

- La Superintendencia debe continuar incorporando más servicios en este canal que permitan reducir la carga de trabajo a las empresas supervisadas.
- Ante cada nuevo servicio que se incorpore en este canal, se recomienda efectuar pruebas piloto con algunas empresas supervisadas.
- Coordinar con los organismos supervisores de Estados Unidos, Reino Unido y/o Alemania para conocer en mayor detalle los servicios que ofrecen a sus supervisados y los mecanismos de seguridad utilizados.
- Dada la alta confidencialidad de la información que se transmitirá por este medio, se recomienda implementar como mínimo dos niveles de

autenticación: 1) Usuario y password (con políticas estrictas para la creación y mantenimiento de las claves) y autenticación mutua con SSL para el servidor y el cliente. 2) Uso de dispositivos de autenticación.

- Las empresas del sistema financiero que se suscriban a este servicio deben contar con una línea dedicada, líneas ADSL u otras que ofrezcan una velocidad de transmisión apropiada. No se recomienda usar conexiones dial-up debido a su lentitud y mayor exposición a ataques.

GLOSARIO DE TÉRMINOS

BROWSER: NAVEGADOR

B2B: BUSINESS TO BUSINESS

B2C: BUSINESS TO CONSUMER

BITS: UNIDAD MÍNIMA DE INFORMACIÓN QUE PUEDE SER PROCESADA POR UNA COMPUTADORA

CRACKERS: LADRÓN DE CÓDIGOS O PROGRAMAS DE CÓMPUTO

DIAL UP: SISTEMA COMERCIAL DE CONEXIÓN TELEFÓNICA

DOE: DEPARTMENT OF ENERGY (USA)

EDI: INTERCAMBIO ELECTRÓNICO DE DATOS

E-MAIL: CORREO ELECTRÓNICO

FTP: SERVICIO DE TRANSFERENCIA DE ARCHIVOS

HACKERS: PIRATAS INFORMÁTICOS QUE SE CARACTERIZAN POR ACCESAR A SISTEMAS PROTEGIDOS SIN AUTORIZACIÓN DEL TITULAR

HARDWARE: ADITAMIENTOS FÍSICOS PARA LA CONSTRUCCIÓN DE COMPUTADORAS

HOST: COMPUTADORA ANFITRIONA

HTML: LENGUAJE DE MARCACIÓN DE HIPERTEXTOS

ISO/IEC: ORGANIZACIÓN DE NORMAS INTERNACIONALES

JAVA: DESARROLLO DE SOFTWARE QUE, INCLUIDO EN LOS NAVEGADORES, PERMITE EJECUTAR APLICACIONES SOBRE CUALQUIER PLATAFORMA

PKI: PUBLIC KEY INFRAESTRUCTURE

SOFTWARE: CONJUNTO DE PROGRAMAS QUE POSIBILITAN EL USO DE UNA COMPUTADORA

TCP/IP: PROTOCOLO DE CONTROL DE TRANSMISIÓN

WEB SITE: SITIO EN LA RED

WWW: WORDL WIDE WEB

XML: ENTENSIBLE MARKUP LANGUAGE

BIBLIOGRAFÍA

Libros

CHESWICK William, BELLOVIN Steven, RUBIN Aviel. Firewalls and Internet Security. Second Edition.
United States of America, Addison Wesley, 2003. 433 p.

COMPTROLLER of the Currency Administrator of National Banks (2000). Strategic Plan 2000 – 2005.
United States of America. 33 p.

JACKSON Greg. An Internet, Intranet, Extranet Architecture for the Information Technology for the State of Ohio. United States of America, The Ohio Department of Administrative Services, 2000. 60 p.

LOSHIN, P. Extranet Design and Implementation. United States, Network press.

SUPERINTENDENCIA de Banca y Seguros. Memoria 2002. 72 p.

SUPERINTENDENCIA de Banca y Seguros. Memoria 2001. 92 p.

U.S. Department of Energy. Systems Engineering Methodology Version 3. September 2002. 308 p.

U.S. Department of Energy. An Analyst's Handbook for Analysis of Benefits and Costs. Volume 2. Junio 1998. 65 p.

Tesis

ANDERSSON Mikael, BACKMAN Lars. Online or Offline? Industrial Promotion Activities - A Case Study of Volvo CE. Master Thesis (International Business). Göteborg University, Graduate Business School, School of Economics and Commercial Law, 2001. 163 p.

ARGUETA Amador, A. Estrategia de seguridad distribuida en redes bajo ambiente de Jini y Java (Tesis Licenciatura. Ingeniería en Sistemas Computacionales). Departamento de Ingeniería en Sistemas Computacionales, Escuela de Ingeniería, Universidad de las Américas-Puebla, 2001.

AZAÑEDO Marcos. Transferencia electrónica de información financiera utilizando tecnología Web. Informe de Suficiencia (Para optar por el título de Ingeniero de Sistemas). Universidad Nacional de Ingeniería, 2002.

BOYLE Brendan. Electronic Government for New Zealand: Managing the Transition. Tesis (Master of Business Administration). Massachusetts Institute Of Technology, 2000. 146 p.

CHANG Ho-Yen. On Real-Time Intrusion Detection and Source Identification. Tesis (Doctor of Philosophy). North Carolina State University, 2000. 162 p.

HERNÁNDEZ Sánchez, Jéssica Adriana. Ambiente de aprendizaje interactivo en Internet, basado en la tecnología JSP para la Educación Ambiental. Tesis (Licenciatura en Ingeniería en Sistemas Computacionales). Puebla, Universidad de las Américas, 2001. 155 p.

KLEMETTI Kari. Authentication in Extranets. Tesis (Master of Science). Helsinki University of Technology, Department of Computer Science, 2001. 87 p.

LOWMAN Tim. Secure Computer Applications in an Enterprise Environment. Tesis (Master of Science). North Carolina State University, 1998. 117 p.

NYKÄNEN Toni. Secure Cross-Platform Single Sign-On Solution for the World-Wide Web. Tesis (Master of Science). Helsinki University of Technology, Department of Computer Science and Engineering, 2002. 79 p.

REYES Krafft, Alfred Alejandro. La firma electrónica y las entidades de certificación. Tesis (Doctorado en. Derecho). México D.F., Universidad Panamericana, 2002. 327 p.

STAMBRO Robert, SVARTBO Erik. Extranet Use in Suply Chain Management – A case of Study of three companies. Master Thesis (International Business and Economics Programme). Lulea University of

Technology, Department of Business Administration and Social Sciences, 2002. 80 p.

TSHISUAKA Daniel. Secure Remote Support. Tesis. University of Stuttgart., 2001. 146 p.

Artículos

CSI/FBI 2002 Computer Crime and Security Survey

CSI/FBI 2000 Computer Crime and Security Survey

INTERNATIONAL Standard Organization (First Edition 2000-12-01) ISO/IEC 17799 - Security Standards.

KELLY Teresa (November 23, 2002) Security Policy Harmonization in Extranet Connection Projects, SANS Institute 2003.

LING R. R, Yen D. C. (2001) *Extranet: A new wave of Internet,* S.A.M. Advanced Management Journal, Vol. 66, Issue 2, p.39-44

LUCENT Technologies. Network Security – Sharing the Knowledge Behind the Network.

COMPTROLLER of the Currency Administrator of National Banks (2000).

Fact Sheet NR 2000-69. September 17, 2000.

United States of America. 3 p.

SUPERINTENDENCIA de Banca y Seguros. Circular G-105-2002 sobre la Administración de los Riesgos de Tecnología de Información en las entidades supervisadas.

VLOSKY R. P, Fontenot R, Blalock L. Extranets: impact on business practices and relationships, Journal of Business & Industrial Marketing, 2000.

Artículos de Internet

DEUTSCHE Bundesbank (December 2002) Bundesbank Extranet – Dokumentation für Kunden Version 0.2, www.bundesbank.de/extranet visitado el 10 de enero de 2003.

HORSBURGH.COM (2000) Extranet Design, www.horsburgh.com/h_extra visitado el 16 de junio de 2003.

KAREN A. Korow-Diks (December 18, 2001) Security Considerations for Extranets, http://www.sans.org/rr/securitybasics/extranets2.php, visitado 03 de mayo de 2003.

SHRUTI Daté – Government Computer News Staff (February 21, 2000; Vol. 19 No. 4) OCC launches an extranet site for national banks, www.gcn.com visitado el 24 de octubre de 2002.

STEVE Hunt (March 15, 2001) Optimal Extranet Security: A Methodology, www.gigaWeb.com (Giga Information Group) visitado el 10 de junio de 2003.

STEVE Hunt (Septembre 5, 2000) Securing the Extranet Web Application, www.gigaWeb.com (Giga Information Group) visitado el 10 de junio de 2003.

VERISING (julio 1999) Guide to Securing Intranet and Extranet Servers, www.verisign.com visitado el 09 de junio de 2003.

Internet

www.banknet.gov, visitado el 17 de octubre de 2002.

www.fsa.gov.uk/industry/, visitado el 08 de enero de 2003.

http://www.scientech.com/services/itconsulting.html, visitado el 16.06.2003.

www.bundesbank.de/, visitado el 03 de julio de 2003.

http://www.cnbv.gob.mx/, visitado el 03 de julio de 2003.

http://www.emprendedores.cl/desarrollo/mantenedores/art_indice.asp?art_id=26, visitado el 03 de Julio de 2003.

Entrevistas

Superintendencia de Banca y Seguros, noviembre 2002
Personal de la Superintendencia Adjunta de Banca

Superintendencia de Banca y Seguros, diciembre 2002
Personal de la Gerencia de Informática (ahora Organización y Sistemas)

ANEXO 1

Directorio de empresas supervisadas

BANCO	FINANCIERA	ALMACENERA	ETCANs
Banco Agropecuario-Agrobanco	Corporación Financiera de Desarrollo SA. COFIDE	Almacenera Continental ALMACONTI	HERMES TRANSPORTES BLINDADOS S.A.
BankBoston, N.A. Sucursal del Perú	Daewoo S.A. FINANDAEWOO	Almacenera del Perú S.A. ALMAPERU	CIA. DE SEGURIDAD PROSEGUR S.A.
Banque BNP Paribas-Andes S.A.	Financiera C.M.R.	Almacenera Peruana de Comercio ALPECO	
Central de Reserva del Perú	Solución - Financiera de Crédito del Perú	Cía. Almacenera S.A. CASA	
Comercio	Volvo Finance Perú S.A.	Depósitos de Lima S.A. DELISA	
BBVA Banco Continental	Financiera Cordillera S.A.	Depósitos S.A.	
Crédito del Perú	**EMP. AFIANZADORA Y DE GARANTÍA**		
De la Nación	Fundación Fondo de Garantía para Préstamos a la Pequeña Industria - FOGAPI		
Del Trabajo	**LEASING**		
Financiero del Perú	América Leasing		
Interamericano de Finanzas	Citileasing		
Internacional del Perú-INTERBANK	Crédito Leasing S.A. - Credileasing S.A.		
Mibanco Banco de la Microempresa -MIBANCO-	Wiese Leasing S.A.		
Standard Chartered	Leasing Total S.A.		
Suc. en el Perú del Citibank N.A.	Mitsui-Masa Leasing S.A.		
Sudamericano S.A.			
Wiese-Sudameris			

Fuente: www.sbs.gob.pe visitado el 29.06.2003

CAJAS RURALES	EDPYMES	CAJAS MUNICIPALES DE AHORRO Y CRÉDITO	ETF s	LIQUIDACIONES SUPERVISÓN SBS
CAJAMARCA	ALTERNATIVA	AREQUIPA	A. SERVIBAN S.A.	SERBANCO
CAJASUR	CAMCO PIURA	CUSCO	ARGENPER S.A.	ORION
CHAVIN S.A.	CONFIANZA	DEL SANTA	CAMBIOS CAPITAL S.A.	BANEX
CREDINKA	CREAR CUSCO	CHINCHA	G.F.P. INTERNATIONAL SRL.	REPUBLICA
CRUZ DE CHALPON	CREAR TACNA	HUANCAYO	JET PERU S.A.	NUEVO MUNDO
DE LA REGION SAN MARTIN	CREAR TRUJILLO	ICA	JOSILVA S.A.	NBK
NOR PERU	CREAR AREQUIPA	MAYNAS	MONEDEX PERU S.A.	LATINO
LOS ANDES S.A.	CREDIVISION	PAITA	PERU SERVICES COURIER S.R.L.	CAJA RURAL SELVA CENTRAL
LOS LIBERTADORES AYACUCHO	EDYFICAR S.A.	PISCO	REYNTEL S.A.	EDPYME CREDINPET
PRYMERA S.A.	NUEVA VISION S.A.	PIURA	SERVICIO EXPRESS INMEDIATO S.A.C.	
PROFINANZAS S.A.	PROEMPRESA S.A.	SULLANA	APOYO INTERNATIONAL SERVICE S.A.	
SEÑOR DE LUREN	RAIZ	TACNA	VIGO DEL PERÚ S.A.	
	SOLIDARIDAD	TRUJILLO	DHL INTERNATIONAL S.A.C.	
	PRO NEGOCIOS S.A.	CMCP. DE LIMA	PERÚ - EXPRESS SERVICIOS INTERNACIONALES	

Fuente: www.sbs.gob.pe visitado el 29.06.2003

ANEXO 2

Alternativas de autenticación

*(*Extraído del libro *Firewalls and Internet Security Second Edition* de 2003*)*

Las alternativas son las siguientes:

1. Recordando passwords

Es necesario elegir buenos passwords y protegerlos de robos o descubrimientos. Como medio de autenticación personal, los passwords son categorizados como "algo que usted conoce". Esta es una ventaja debido a que no se requiere usar algún equipo especial y también una desventaja debido a que su password puede ser dicho a otra persona, capturado o adivinado.

2. Time-based One-Time Password

Se puede lograr un incremento significativo en la seguridad usando *one-time passwords*. Un *one-time passwords* es tal como su nombre lo indica: sólo para ser usado exactamente una vez, después del uso ya no es más válido.

Provee una muy fuerte defensa contra los *eavesdroppers* (alguien que escucha una conversación privada).

Existen numerosas formas de implementar *one-time passwords*. La mejor considera el uso de alguna clase de autenticador portátil, también conocido como un *dongle* (dispositivo que se conecta en la salida del computador para verificar que el programa es original y no una copia) o un *token*.

SecurId hizo autenticador común que usa un reloj interno, una clave secreta y una pantalla. La pantalla muestra algunas funciones del tiempo

actual y la clave secreta. El valor de salida, usualmente combinado con un PIN, es usado como el mensaje de autenticación. El valor de salida cambia cada minuto, y generalmente se permite sólo una sesión por minuto. Estos passwords nunca son repetidos.

El cliente toma la respuesta del SecurID token y envía esto al servidor, el cual consulta a un servidor de autenticación, identificando el usuario y la respuesta ingresada. El servidor de autenticación usa esta copia de la clave secreta y registra el tiempo para calcular el valor esperado de salida. Si ellos coinciden, el servidor de autenticación confirma la identificación.

En la práctica, el registrar el tiempo entre el dispositivo y el host puede ser un problema. Ante esto, diversos candidatos de passwords son calculados, y el valor usuario es verificado contra todo este conjunto.

Es importante asegurar el enlace entre el servidor y el servidor de autenticación.

3. Challenge/Response One-Time Password

A diferencia del sistema *one-time password*, este método usa un probador no repetible desde el servidor. La respuesta es una función del probador y una clave conocida por el cliente. El probador/respuesta puede ser implementado en el software cliente o con un hardware token, o quizás calculado por el usuario.

Challenge: 00193 Wed Sep 11 11:22:09 2002

Response: ab0dh1kd0jkfj1kye

Esta respuesta puede ser rápidamente calculada por el usuario basado en un texto probador. En este caso, el algoritmo es secreto, y no la clave. El algoritmo debe ser fácilmente aprendido, recordado y luego cubierto.

Varios protocolos de Internet pueden usar este método: ppp tiene CHAP y pop3 tiene APOP. Pero el tipo más fuerte de autenticación incluye hardware *token* que calcula la respuesta. Algunas agencias espías usan este mecanismo.

4. Lamport's One-Time Password Algorithm

Lamport propuso *one-time password* que puede ser implementado sin un hardware especial. Este método asume la existencia de alguna función F que es razonablemente fácil de calcular directamente pero imposible de hacerlo en forma inversa. Más aún asume que el usuario tiene algo secreto – quizás un password- x. Para permitir al usuario hacer *login* un número de veces, el host calcula F(x) para este número de veces. En consecuencia, para permitir 1000 ingresos antes de cambiar un password, el host podría calcular $F^{1000}(x)$ y almacenar solo este valor.

La primera vez que el usuario hace *login*, él o ella deben suplir $F^{999}(x)$. El sistema validaría esto calculando:

$F(F^{999}(X)) = F^{1000}(X)$

Si el *login* es correcto, el password provisto $F^{999}(X)$ llega a ser el nuevo valor almacenado. Este es usado para validar $F^{998}(x)$, el siguiente password a ser suplido por el usuario.

El cálculo del usuario $F^{n}(x)$ puede se hecho por un autenticador portátil, una estación confiable o una computadora portátil. La implementación de la

empresa Telecordia en este campo conocida como S/Key fue un paso más adelante. Mientras el usuario hace *login* a una máquina segura, el usuario podría ejecutar un programa que calcula las secuencias.

5. Smart Card

Es un dispositivo portable que tiene una CPU[15], algunos puertos de entrada y salida, y unos pocos miles de bites de memoria que son accesibles sólo a través de la tarjeta del CPU.

6. Biometría

Como la huella digital, voz, la forma de su mano, imagen de la cara, el patrón de retina o el iris, o una firma. Se requiere hardware especial, lo que limita la aplicabilidad de las técnicas de biometría en algunos entornos (aunque ya los videos cámaras son más comunes en PCs). Lo atractivo es que una identificación biométrica no puede ser entregada a otra persona o ser robada.

En la práctica, existen algunas limitaciones a la biometría. La sabiduría convencional en seguridad dice que la autenticación de datos debería cambiar periódicamente. Existe una gran diferencia entre forzar a alguien a cambiar su clave y permitir hacerlo. Cambiar la autenticación es difícil de hacer cuando se trata de una huella digital.

No todos los mecanismos biométricos son amigables, algunos métodos han encontrado resistencia. Por ejemplo, dos firmas no son absolutamente idénticas aunque se trate del mismo individuo.

[15] Unidad de Central de Procesamiento

Actualmente, se desconoce algún uso biométrico en la Internet. Pero como los micrófonos llegaron a ser comunes, su uso podría extenderse. Cabe indicar que existe un marco para generar claves criptográficas desde la voz, el problema es que alguien podría reproducir su voz. Quizás en el futuro las personas tendrán constantemente que disfrazar su voz excepto cuando ellos estén ingresando a su PC.

El problema real con la biometría en Internet es que la máquina remota no lee una huella digital, lee una cadena de bits. Estos bits van supuestamente desde un sensor biométrico, pero no existe forma para asegurarlo. Otro problema es que no cambia.

7. PKI

Public Key Infraestructura (PKI) es una de los más incomprendidos conceptos en seguridad. Durante un tiempo se creía que PKI era la solución mágica que podría hacer seguro cualquier sistema.

En general, PKI se refiere a un entorno donde principios (personas, computadoras, redes) poseen claves públicas y privadas, y existe algún mecanismo donde las claves públicas son conocidas por otros en un entorno confiable. Típicamente, la prueba de una clave pública es cumplida vía un certificado.