UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGURIDAD DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA

INFORME DE SUFICIENCIA

PARA OPTAR POR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

GIOVER ERGIO AYALA BUSTAMANTE

PROMOCIÓN 2004-I

LIMA – PERU
2009

SEGURIDAD DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA

A mis padres por todo su amor y apoyo

SUMARIO

El presente informe contempla las principales actividades necesarias para implementar la metodología de Seguridad de la Información en una Institución Financiera. Comentamos las tendencias actuales y las mejores prácticas. El informe se basa en mi experiencia profesional en el área de Seguridad de la Información en un Banco local. Contemplaremos los siguientes puntos: Sistemas Informáticos, Objetivos y Procesos, Análisis de Riesgo, Estrategias en Seguridad de la Información, Implementación de Controles, Monitoreo de la Seguridad y Pruebas de Seguridad.

INDICE

PROLOGO

La información es uno de los más importantes activos en una institución financiera. La protección de la información es necesaria para establecer y mantener la confianza entre la institución financiera y sus clientes, mantener el cumplimiento con la ley y proteger la reputación de la institución. Las ganancias y capital de una institución financiera se pueden ver adversamente afectadas si la información se hace conocida por personas no autorizadas, es alterada o no es disponible cuando es necesaria.

La información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad (situación que no se produce con los equipos informáticos, la documentación impresa o las aplicaciones) y, además, las medidas de seguridad no contribuyen a mejorar la productividad de los sistemas y redes informáticas, sino, mas bien, todo lo contrario, ya que pueden reducir el rendimiento de los equipos y las aplicaciones (los sistemas criptográficos, por ejemplo, consumen mayores recursos computacionales y ancho de banda en las conexiones a Internet), por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

La seguridad de la información se basa en los conceptos de: Confidencialidad, Integridad y Disponibilidad, y a partir de éstos se construye toda la arquitectura, procedimientos, controles y metodologías, las cuales serán discutidas a lo largo de éste informe cuyo objetivo principal es de mencionar las mejores prácticas y describirlas para poder tener el concepto global de la seguridad de la información en un Banco o Institución Financiera.

CAPITULO I
VULNERABILIDAD DE LOS SISTEMAS INFORMATICOS EN UNA ENTIDAD FINANCIERA

Los sistemas informáticos, como en cualquier empresa son necesarios para poder brindar la infraestructura necesaria para el transporte, almacenamiento, manejo y seguridad de la información.

En una entidad financiera se requiere que éstos sistemas y equipos sean los mas seguros y estables posibles, para tal, hay que conocer las ventajas y desventajas de cada uno de ellos y sus posibles puntos de falla para así poder garantizar el correcto funcionamiento del sistema en conjunto.

Se cuentan con diversos dispositivos de acuerdo al área de aplicación y necesidad, así para los usuarios o empleados es de uso básico para sus funciones una computadora y un teléfono, para un gerente o director es de uso obligatorio además un dispositivo móvil en donde pueda revisar su correo y mantenerse "on line", además opcionalmente es posible contar con Laptops empresariales para trabajar en varias sedes corporativas o desde casa.

1.1 Desktops y Laptops

Las computadoras de escritorio y móviles, son los terminales de trabajo de los empleados en donde cada uno interactúa ingresando, retirando o revisando información.

Para asegurar correctamente dicha información es necesario implementar diversos mecanismos de control, los cuales algunos de ellos se explicarán. Los mecanismos de control para asegurar la información mencionados en el presente informe son de los más actuales a la fecha.

En una entidad financiera corporativa a nivel internacional, usualmente se conservan estándares en todo ámbito de las Tecnologías de Información (al ser la tecnología la misma globalmente), con ciertas variaciones en cuanto a temas regulatorios de cada País. Tal es así que lo usual es encontrar estándares en equipos de oficina, Laptops, PCs, Servidores, dispositivos de red, Sistema Operativo, software, etc.

El sistema operativo base para la mayoría de las empresas (las cuales incluyen Bancos) es Windows XP. Con los Service Packs más actualizados y una correcta configuración de las políticas y mejores prácticas de seguridad el sistema puede resultar uno muy estable. Sin embargo, los sistemas informáticos basados en Windows de Microsoft constituyen el objetivo primordial de muchos atacantes, ya que es la plataforma informática más popular, con cientos de millones de usuarios en todo el mundo.

Podemos resumir en tres puntos principales lo que se recomienda para un sistema operativo Windows:

- Disponer de una imagen base con las opciones del sistema por defecto correctamente configuradas y respetando las mejores prácticas.
- Mantener una actualización de los parches del sistema periódica y priorizar las actualizaciones críticas de alto riesgo.
- Mantener el antivirus correctamente configurado y actualizado con los últimos DATs (configurar actualización automática y periódica).

La preparación de la imagen se realiza una vez y puedes durar por varios meses hasta que las condiciones del sistema cambien en una medida razonable, posteriormente se pueden ir creando nuevas imágenes mas actualizadas.

La actualización de los parches y cualquier deployment se puede realizar con herramientas de instalación remota como el SMS (System Management Server de Microsoft), lo cual me permite realizar instalaciones a grandes grupos de dispositivos centralizadamente y pre-programadas. Ver **Figuras 1.1** y **1.2**.

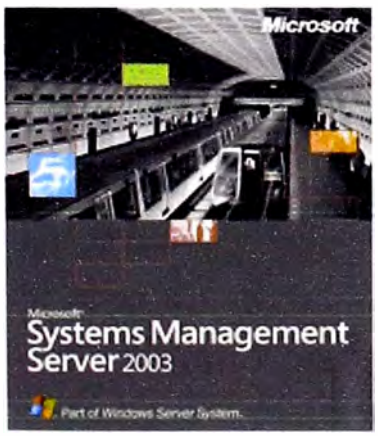

Fig. 1.1 Guía SMS

Fig. 1.2 Esquema SMS

Respecto a la actualización de la base de datos de antivirus, lo recomendable es disponer de un repositorio local a partir del cual todas las PCs, Laptops y Servidores de la empresa puedan actualizarse periódicamente. Esto contribuye a efectivizar el ancho de banda.

El área de seguridad de la información de la entidad financiera es la encargada de controlar y monitorear las amenazas de virus e informar de las mismas al área operativa para su información y/o corrección.

Los dispositivos portátiles como Laptops, deben contar en manera mandatoria con protección extra en caso de robo o extravío dado que la información almacenada en sus discos duros puede ser fácilmente visualizada por diversos mecanismos. Bajo la política de confidencialidad de la información es necesario cifrar la información que se lleva en éstos discos duros tal que si se trata de visualizar la información contenida esto no sea posible.

Herramientas como **Safeboot®** de **McAfee®** (**Figura 1.3**) cifran el disco duro de PCs y Laptops para así mitigar el riesgo de robo y uso de la información por personas no autorizadas.

Fig. 1.3 Logo Safeboot

Mas usado en Laptops (por la probabilidad de robo) éste software requiere un usuario y clave inicial antes de iniciar la carga del sistema operativo. El área de seguridad de la información de la entidad financiera son los encargados de administrar éste sistema mediante una consola que centraliza las cuentas de usuario y dispositivos.

1.1.1 Redes WIFI y puertos USB

Una red inalámbrica de datos es muy versátil dado que es posible tener conectividad de red sin cables, sin embargo dicho acceso aún cuenta con vulnerabilidades y herramientas que pueden explotar dichas vulnerabilidades o debilidades, especialmente si no se diseña una arquitectura adecuada para el soporte de seguridad.

Para tales casos, si la red de una entidad financiera, no usa redes inalámbricas de datos, es mejor deshabilitar dicha funcionalidad en las Laptops o dispositivos que lo soporten, usualmente es posible deshabilitarlo desde la opción de BIOS del dispositivo. De ésta manera evitamos el riesgo de que un usuario no autorizado que pueda "captar" la señal inalámbrica se pueda conectar a la red corporativa y robar, adulterar, visualizar o indisponer información.

Otra forma muy habitual de fuga de información, ésta vez por usuarios internos de la entidad financiera, es la del uso de dispositivos de almacenamiento masivo como memorias USB, discos duros externos, CDs/DVDs, disquetes, entre otros. Almacenar información que no sea pública de propiedad de la entidad financiera es considerado almacenar información confidencial, que no debería salir fuera de los dominios físicos de la empresa. Sin embargo el uso de estos dispositivos es cotidiano y normal para la mayoría de usuarios.

La pérdida o robo de dicha información es sumamente perjudicial para los intereses de la entidad financiera. Por ello, se deben de establecer mecanismos de control y filtrado para evitar la fuga de información (data leakage) por éstos medios. Herramientas como el **Sanctuary®** de la empresa **Lumensión®** (detallado más adelante en el presente informe) ayudan a prevenir y controlar éstas fugas.

1.2 Routers, switches y modems

Las vulnerabilidades detectadas en éstos dispositivos permiten acceder a los equipos y redes conectadas por los routers, switches o modems afectados, o facilitan la ejecución de ataques de Denegación de Servicio (DoS) que tengan como consecuencia un bloqueo total o parcial de los ordenadores conectados a través de éstos dispositivos.

Es importante mantener la correcta administración de éstos equipos, recomendando la administración centralizada mediante herramientas y metodologías adecuadas como el AAA (Authentication, Authorization, Accounting) que permite el control total, autenticación, autenticación y monitorización a detalle de éstos dispositivos permitiendo crear usuarios y diferentes perfiles asociados a los mismos según sus funciones, todo desde una plataforma centralizada y escalable. Ver **Figura 1.4**.

Fig. 1.4 AAA

Authentication: Provee el método para poder identificar a usuarios, incluyendo la forma tradicional de consulta de usuario y password y mas métodos modernos y seguros como desafío y respuesta como CHAP y claves de una sola vez (one time passwords, OTP).

Authorization: Provee el método para controlar que servicios o dispositivos el usuario autenticado tiene acceso. Muchas personas puedes tener acceso a la red, sin embargo, sólo algunas de ellas podrían tener acceso a la red core, dispositivos y servicios críticos de la misma.

Accounting: Provee el método para colectar y enviar información de seguridad. Cuando los usuarios tratan de acceder a los recursos e infraestructura de la red, el administrador de red puede querer saberlo. La información grabada puede incluir identificadores de usuario, tiempos de inicio y de fin y comandos ejecutados. La información recolectada puede ser usada para facturación, auditoria, reportes, entre otros propósitos.

Una herramienta muy adecuada para éste tipo de control es el ACS de Cisco (Cisco Secure Access Control Server). Esta herramienta provee AAA sobre los dispositivos de red **Cisco®** en la entidad financiera. Ver **Figura 1.5**.

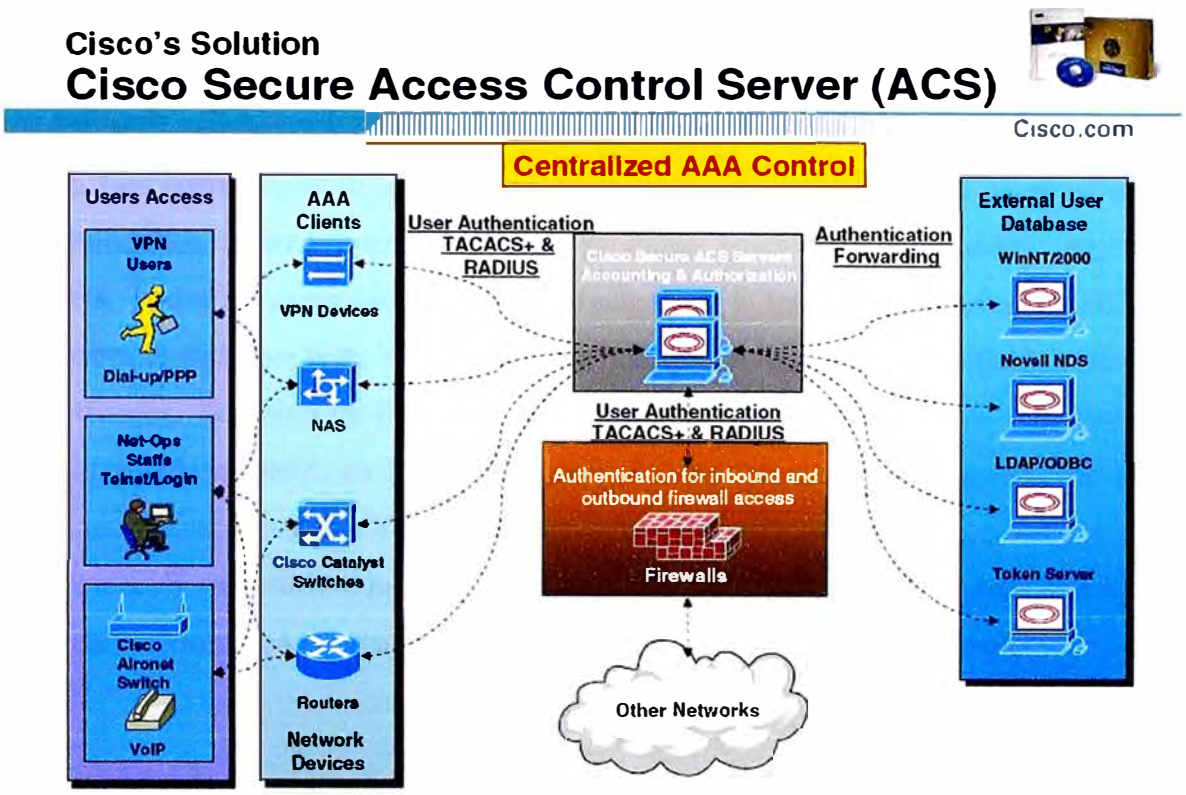

Fig. 1.5 Esquema ACS Cisco

Como medida de protección de los equipos mencionados y las redes que soportan, la institución financiera siempre debe de contar con equipos especializados como Firewalls, IPSs e IDSs. Estos equipos permiten la protección de la red ante ataques externos (vía Internet o extranet). Los Firewalls protegen la red a partir de IPs y puertos permitidos, bloqueando todos los demas. Los IPSs e IDSs protegen la red a partir del análisis de la información contenida en los paquetes analizando patrones reconocibles como riesgosos, los IPSs en modo preventivo y los IDSs en modo reactivo. A continuación damos una breve descripción de cada uno.

Firewall:

Un Firewall es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo autorizar la comunicación que realmente se requiera. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir,

limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los Firewall pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del Firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el Firewall a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un Firewall correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

IPS:

Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

IDS:

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a

una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

1.3 Dispositivos móviles

En una entidad financiera, para un gerente, director o un personal de cargo crítico, es importante mantenerse enterado en todo momento de lo que acontece o en la toma de decisiones y aprobaciones que se dan muchas veces a lo largo del día, así no esté presente físicamente en su oficina. Para tal, el dispositivo móvil se ha convertido en una poderosa herramienta para poder revisar correos, utilizar mensajería instantánea, administrar su agenda, entre otras funciones. Por ello, por el manejo de información crítica y confidencial, es necesario implementar los controles necesarios para asegurar la información contenida en los mismos.

Para citar un ejemplo, podemos destacar la solución Blackberry. Esta alternativa presenta movilidad con correo electrónico, agenda, mensajería instantánea, entre otras funciones, administradas centralizadamente desde un servidor central BES (Blacberry Enterprise Server), utilizando la comunicación de ésta data en forma segura.
BlackBerry Enterprise Solution™ se diseñó teniendo en cuenta la seguridad de los datos corporativos. Incluye un modelo de seguridad diseñado para proteger de forma continua la

información corporativa contra ataques mientras los usuarios envían y reciben correo electrónico y acceden a los datos de forma remota.

BlackBerry protege la integridad, confidencialidad y autenticidad de los datos corporativos con un esquema de cifrado seguro que cifra los datos mientras se transfieren entre BlackBerry Enterprise Server™ y los dispositivos BlackBerry®.

Cifrado Integral en Movilidad

BlackBerry Enterprise Solution ofrece dos opciones de cifrado de transporte, cifrado AES y Triple DES, para todos los datos que se transfieren entre BlackBerry Enterprise Server y el dispositivo Blackberry (**Figura 1.6**).

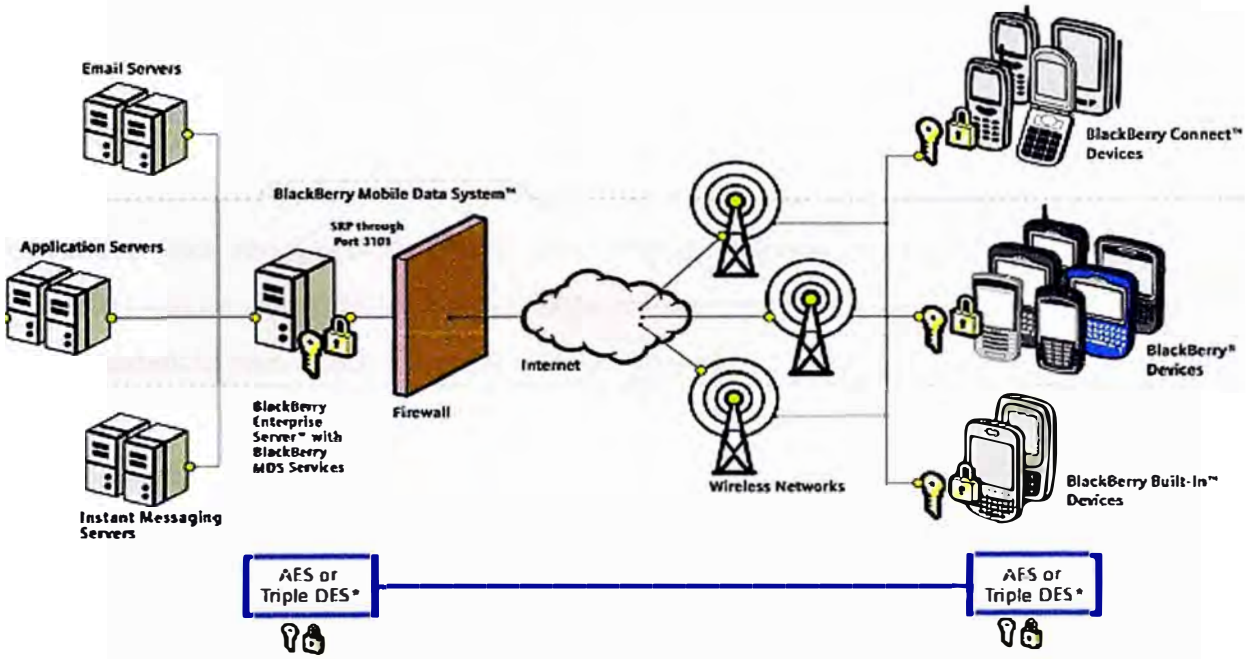

Fig. 1.6 Arquitectura BES

Seguridad de Blackberry para datos almacenados

BlackBerry extiende la seguridad corporativa al dispositivo móvil y proporciona a los administradores herramientas para administrar dicha seguridad.

Para proteger la información almacenada en dispositivos BlackBerry, es posible aplicar la autenticación por contraseña mediante las directivas de TI personalizables de BlackBerry Enterprise Server. De forma predeterminada, la autenticación por contraseña está limitada a diez intentos, después de los cuales se borra la memoria del dispositivo.

También es posible aplicar el cifrado local de todos los datos (mensajes, entradas de la libreta de direcciones, notas y tareas) a través de la directiva de TI. Además, el servicio de mantenimiento de contraseñas permite almacenar contraseñas de forma segura en el dispositivo (como contraseñas bancarias, PIN, etc.) mediante la tecnología de cifrado AES. Además, los administradores del sistema pueden crear y enviar comandos remotamente para cambiar las contraseñas de los dispositivos o bloquear o borrar información de forma remota de los dispositivos perdidos o robados.

1.4 Sistemas operativos

Los sistemas operativos se encuentran susceptibles a una gran cantidad de fallos y vulnerabilidades.

Los diversos sistemas operativos tales como Windows, Linux, MacOS, entre otros son utilizados para servidores de forma que brindan diversos servicios en la empresa. Estos servicios son de alta criticidad y necesitan estar correctamente configurados, asegurados y en redundancia para evitar los puntos únicos de falla.

1.4.1 Seguridad en servidores Windows

Se deben seguir las mejores prácticas en la configuración de los servidores. Algunas de las recomendaciones para la configuración de los servidores Windows son:

- Habilitar el password de administrador de BIOS.
- Todas las particiones utilizadas deben ser NTFS.
- Utilizar listas de control de acceso para los archivos más críticos.
- Sólo los componentes de Windows que sean necesarios deben ser instalados.
- Sólo activar los servicios que son utilizados (Ejemplo: IIS para un servidor Web).
- La cuenta de invitado debe ser deshabilitada y renombrada.
- Los passwords deben cumplir con los requisitos mínimos de complejidad.
- Habilitar las opciones necesarias para audits y logs.

- El antivirus debe ser instalado y actualizado (revisión de actualizaciones cada 24 horas a lo mucho).

1.4.2 Comparativa de sistemas operativos para servidores

Existen tres alternativas a la hora de elegir un sistema operativo para un servidor web: Microsoft, Unix y Linux. A continuación se analizan algunas de las principales características de cada una de las opciones, así como sus ventajas y desventajas.

Microsoft

Una implantación bajo el entorno que proporciona Microsoft, cuenta en primer lugar con la completa integración de todos los servicios que se escojan (web que interactúa con servidores de correo Exchange, SQL Server, IIS, Noticias, nuevos entornos de desarrollo como la tecnología .NET, etc.). A su vez, podemos contar con el soporte que las licencias que adquiramos nos proporciona ante cualquier problema que se nos pueda plantear (muy útil es situaciones críticas de pérdida de información).

Entre las desventajas de la opción de Microsoft aparecen los aspectos de seguridad y rendimiento. Quizá debido al constante análisis al que se encuentran sometidos, los productos Microsoft poseen una larga lista de fallos de seguridad publicados, y se ven sometidos a constantes actualizaciones (Service Packs). A la hora de adquirir hardware, también debemos saber que las necesidades de memoria y velocidad de proceso aumentan cuando elegimos este modelo de implantación.

Unix

Decantarnos por SUN Microsystems soluciona algunos de los problemas que plantea Microsoft. SUN proporciona una solución completa a niveles hardware y software. Algunos proveedores, como Oracle, cobran más cara una licencia de un producto que vaya a ejecutarse bajo un procesador SPARC (multiplicadores de 1,5 por encima de la ejecución por procesadores INTEL), debido a sus altas prestaciones. En seguridad, contamos con el

sistema operativo Solaris (un modelo comercial de UNIX), que proporciona características nativas orientadas a evitar un uso y accesos inadecuados al sistema.

Linux

Avanzando terreno están las soluciones basadas en GNU (software de uso público) como Linux. El nacimiento de distribuciones comerciales (RedHat, S.U.S.E o Caldera) y entornos de instalación y uso más amigables (Gnome, KDE) hacen de Linux una de las mejores soluciones existentes en el momento.

Hoy por hoy existen aplicaciones gratuitas o semigratuitas para suplir las necesidades de cualquier empresa: MySQL como sistema gestor de base de datos (adoptado recientemente por la NASA), Apache como servidor web, PHP, servidor de aplicaciones ZOPE, proyectos de clustering como LVS dotan a las implantaciones Linux de potencia y prestaciones a muy bajo coste. Además, al funcionar bajo plataformas INTEL, no nos vemos obligados a depender de un proveedor, como era el caso de SUN.

Para una comparativa entre los distintos sistemas operativos ver **Tabla 1.1**. Referencia 8 de Bibliografía.

TABLA 1.1 Comparación entre sistemas operativos

Características de los proveedores de soluciones

	Coste	Presta-ciones	Segu-ridad	Inte-gración	TOTAL
Microsoft	8	7	6	10	7,75
Unix	5	10	9	8	8
Linux	10	9	9	7	8,75

CAPITULO II
SEGURIDAD DE LA INFORMACION, OBJETIVOS Y PROCESOS

La seguridad de la información permite a una institución financiera conocer sus objetivos empresariales implementando sistemas con la consideración de los riesgos relacionados de las tecnologías de información de la organización, socios de negocios, alianzas, proveedores de servicios de tecnología y clientes.

2.1 Objetivos

Las organizaciones alcanzan éste objetivo logrando lo siguiente:

- Disponibilidad
- Integridad de la información o sistemas
- Confidencialidad de la información o sistemas
- Responsabilidad
- Aseguramiento

Disponibilidad- La disponibilidad de sistemas se refiere a los procesos, políticas y controles usados para asegurar el rápido acceso a los usuarios autorizados. Este objetivo protege el que usuarios legítimos puedan ser afectados en los accesos a sistemas e información intencional o no intencionalmente. Existen estándares en el tema de la disponibilidad, tal como en un Datacenter, el cual alberga los principales equipos de la infraestructura de la institución financiera (ver **Anexo C** para más detalle).

Integridad de Datos y Sistemas- Sistemas e integridad de datos tratan sobre los procesos, políticas y controles usados para asegurar que la información no ha sido alterada de una manera no autorizada y que los sistemas están libres de manipulación no autorizada que comprometan la exactitud y la confiabilidad de la información.

Contabilidad- Contabilidad clara trata sobre los procesos, políticas y controles necesarios para trazar las acciones hacia su fuente. Contabilidad directamente soporta la disuasión, prevención de intrusos, monitoreo de la seguridad, recuperación y admisión legal de registros.

Aseguramiento- Aseguramiento trata sobre los procesos, políticas y controles usados para desarrollar confianza en que las mediciones técnicas y operacionales de seguridad trabajan como deben. Los niveles de aseguramiento son parte del diseño de sistemas e incluyen disponibilidad, integridad, confidencialidad y contabilidad. Aseguramiento resalta la noción que sistemas seguros brindan la funcionalidad requerida mientras se evitan acciones no deseadas.

Integridad y contabilidad se combinan para producir lo que es conocido como "no-rechazo" (non-repudation). No-Rechazo ocurre cuando la institución financiera demuestra que los originadores que iniciaron la transacción son quienes ellos dicen que son, el receptor es la parte pretendida, y no ocurren cambios en el tránsito o almacenamiento. No-rechazo puede reducir el fraude y promover el reforzamiento legal de acuerdos electrónicos y transacciones. Mientras no-rechazo es una meta y es conceptualmente clara, la manera en que no-rechazo puede ser lograda para sistemas electrónicos en una manera practica y legal puede tener que esperar por clarificación judicial.

2.2 Guía regulatoria, recursos y estándares

Instituciones financieras desarrollando o revisando sus controles en seguridad de la información, políticas, procedimientos o procesos tienen una variedad de fuentes sobre las que se pueden dibujar. Primero, leyes federales y regulaciones brindan el lineamiento de seguridad y los reguladores han realizado numerosos documentos y guías relacionados al tema de seguridad. Las instituciones adicionalmente cuentan con terceros, fuentes de seguridad de la industria para bosquejar las guías, incluyendo auditores externos, firmas consultoras, compañía de seguros y organizaciones profesionales en seguridad de la información. Adicionalmente, muchas organizaciones estandarizadoras nacionales e internacionales están trabajando para definir los estándares de seguridad y las mejores prácticas para el comercio electrónico. Mientras no existan estándares aceptados para la seguridad de la información, estos estándares proveen lineamientos que instituciones financieras y sus reguladoras pueden seguir para el desarrollo de las expectativas de la

industria y prácticas de seguridad. Algunos de los grupos de definidores de estándares incluyen las siguientes organizaciones:

- El Insituto Nacional de Estandares y Tecnología (National Institute of Standars and Technology - NIST) en www.nist.gov

- La organización Internacional para Estandarización (International Organization for Standardization - ISO) tecnología de la Información en www.iso.ch con estándares específicos como:

El código de práctica para la administración de la seguridad de la información (ISO/IEC 17799) y Tecnología de la Información - Técnicas de Seguridad - Criterios de evaluación para IT Security (ISO/IEC 15408); y la asociación en Sistemas de Información Auditoría y Control (ISACA) - Objetivos de Control para Tecnología de Información (COBIT), en www.isaca.org/cobit.htm.

2.3 Procesos

El proceso de seguridad es el método que una organización usa para implementar y łograr sus objetivos en seguridad. El proceso es diseñado para identificar, medir, administrar y controlar los riesgos de los sistemas, disponibilidad de la información, integridad y confidencialidad.

Los procesos incluyen 4 áreas que sirven como base de éste informe:

- Análisis de riesgo de la información
- Estrategia de la seguridad de la Información
- Implementación de Controles de Seguridad
- Monitoreo de la Seguridad y Actualizaciones

Análisis de Riesgo de la Seguridad de la Información

Un proceso para identificar y evaluar amenazas, vulnerabilidades, ataques, posibilidades de ocurrencia y hallazgos.

Estrategia de Seguridad de la Información

Un plan para mitigar el riesgo que integra la tecnología, políticas, procedimientos y entrenamiento. El plan debería ser revisado y aprobado por el jefe de directores.

Implementación de Controles de Seguridad

La adquisición y operación de tecnología, la asignación específica de deberes y responsabilidades hacia gerentes y staff, el desarrollo de controles apropiados de riesgo y el aseguramiento que gerentes y satff entienden sus responsabilidades y tienen el conocimiento, habilidades y motivación necesaria para cumplir sus necesidades.

Monitoreo de la Seguridad y Actualizaciones

El uso de varias metodologías para asegurarse que los riesgos son apropiadamente realizados y mitigados. Estas metodologías deberían ser verificar que los controles son efectivos y funcionando como deberían. Monitoreo y actualización de los nuevos riesgos encontrados en éste monitoreo continuo hace el proceso continuo en vez de un evento de una sola vez.

Riesgos de seguridad incluyen amenazas, vulnerabilidades, técnicas de ataque, frecuencia esperada de ataque, operaciones y tecnología de instituciones financieras y posturas de defensa de las instituciones financieras. Todas éstas variables cambian constantemente. Por tanto, la administración de los riesgos de una institución requiere un proceso continuo.

CAPITULO III
ANALISIS DE RIESGO DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA

Las instituciones financieras deben mantener constantes análisis de riesgo de la información que efectivamente:

- Obtenga datos acerca de la información y activos tecnológicos de la organización, amenaza a éstos activos, vulnerabilidades, procesos y controles de seguridad existentes y los estándares y requerimientos de seguridad actuales.
- Analice la probabilidad e impacto asociado con las amenazas y vulnerabilidades conocidas; y
- Priorice los riesgos presentes debido a amenazas y vulnerabilidades para determinar el nivel apropiado de entrenamiento, controles y aseguramiento necesario para un mitigamiento efectivo.

Análisis de riesgos de seguridad de la información es el proceso usado para identificar y entender riesgos a la confidencialidad, integridad y disponibilidad de la información y sistemas. En su forma más simple, un análisis de riesgo consiste de la identificación y valoración de activos y un análisis de ésos activos en relación a amenazas y vulnerabilidades potenciales, resultando en un orden de riesgos a mitigar. La información resultante debería ser usada para desarrollar estrategias para mitigar esos riesgos.

Una evaluación adecuada identifica el valor y sensibilidad de la información y componentes de sistemas, posteriormente balancea el conocimiento con la exposición de amenazas y vulnerabilidades. Un análisis de riesgo es un pre-requisito para la información de estrategias que guían la institución mientras desarrolla, implementa, testea y mantiene su postura de seguridad de información de sistemas. Un análisis de riesgo inicial puede

envolver un esfuerzo considerable de tiempo, pero el proceso de análisis de riesgo debe ser una constante en el programa de la seguridad de la información.
De los resultados de los análisis de riesgo de los distintos procesos que tiene la institución financiera se obtendrán riesgos bajos, medios bajos, medios y altos. Se pueden usar letras para identificar cada uno de ellos.

Los riesgos de resultado alto, deben ser mitigados lo más antes posible. Se recomienda establecer planes de acción con fechas programadas en conjunto con las áreas y personas involucradas para el establecimiento de los planes de acción.

Mitigar un riesgo podría ocasionar gastos considerables en una institución financiera, la decisión debe ser tomada para asumir el costo o ver alguna otra alternativa, que podría ser menos eficiente o mas operativa pero que puede llegar a mitigar el riesgo o al menos bajarlo a un nivel medio o bajo.

Para la evaluación del nivel del riesgo ver **Anexo B** del presente informe.

CAPITULO IV
ESTRATEGIA PARA LA SEGURIDAD DE LA INFORMACIÓN

Las instituciones financieras deben de desarrollar una estrategia que defina objetivos de control y establezca un plan de implementación. La estrategia de seguridad debe incluir:

- Consideraciones apropiadas para prevención, detección y mecanismos de respuesta.
- Implementación del concepto de menos permisos y menos privilegios.
- Control por capas que establezca múltiples puntos de control entre amenazas y los activos de la organización
- Políticas que guíen a los jefes y empleados en implementar el programa de seguridad.

Una estrategia de seguridad de la información es un plan para mitigar riesgos mientras se cumplen los requerimientos legales, contractuales y requerimientos internos desarrollados. Los típicos pasos para construir una estrategia incluyen la definición de objetivos de control, la identificación y pruebas de aproximación para conocer los objetivos, la selección de controles, el establecimiento de puntos de referencias y métricas y la preparación de implementaciones y planes de testeo.

4.1 Conceptos claves

La seguridad requiere la integración de personas, procesos y tecnología. Cada uno de los tres conceptos deben ser administrados considerando las capacidades y limitaciones de los otros componentes. Cuando los componentes son considerados totalmente, deberían brindar una adecuada mitigante a los riesgos existentes.

Estrategias de seguridad deben establecer limitaciones de acceso y limitaciones para la habilidad de realizar acciones no autorizadas. Estas limitaciones derivan de conceptos conocidos como dominios de seguridad, menos permisos y menos privilegios.

Las instituciones financieras deben diseñar múltiples capas de controles de seguridad para establecer muchas líneas de defensa entre el atacante y el activo siendo atacado.

Un ejemplo de seguridad en Internet de éste concepto puede incluir la siguiente configuración:

Un router con estrictas reglas de control de acceso, en frente de un Firewall de nivel de aplicación, en frente de servidores Web, en frente de un servidor transaccional, en frente de un servidor de base de datos, con sistemas de detección de intrusos ubicados en varios puntos entre los servidores y en ciertos hosts. Ver **Figura 4.1**.

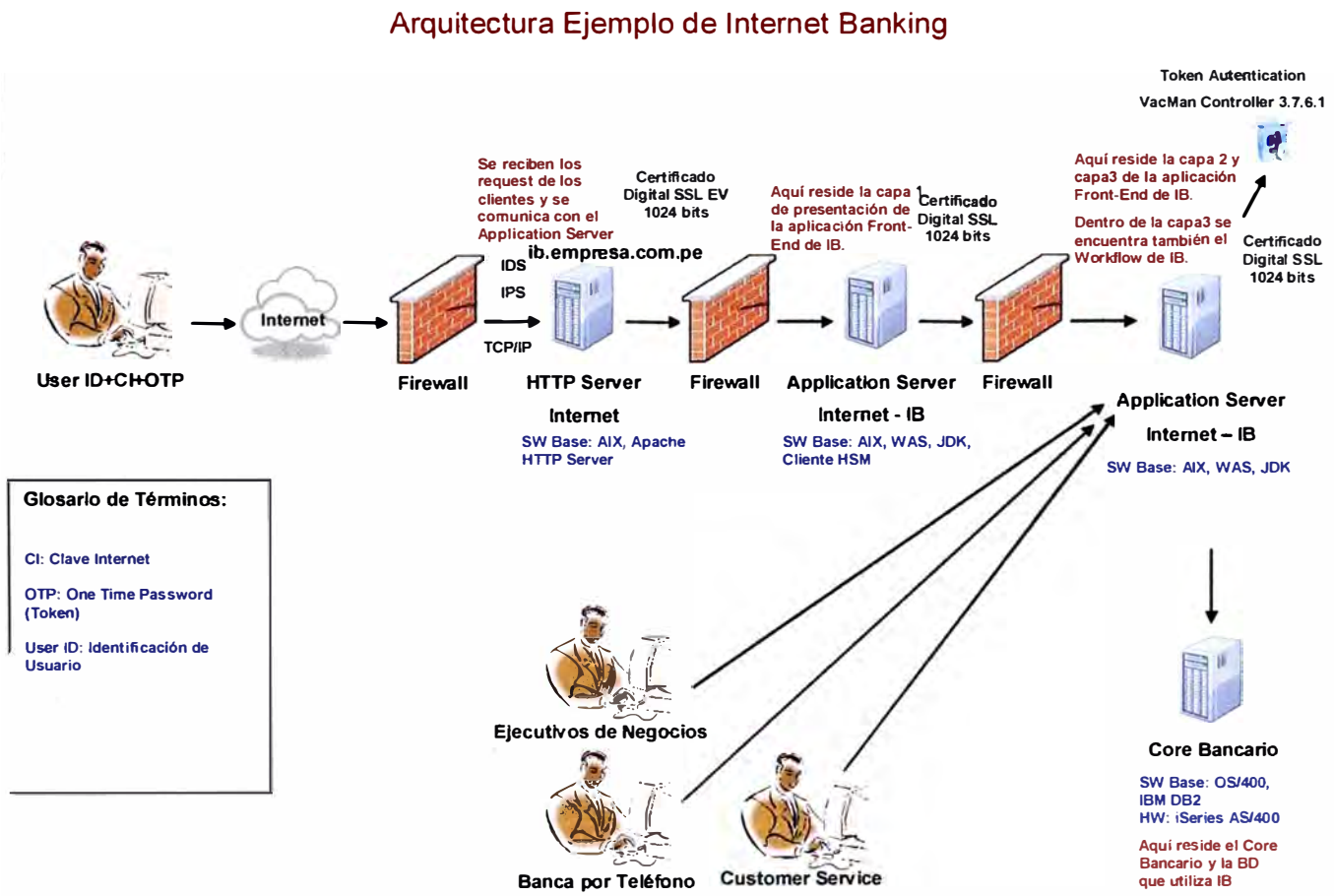

Fig. 4.1 Diagrama modelo de arquitectura de Internet Banking

4.2 Reacción rápida ante incidentes de seguridad

Un procedimiento claro y directo ante respuestas a incidentes de seguridad debe ser establecido. Un evento de seguridad al momento de ser detectado debe ser mitigado inmediatamente para posteriormente hacerse un seguimiento inmediato al atacante o falla. Tales eventos pueden ser generados por ejemplo por atacantes (hackers) o virus o troyanos.

Posteriormente, el evento debe ser documentado y archivado para el conocimiento del área de seguridad como un precedente y evitar su futura ocurrencia.

4.3 Autorizaciones de acceso

En una institución financiera existen distintos sistemas necesarios por las distintas áreas de la empresa. Para que a un usuario se le otorgue el acceso a dichos sistemas requiere pasar por una política de autorizaciones. El área de seguridad de la información de la institución financiera debe tener bien en claro la lista de autorizadores por sistema y perfil necesario basados en los dueños de la información y criticidad de acceso al mismo.

Estos accesos deben ser ratificados o depurados periódicamente por un proceso de certificación. De esta manera se mantiene la política de otorgar los permisos necesarios y suficientes que requieren los empleados de la institución financiera.

Por ejemplo: Si la institución financiera cuenta con una base de datos SQL, dicho sistema cuenta con usuarios los cuales tienen permisos sobre diversas bases de datos con diferentes perfiles tales como lectura, escritura, dueño, etc. Estos accesos debe ser ratificados o depurados periódicamente por el dueño de la información y el dueño de la plataforma tal que sólo se otorguen los permisos necesarios, por decir, un usuario que cambió de puesto y ya no necesita el acceso. Realizar ésta certificación también ayuda en los temas de auditorias a sistemas.

CAPITULO V
IMPLEMENTACION DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

5.1 Control de acceso

El objetivo del control de acceso es el de permitir acceso a personas y dispositivos autorizados y denegar el acceso a otros.

Personas autorizadas pueden ser empleados, proveedores de servicios de tecnología, contratistas, clientes o visitantes. El acceso debe ser autorizado y brindado solamente a individuos cuya identidad es establecida y sus actividades deben ser limitadas a las mínimas requeridas por el propósito de sus actividades.

Dispositivos autorizados son aquellos que su colocación en la red es aprobada en concordancia con las políticas de la institución. Controles de cambio son usados típicamente para dispositivos dentro del perímetro externo y para configurar los dispositivos de la institución para aceptar conexiones autorizadas desde fuera del perímetro.

5.2 Administración de derechos de acceso

Las instituciones financieras deben contar con un proceso efectivo para administrar derechos de usuario. El proceso debe incluir:

- Asignar a los usuarios y dispositivos sólo el acceso requerido para el desarrollo normal de sus funciones.
- Actualizar derechos de acceso basados en personal o cambios en sistemas.
- Revisión periódica de los derechos de acceso de los usuarios en una frecuencia adecuada basados en el riesgo de la aplicación o el sistema.

- Diseñar políticas apropiadas de aceptación de usuario y requerir a los usuarios su aceptación a ésta en forma escrita.

El acceso a los sistemas de la institución financiera debe ser limitado y autorizado. No se debe suponer un acceso, es necesario que el mismo se requiera por una persona que tenga la facultad de autorizar el mismo. Adicionalmente a requerir un acceso se debe definir el perfil con el que se requiere, el perfil se refiere a lo autorizado a hacer en el sistema una vez que tiene acceso al mismo.

Para citar un ejemplo:

Un empleado recién contratado por la institución financiera. Al área de seguridad de la información o la encargada de administrar los accesos a los sistemas le debe llegar una solicitud formal de creación de accesos desde el área de recursos humanos u otra autorizada. La solicitud debe contar con el detalle de que accesos a sistemas y con que perfil éste nuevo usuario debe contar. Para el caso de una empresa financiera Peruana por ejemplo se puede requerir acceso a: Active Directory, correo electrónico, archivos compartidos en red, si requiere Internet o no, acceso a páginas de consulta financiera como SBS, Infocorp, acceso a páginas de validación de identidad como RENIEC, acceso al Core Bancario especificando el perfil, entre otros.

Para el caso de éste nuevo empleado es crítico validar la identidad del mismo al momento que él solicita el acceso al área de administración de accesos (usualmente vía telefónica). Para tal se pueden implementar mecanismos de validación como fecha de nacimiento, número de DNI y un código inicial que recursos humanos le puede hacer llegar al momento de su presentación al Banco, éste código inicial debe ser validado por la persona encargada de entregarle sus accesos iniciales como cuenta de red (Active Directory de Microsoft por ejemplo) y correo electrónico.

Para las rotaciones internar de personal se debe implementar mecanismos para los cambios en accesos a sistemas. El área de recursos humanos u otra autorizada debe publicar el cambio al área de administración de accesos y otras que necesitan dicha información como administración o seguridad física, indicando la fecha de aplicación de baja de accesos y

habilitación de los nuevos por asumir nuevas funciones. Esta baja y alta de accesos debe ser coordinado con el usuario para no alterar sus funciones normales en el banco.

Los accesos del personal deben ser revalidados en una frecuencia de acuerdo a la criticidad y riesgo de acceso al sistema. Este proceso se denomina certificación de sistemas y debe ser autorizado y firmado por el dueño de la información y una persona de reemplazo con facultad de autorizar cambios en caso la principal esté ausente.

En la certificación se debe de incluir sustento de los accesos a sistemas actuales de cada empleado (por ejemplo reportes originarios del sistema) adjunto a un resumen del mismo. El perfil sobre dicho sistema debe ser autorizado y revalidado tanto como el acceso. Se debe realizar a todo sistema o software que la institución financiera tenga implementado.

Las políticas de acceso a sistemas de la institución financiera usualmente necesitan tener dispensa para casos puntuales plenamente justificados. Dicha dispensa debe ser firmada por el solicitante, el gerente de seguridad de la información y el director del área. La dispensa debe nombrar los riesgos y el compromiso del usuario a cumplirlos y aceptarlos.

5.3 Autenticación

Las instituciones financieras deben usar un efectivo método de autenticación apropiados para los niveles de riesgo. Los pasos incluyen:

- Seleccionar mecanismos de autenticación basados en el riesgo asociado con el servicio o aplicación en particular.
- Considerar si se debe usar autenticación de múltiple factor para una aplicación, teniendo en cuenta que dicho mecanismo cada vez es mas necesario para muchas formas de banca electrónica y actividades de pagos electrónicos.
- Cifrar la transmisión y almacenamiento de autenticadores (por ejemplo: claves, números de identificación personal (PINs), certificados digitales y plantillas biométricas).

Autenticación es la verificación de identidad por un sistema basado en la presentación de credenciales únicas para ése sistema. Las credenciales únicas están en la forma de algo que el usuario conoce, algo que el usuario tiene o algo que el usuario es. Esas formas existen como secretos compartidos, tokens o biométricas. Más de una forma puede ser usada en cualquier proceso de autenticación. La autenticación que es basada en más de una forma se denomina autenticación de múltiple factor y es generalmente más fuerte que el método de autenticación simple.

Los autenticadores deben ir cifrados, es decir, los usuarios y claves a los sistemas cada vez que se validan con el servidor de autenticación deben viajar en forma cifrada así como su almacenamiento en los host o servidores. De ésta manera, si una persona intercepta el tráfico de red no podrá visualizar las credenciales, de igual manera si una persona no autorizada llega a tener acceso a los servidores de autenticación, los archivos que almacenan dichas claves deben estar cifrados.

La autenticación en una entidad financiera esta en prácticamente cada sistema que ésta maneja y dependiendo del nivel de criticidad se pueden establecer niveles mas complejos. Por ejemplo: Se puede exigir claves más complejas como pedir al menos 8 caracteres que al menos 1 sea numérico y otros alfanuméricos con al menos 1 combinación entre mayúscula y minúscula y que además caduque cada 2 meses y que la nueva clave debe ser distinta cada vez y que no pueda contener nombres o apellidos.

Otra forma de hacer mas compleja la autenticación, con la intención de que sea mas segura, es la de usar múltiples factores, como el uso de un token. El token es un dispositivo cuya numeración cambia en el tiempo (clave variable). Es usado principalmente en las instituciones financieras para conexiones a páginas de Banca por Internet, la clave de IB (Internet Baking) correspondería a una clave fija + la clave variable del token. Otro uso común del token es para realizar conexiones VPN mas seguras, como para que un trabajador remoto se conecte vía Internet a sistemas del banco. Cabe resaltar que una conexión VPN es segura por el lado de confidencialidad pues cifra la data transmitida y el token le da un nivel adicional de seguridad a la autenticación.

5.4 Seguridad física

Las instituciones financieras deben definir zonas de seguridad física e implementar controles apropiados de prevención y detección en cada una de estas zonas para protegerse contra el riesgo de:

- Penetración física por personas maliciosas o no autorizadas.
- Daño hecho por contaminantes ambientales y
- Penetración electrónica a través de emisiones activas o pasivas.

La confidencialidad, integridad y disponibilidad de la información puede verse afectada por intrusión física no autorizadas, daño o destrucción de componentes físicos. Conceptualmente, esos riesgos en seguridad física son mitigados con la implementación de zonas de seguridad. Los requerimientos en seguridad de dichas zonas están en función de sensitividad de la información contenida o de los componentes informáticos presentes en la zona. Por ejemplo, el data center debe estar en la zona de seguridad mas alta mientras que una oficina administrativa podrí estar en la mas baja. Diferentes zonas de seguridad pueden existir dentro de la misma infraestructura. Por ejemplo, los Routers, Switches y Servidores en una agencia del banco, deben estar protegidos en un ambiente especial denominado Cuarto de Comunicaciones, donde sólo personal autorizado tenga la llave de acceso al mismo. Adicionalmente dicho cuarto debe estar monitoreado con las cámaras de seguridad de la empresa 24x7.

5.5 Cifrado

Las instituciones financieras deberían utilizar cifrado para mitigar el riesgo de visualización y alteración de la información de información sensible almacenada y en tránsito. Las implementaciones de cifrado deberían incluir:

- Fortaleza de cifrado suficiente para proteger la información de ser visualizada hasta el momento en que se pueda no sea un riesgo.
- Prácticas eficientes de administración de llaves.

- Fiabilidad robusta, y
- Protección apropiada de los puntos de comunicación cifrados.

El cifrado es usado para asegurar la comunicación y almacenamiento de data, particularmente credenciales de autenticación y transmisión de información sensible. Puede ser usada por todo un entorno tecnológico, incluyendo sistemas operativos, capas medias (middleware), aplicaciones sistemas de archivos y protocolos de comunicación.

El cifrado puede ser usado como un control preventivo, un control detectivo o ambos. Como un control preventivo, el cifrado actúa para proteger la información de ser visualizada por terceros no autorizados. Como un control detectivo, el cifrado es usado para permitir descubrir cambios no autorizados de la información y de asignar responsabilidad de la información a partes autorizadas. Cuando la prevención y la detección son juntadas, el cifrado es un control clave para asegurar la confidencialidad, integridad y aseguramiento de la información.

El cifrado correctamente usado puede reforzar la seguridad de los sistemas de una institución. Adicionalmente, sin embargo, el cifrado tiene el potencial de debilitar otros aspectos de seguridad. Por ejemplo, la información cifrada puede debilitar drásticamente la efectividad de cualquier mecanismo de seguridad basado en inspección de data, tales como escaneo de anti-virus y sistemas de detección de intrusos. Cuando se usan comunicaciones cifradas, las redes pueden tener que ser reconfiguradas para permitir una detección adecuada de código malicioso e intrusión en sistemas.

Las instituciones financieras deben emplear algoritmos de cifrado lo suficientemente robustos para proteger la información de ser visualizada. Por ejemplo, los autenticadores deben ser cifrados con la robustez suficiente para permitir a la institución tiempo para detectar y reaccionar a un autenticador falso antes que un atacante pueda descifrar los autenticadores robados.

Las decisiones acerca de que data cifrar y en que puntos cifrar la data son típicamente basadas en el riesgo de la visualización y los costos y riesgos del cifrado. Los costos

incluyen gastos elevados en hosts y redes. Generalmente hablando, los autenticadores son cifrados tanto en redes públicas como en la misma institución financiera.

El cifrado no puede garantizar la seguridad de la data. Incluso si el cifrado es usado apropiadamente, por ejemplo, una brecha de seguridad en uno de los puntos extremos de la comunicación puede ser usada para robar la data o permitir un intruso hacerse pasar como un usuario legítimo del sistema.

5.5.1 Como trabaja el cifrado

En general, el cifrado funciona tomando una data y una variable, llamada "llave" y procesar éstos items por un algoritmo establecido para crear un texto cifrado. La fuerza del texto cifrado es determinada por la entropía o el grado de incertidumbre en la llave y el algoritmo. La longitud y selección de la llave son importantes determinantes para la entropía. Llaves de longitud mayor generalmente determinan mayores posibilidades de llaves. Más importante que longitudes de llaves, sin embargo, es la limitación de posibles llaves impuestos por el criterio de selección de la misma. Por ejemplo, una llave de 128 bits tiene mucha menos entropía si sólo se usan letras y números. La entropía máxima de 128 bits se alcanza sólo cuando la llave es aleatoriamente seleccionada dentro del rango entero de 128 bits.

El algoritmo de cifrado es también importante. Crear un algoritmo matemático que no limita la entropía de la llave y testear el algoritmo para asegurar su integridad es difícil. Dado que la fuerza de un algoritmo es relacionado a maximizar la entropía, en lugar de mantenerse ocultos, los algoritmos son generalmente hechos públicos y sujetos a análisis. Mientras mas se analiza un algoritmo para su análisis por expertos mas se puede aseverar como trabajará. Ejemplos de algoritmos públicos son AES, DES y 3DES, HSA-1 y RSA.

Existen 3 tipos de cifrado: El hash criptográfico, el cifrado simétrico y el cifrado asimétrico.

5.6 Prevención de código malicioso

Las instituciones financieras deben protegerse de los riesgos de códigos maliciosos implementando controles adecuados a nivel de host y red para prevenirse de los mismos y a la vez mejorar la educación adecuada del usuario.

5.7 Desarrollo, adquisición y mantenimiento de sistemas

Las instituciones financieras deben asegurar que los sistemas sean desarrollados, adquiridos y mantenidos con los controles de seguridad adecuados. Los pasos incluyen:

- Asegurarse que los sistemas sean desarrollados e implementados con las funciones de seguridad apropiadas.
- Asegurarse que el software sea confiable implementado controles apropiados en el proceso de desarrollo, revisión de código fuente, revisión de la historia y la reputación de los vendors y desarrolladores terceros, además de implementar los controles adecuados fuera del software para mitigar el inaceptable riesgo de cualquier deficiencia.
- Mantener apropiadamente una sólida administración de la configuración y proceso de control de cambio.
- Establecer un efectivo proceso de parches de sistemas y software.

El software es la base más importante en la infraestructura tecnológica de una institución financiera. El software debe proveer los requerimientos de la institución respecto a controles de seguridad, debe ser protegido de uso inadecuado y ser mantenido a un nivel que sea confiable.

5.7.1 Desarrollo y adquisición de software

Las instituciones financieras obtienen software por desarrollo propio, desarrollo por contratistas, compra de código pre-escrito o varios de esos desarrollos y adquisiciones. Los temas de seguridad asociados con los pedidos incluyen los controles de seguridad implementados dentro del código y la confianza del código que es puesto en producción en

la institución financiera. Las características de seguridad del código puede ser evaluado cualquier sea el caso del desarrollo o adquisición. La confianza del código, sin embargo, es establecida de una forma distinta dependiendo de la disponibilidad de la información necesaria para realizar la evaluación.

5.7.2 Control de cambios a los ambientes

Las instituciones financieras deben tener un adecuado proceso para introducir cambios en aplicaciones y sistemas en sus ambientes. El proceso debe abarcar, desarrollo, implementación y testeo de cambios tanto a software desarrollado internamente como adquirido. Procedimientos débiles pueden corromper aplicaciones e introducir nuevas vulnerabilidades en seguridad. Las consideraciones en control relacionados a seguridad deben incluir:

- Restringir cambios a usuarios autorizados.
- Repasar el impacto que los cambios tendrán en los controles de seguridad.
- Identificar todos los componentes de sistemas que son afectados por los cambios.
- Asegurarse que el dueño de la aplicación o sistema halla autorizado los cambios antes del impacto.
- Mantener un estricto control de versiones de todas las actualizaciones de software.
- Mantener pistas de auditoría para los cambios.

Cambios a sistemas operativos pueden degradar la eficiencia y efectividad de aplicaciones que se basan en el sistema operativo para conectarse a la red, otras aplicaciones o datos. Generalmente, la administración debe implementar un proceso de control de cambios a sistemas operativos similar al usado para controlar los cambios a las aplicaciones. Adicionalmente, la administración de cambios debe revisar las aplicaciones siguiendo los cambios a sistemas operativos para proteger al sistema de un problema en la seguridad o la integridad de las operaciones. Se deben usar librerías de software aisladas para la creación

y mantenimiento de software. Típicamente, librerías separadas existen para los ambientes de desarrollo, pruebas, pre producción y producción.

Así como a los sistemas operativos, control de cambios debe crear un procedimiento similar para los cambios en equipos de comunicaciones y seguridad como Routers, Switches, Firewalls, etc. Estos cambios deben ser también autorizados y monitoreados con herramientas que centralicen los eventos y cambios en scripts. Así cualquier cambio a los mismos se almacena para pode seguir una pista en caso de un problema o cambio no autorizado.

El procedimiento debe incluir una hoja de control de cambio que incluyan las firmas del ejecutor del cambio, el supervisor del cambio, el dueño de la plataforma, el dueño de la aplicación el área de administración de cambios y el área de seguridad de la información. Se debe atachar a éste documento las instrucciones del cambio y las instrucciones de vuelta atrás. Así también indicar un resumen de la tarea a realizar, la fecha de impacto la criticidad del cambio y la urgencia del mismo. En la **Figura 5.1** se muestra un formato típico.

5.8 Protección de la data

Las instituciones financieras deben controlar y proteger el acceso a documentos, videos y medios basados en computadoras para evitar la perdida, fuga o daño de la información. Las instituciones deben:

- Establecer y asegurar el cumplimiento con las políticas para el manejo y almacenamiento de la información.
- Asegurar los medios de almacenamiento.
- Asegurar la información en tránsito o la transmisión a terceros.

Los backups o copias de respaldo realizados los servidores, debe ser cifrada y almacenada en medios seguros y confiables. El password para descifrar dicha información en caso necesite ser usada debe ser resguardado en sobre y guardado en bóveda.

LOGO DE LA INSTITUCIÓN FINANCIERA	FECHA DE EMISIÓN:	RESPONSABLE:	NÚMERO:

FORMATO DE CONTROL DE CAMBIOS EN INFRAESTRUCTURA

EQUIPO IMPACTADO				
UBICACIÓN FÍSICA DEL EQUIPO				
PLATAFORMA IMPACTADA	☐ AS400 - ☐ WINDOWS - ☐ CISCO IOS ☐ - OTROS:_____			
AMBIENTE IMPACTADO	☐ Desarrollo - ☐ Pruebas - ☐ Pre Producción - ☐ Producción			
DESCRIPCIÓN DEL CAMBIO				
Tipo de Infraestructura cambiada	☐ Hardware - ☐ Software - ☐ Otros: _____			
Servicio Impactado:		Corte Servicio: ☐ Si - ☐ No	T.Aprox.Corte: _____	
TIPO DE IMPACTO	☐ PROGRAMADO	EMERGENCIA ☐ URGENCIA ☐ INCIDENCIA	☐ OBSOLETO	
TIPO DE CAMBIO	☐ Implementación - ☐ Corrección - ☐ Mantenimiento - ☐ Nuevo Requerimiento			
CLASIFICACIÓN DE RIESGO	☐ Alto - ☐ Medio - ☐ Bajo			
ADJUNTA	☐ Instr. de vuelta atrás ☐ Instr. del cambio ☐ Documentación			
FECHA DEL CAMBIO				
IMPACTO EN LA SEGURIDAD	☐ No tiene impacto en los estándares de seguridad. ☐ Si tiene impacto en los estándares de seguridad controlados con el cambio propuesto			
DUEÑO DE LA APLICACIÓN (Solo si el cambio afecta el desempeño de la aplicación)		Fecha	Firma	
SUPERVISOR DEL CAMBIO		Fecha	Firma	
DUEÑO DE LA PLATAFORMA		Fecha	Firma	
IT OPERACIONES		Fecha	Firma	
SEGURIDAD DE LA INFORMACIÓN		Fecha	Firma	
CONTROL DE CAMBIOS		Fecha	Firma	
RESULTADO DEL CAMBIO				
SUPERVISOR DEL CAMBIO (Aceptación del Cambio en infraestructura debe llenar informe posterior al cambio en infraestructura)		Fecha	Firma	

OBSERVACIONES: _____

Fig. 5.1 Formato típico de control de cambio

La información debe ser asegurada. Especialmente la información confidencial que viaja por medios no seguros como Internet. Adicionalmente a la confidencialidad debe evitarse en la medida de lo posible la fuga de información en sus distintas formas.

5.8.1 Envío de información a terceros – Correo electrónico

Las instituciones financieras deben intercambiar información confidencial con sus distintos proveedores y clientes. Dicha información al viajar por Internet que es un medio non seguro podría ser interceptada y visualizada por una persona malintencionada, con dicha información puede sacar provecho y repercutir en las operaciones de la institución y hasta en su imagen reputacional la cual es muy valiosa.

Para tales casos existen diversas herramientas que permiten asegurar la información que se intercambio por correo electrónico, una de las más usadas es la herramienta llamada PGP (de PGP Corporation). Una de las formas de trabajo de la herramienta que sirve para el intercambio seguro de correos electrónicos es mediante el intercambio de llaves públicas entre las partes, es decir, si una persona X desea mandar un correo seguro a una persona Y, la persona X debe contar con la llave pública de la persona Y y viceversa. La llave pública no es confidencial, la confidencialidad se basa en la posesión de la llave privada que sirve para descifrar la información cifrada con la llave pública. Por tanto mediante un intercambio de llaves públicas es posible enviarse recíprocamente información segura así sea que viaje por Internet (ver **Figura 5.2**).

En la siguiente figura se ve el intento de abrir un archivo cifrado con una llave pública que le pertenece al usuario que trata de abrir el archivo adjunto, siempre es necesario ingresar una clave personal para poder descifrar el archivo.

5.8.2 Prevención de fuga de información

La fuga de información es otro aspecto importante de cuidado de la data que se maneja en una institución financiera.

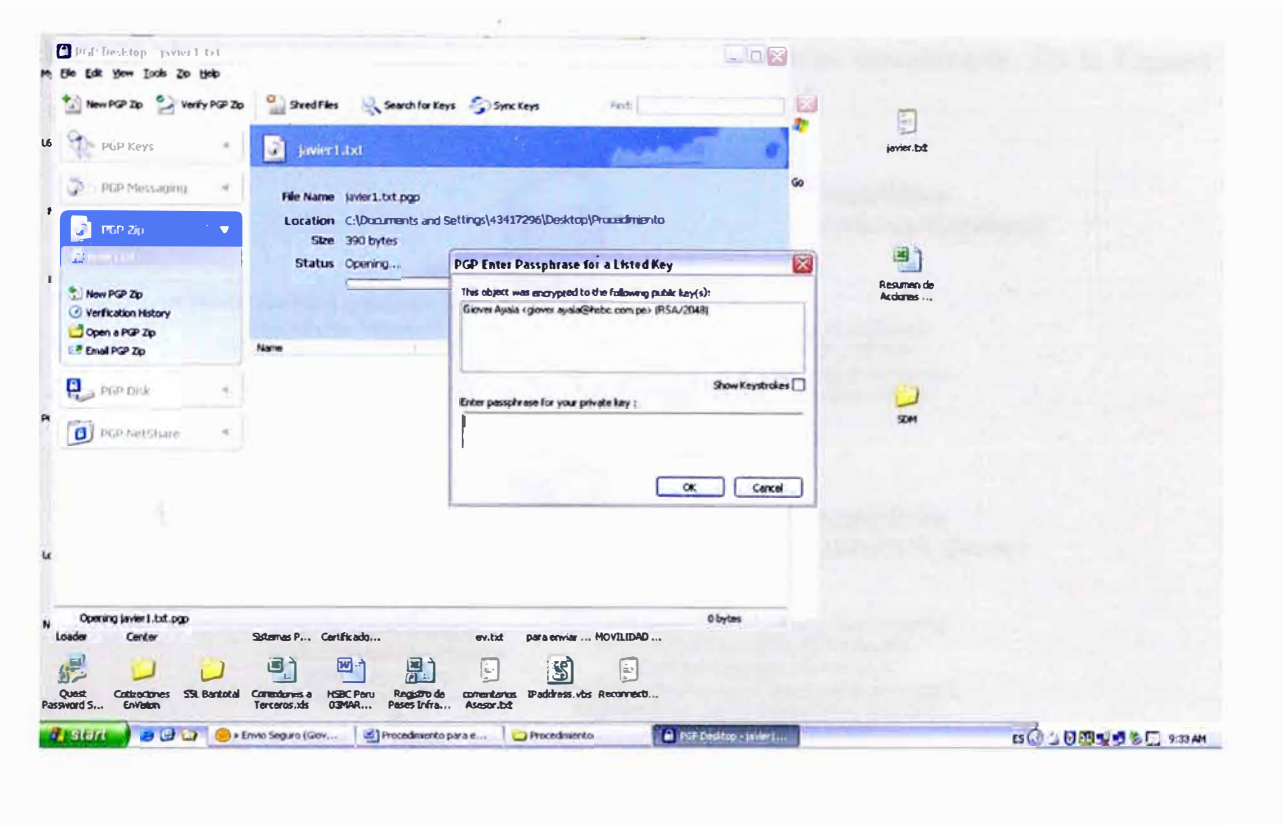

Fig. 5.2 PGP requerimiento de clave

Uno de los medios mas usado en la actualidad para el transporte de información es el uso de memorias USB, las cuales pueden ser de capacidades de hasta Giga Bytes. Controlar el uso de los mismos así como el de CDs y DVDs es de vital importancia en una institución financiera, sobre todo en áreas que manejan información altamente confidencial (**Figura 5.3**). Lo anterior mencionado es conocido como Data Leakage.

Fig. 5.3 Data Leakage

Una de las mejores y prácticas herramientas para el control de acceso a estos dispositivos es el producto Sanctuary de Lumension. Sanctuary filtra el uso de cualquier dispositivo de conectividad externa como USBs, Flopys, CD/DVD, modems, PDAs, entre otros. El provisto principal de Sanctuary en una entidad financiera es controlar que usuarios tienen permisos de usar dispositivos externos, que dispositivos tienen permiso y que nivel sobre los mismos (lectura o escritura). Sólo usuarios autorizados con un procedimiento de dispensa aprobado por el director de su área podrían tener permiso de escritura, estos casos

deben ser plenamente justificados y revalidados a lo mucho anualmente. En la **Figura 5.4** se ilustra como funciona Sanctuary:

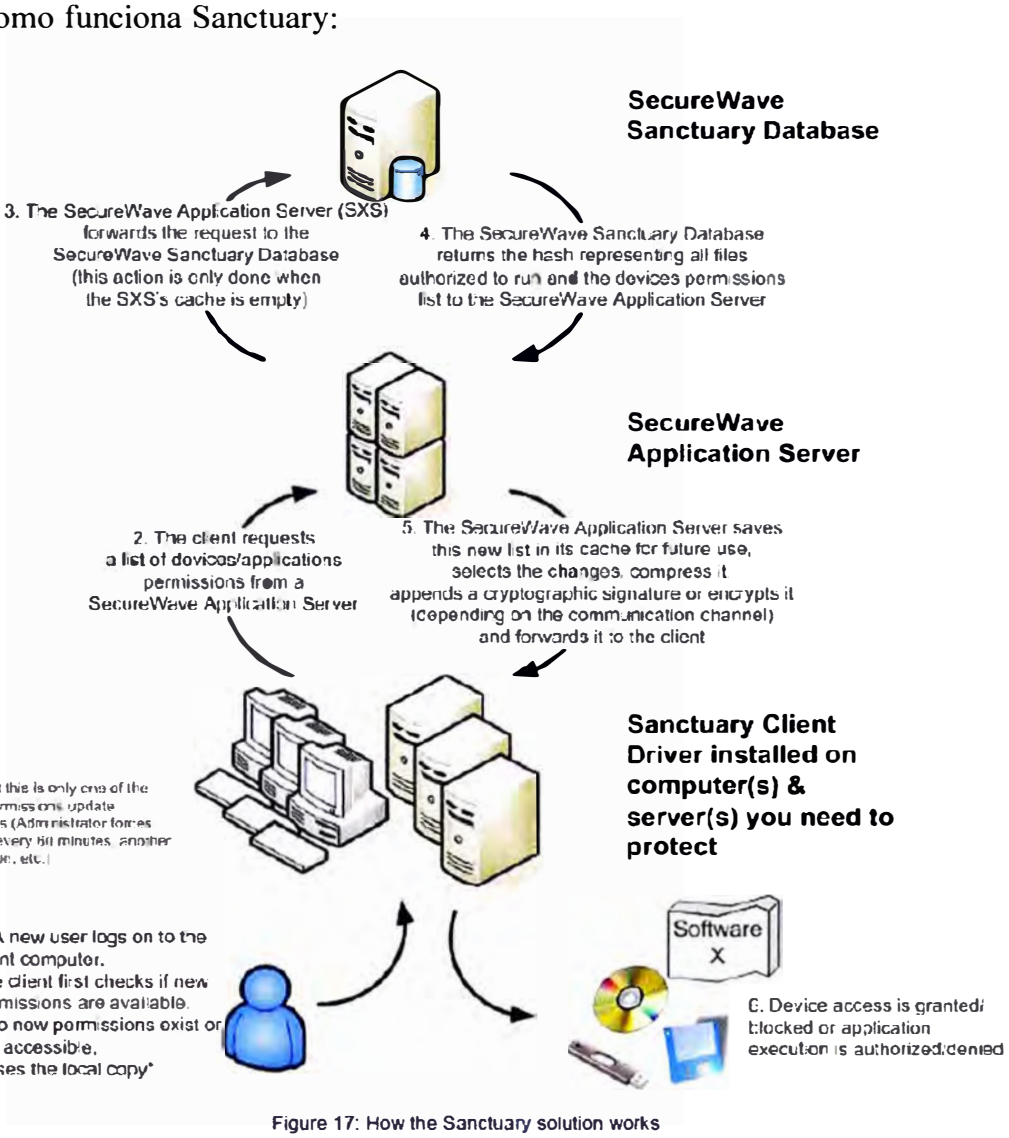

Figure 17: How the Sanctuary solution works

Fig. 5.4 Esquema Sanctuary

La administración de los permisos a los dispositivos puede centralizarse en un entorno Microsoft desde el Active Directory. Es decir, permitir o denegar un permiso a un usuario puede ser tan sencillo como agregar o sacar a un usuario de un grupo de Windows, desde donde también se administran las cuentas de usuario de la institución.

5.9 Supervisión del proveedor de servicios

Las instituciones financieras deben extender sus responsabilidades con la seguridad de la información para sus operaciones con terceros de la siguiente manera:

- Una elección apropiada del proveedor del servicio.
- Aseguramientos contractuales acerca de las responsabilidades en temas de seguridad de la información, controles y reportes.
- Acuerdos de confidencialidad de la información acerca de los sistemas y la data.
- Revisiones independientes de la seguridad del proveedor de servicios a través de pruebas y auditorias apropiados.
- Coordinación para políticas de respuesta a incidentes y requerimientos de notificación contractuales.

La conectividad de red entre las distintas sedes y agencias que la institución financiera pueda tener, se basa en los carrier de comunicaciones o Service Providers. La data que la institución financiera usa por sus redes internas también es transmitida por sus redes, de ésta forma, es hasta cierto punto un riesgo que dicha información viaje por éstos proveedores de comunicaciones.

Es mandatario contar con cláusulas de confidencialidad en los contratos establecidos con las mismas en donde el proveedor se comprometa legalmente a no manipular (mas que en transporte) la información de la institución financiera que viaja por sus redes de datos.

Sin embargo ésta cláusula de confidencialidad no es suficiente, se debe elegir a la empresa proveedora de servicio que apruebe una adecuada evaluación por parte del área de seguridad de la información de la institución financiera. Este análisis debe incluir consultas y pruebas concretas de sus operaciones y forma de trabajo y así poder garantizar que la empresa cumple con las políticas y mejores prácticas que la institución considere importantes.

En el Perú, 2 de las principales empresas que brindan servicios de transporte de data son Telmex y Telefónica. **Figuras 5.5** y **5.6**.

Fig. 5.5 Logo Telmex

Fig. 5.6 Logo Telefónica

Respecto a la disponibilidad, es recomendable contar con un proveedor de servicios para soportar los enlaces principales de datos que usualmente son enlaces WAN MPLS (que soportan calidad de servicio) y otro proveedor distinto en caso de falla del servicio del proveedor (ya sea falla física o lógica).

Usualmente los enlaces de contingencia son líneas ISDN que soportan transmisión de Data "on demand" tal que, si no se usa la línea o no se transfiere información no se cobra, es decir se cobra por tiempo de uso de la misma cuando se establece la conexión. Esto es usualmente usado por las empresas o instituciones financieras para abaratar costos, dado que un enlace redundante raramente es usado.

Adicionalmente, para alta disponibilidad en sedes o agencias es recomendable usar 02 Routers frontera, tal que si el principal falla por algún motivo, el de backup entra a funcionar automáticamente (manejando protocolos de alta disponibilidad como HSRP). En la **Figura 5.7** se ve un ejemplo típico de éste enlace redundante:

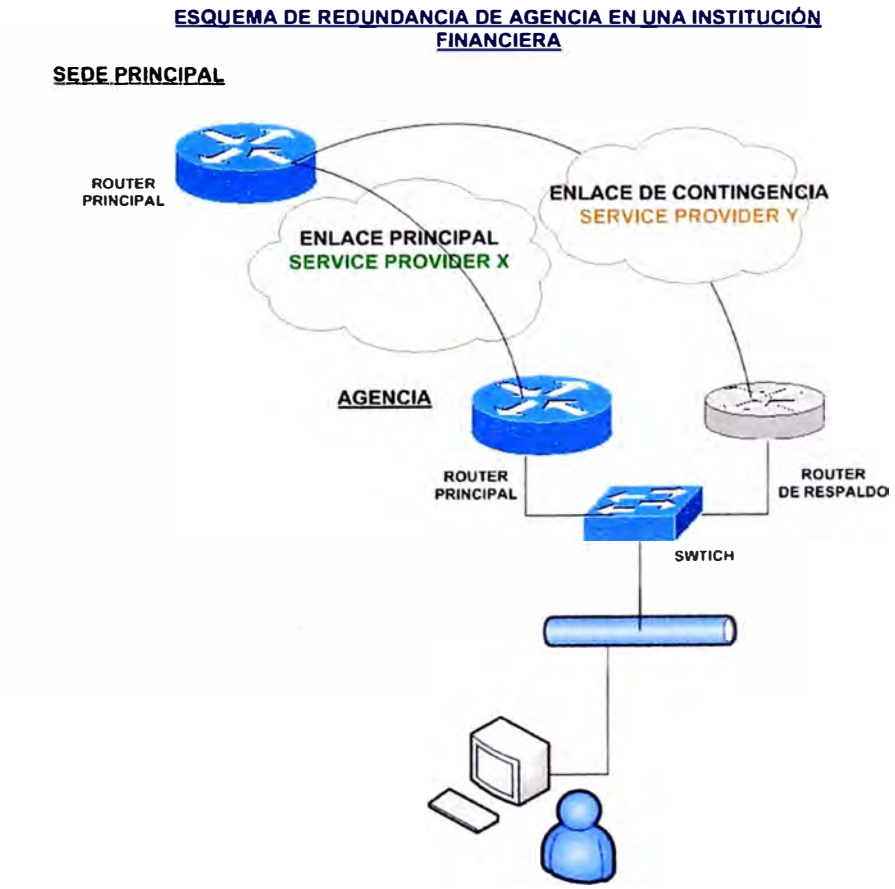

Fig. 5.7 Esquema de alta disponibilidad de Agencia Financiera

CAPITULO VI
MONITOREO DE LA SEGURIDAD

Las instituciones financieras deben asegurarse del correcto funcionamiento de sus estrategias de mitigación de riesgos e implementación de la siguiente manera:

- Monitoreando la actividad de la red y los host para identificar violaciones a las políticas y comportamientos anómalos.
- Monitoreando la condición de la red y los host para identificar configuraciones no autorizadas y otras condiciones que incrementan el riesgo de intrusión y otros eventos de seguridad.
- Analizando los resultados del monitoreo adecuadamente para que se pueda identificar, clasificar, escalar, reportar de una manera rápida y posteriormente guiar la respuesta a los eventos de seguridad.
- Respondiendo a intrusiones, debilidades y otros eventos de seguridad apropiadamente para poder mitigar el riesgo de éstos eventos a la institución y sus clientes además de restaurar la estabilidad del sistema.

El monitoreo de la seguridad de una institución financiera debe guardar relación con el riesgo, ser capaz de identificar fallas en los controles antes que un incidente de seguridad ocurra, detectar una intrusión u otros incidentes de seguridad en tiempo suficiente para dar una respuesta y soportar actividades forenses posteriores al evento.

Una institución financiera cuenta con Servidores, Equipos de Comunicaciones, PCs, Laptops y otros sistemas informáticos críticos para la operatividad. Estos logs que cada equipo genera al percibir un evento o alarma brindan información detallada de que esta aconteciendo en el mismo equipamiento, la data que almacena, la data que pasa por el mismo, lo que pasa en el sistema operativo del mismo, etc. Estos "Logs" categorizados por su criticidad pueden significar en alertas o simples eventos.

Estos sistemas en la actualidad actúan sobre una red de datos (principalmente IP) lo que permite una centralización de los eventos y alarmas que los mismos pueden generar para su análisis posterior o en tiempo real. Una de las herramientas centralizadoras líderes en el mercado actual es el appliance EnVision de RSA, división de seguridad de EMC, la cual damos una breve reseña:

6.1 Ejemplo de plataforma de recolección de eventos

6.1.1 ¿Qué hace la plataforma RSA EnVision?

La plataforma RSA enVision recopila todos los logs de eventos generados por dispositivos IP dentro de su red, hace archiving de copias de los datos de manera permanente, procesa los logs en tiempo real y genera alertas cuando observa patrones de comportamiento sospechosos. La consola intuitiva permite que los administradores consulten el volumen completo de datos almacenados, y el software analítico avanzado convierte el complejo conjunto de datos raw no estructurado en información estructurada, lo que proporciona datos útiles a los administradores con el fin de brindarles ayuda en tres áreas principales:

- Simplificación del Cumplimiento de Normas
- Seguridad Mejorada y Mitigación de Riesgos
- Optimización de TI y Operaciones de Red

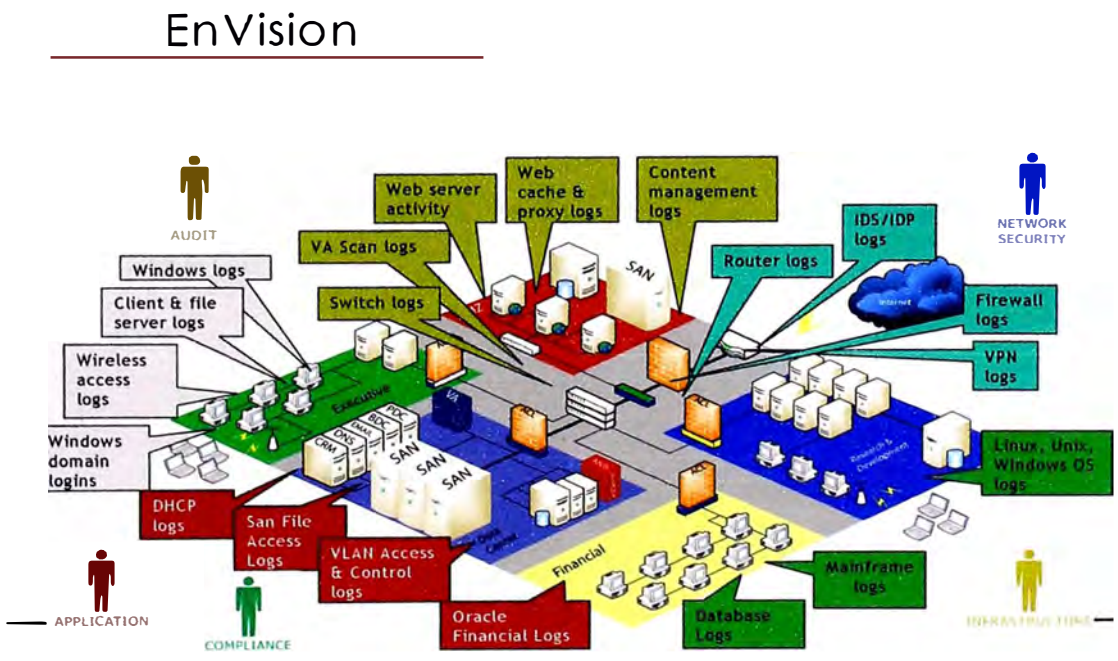

Fig. 6.1 Visión de alcance de EnVision

6.1.2 ¿Cómo funciona?

La plataforma RSA enVision permite obtener logs de decenas de miles de dispositivos al mismo tiempo: incluyendo servidores Windows®, firewalls Check Point® y routers Cisco® sin necesidad de agentes de software de cliente. Esto garantiza que All the Data™ se recopile continuamente, todo el tiempo. Ver **Figura 6.1**.

La funcionalidad de reporting, tendencias y bases de RSA enVision proporciona a TI y los administradores de red una visión general gráfica a largo plazo de los eventos de seguridad y performance, lo que mejora la efectividad de planificación y reduce la carga de trabajo.

La plataforma se puede implementar como una solución plug and play independiente o como parte de una arquitectura distribuida escalable de alta disponibilidad para enfrentar las demandas de las redes empresariales más grandes. Cuando se implementa como una solución independiente (con la gama ES) permite que una aplicación autónoma de seguridad consolidada haga todo, incluso recopilación de datos, administración, análisis y almacenamiento de información.

Cuando se implementa en una arquitectura distribuida (con la gama LS), permite implementar múltiples aplicaciones dedicadas cuando se requieren realizar funciones clave. Los recopiladores locales y remotos reúnen datos. Los servidores de datos administran los datos. Los servidores de aplicaciones realizan análisis y reporting. Los datos mismos se pueden almacenar mediante almacenamiento de información de conexión directa, en línea, near-line u offline de la cartera completa de almacenamiento de información de EMC. Ver **Figuras 6.2, 6.3** y **6.4**.

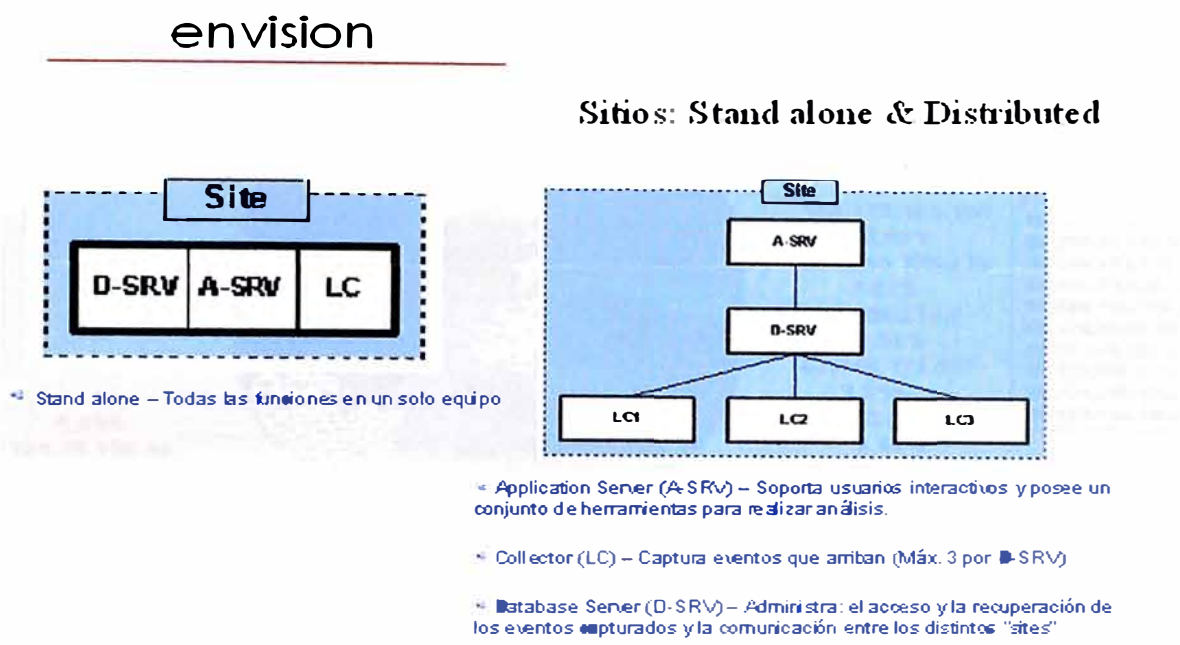

Fig. 6.2 Arquitecturas de Funcionamiento EnVision

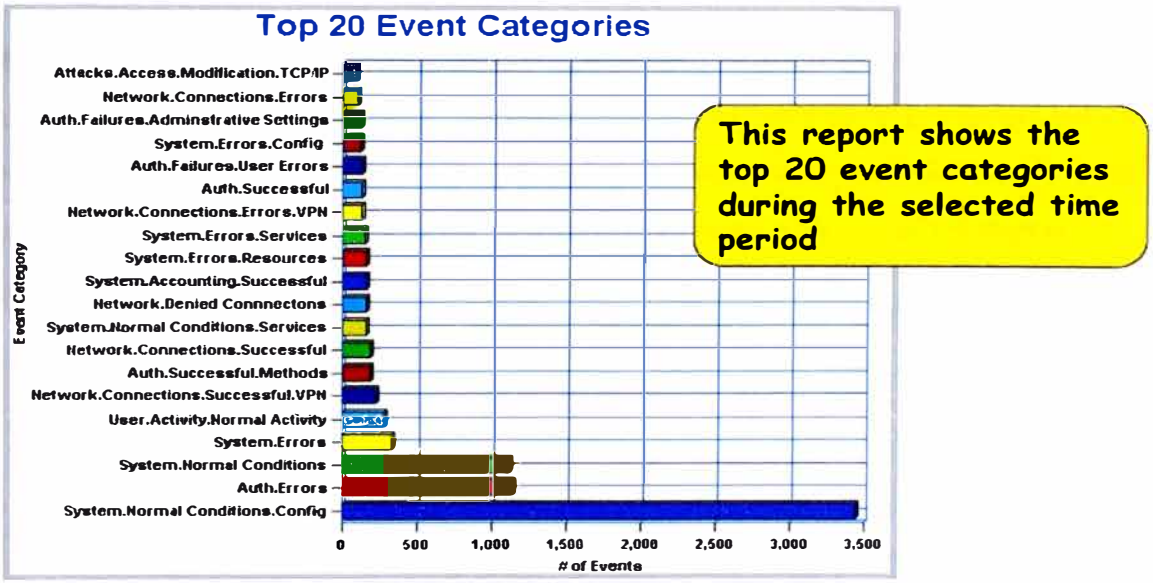

Fig. 6.3 Diagrama ejemplo de eventos

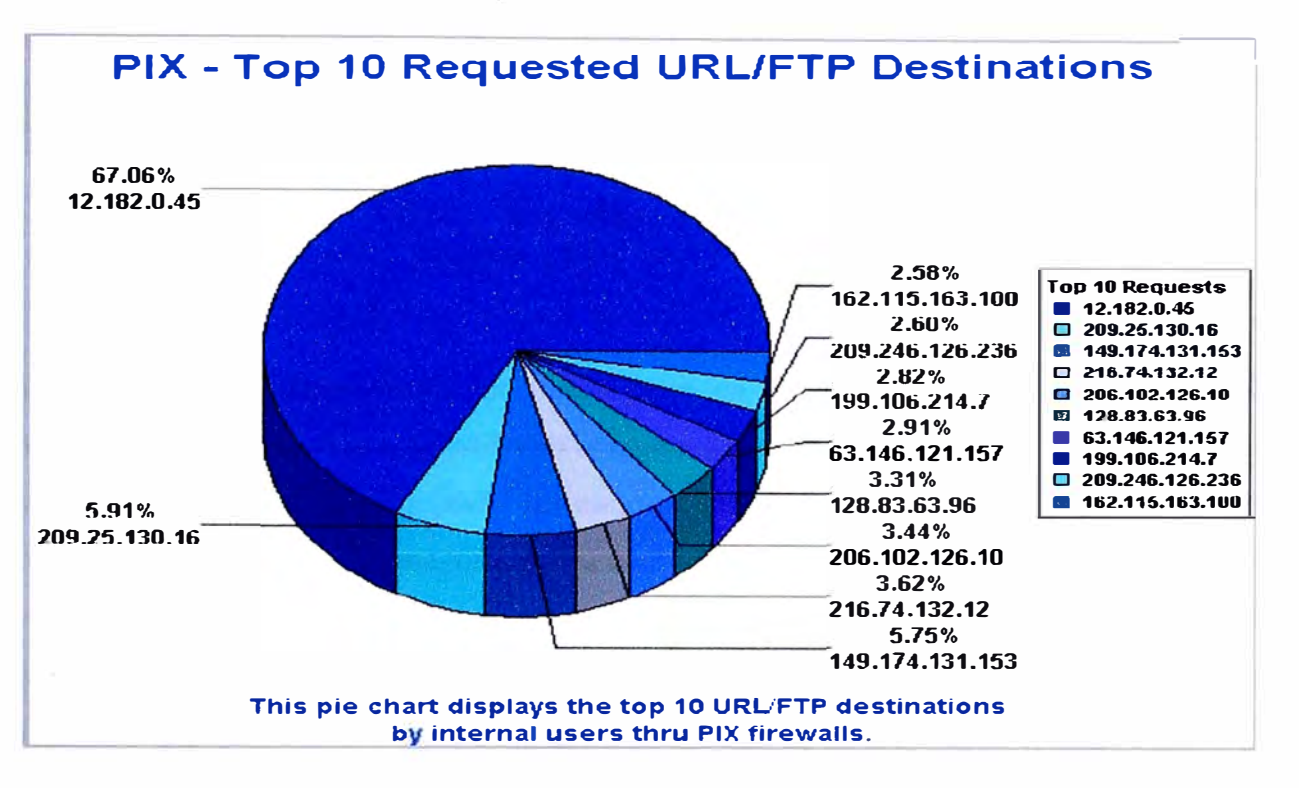

Fig. 6.4 Ejemplo de muestra estadísticas de un Proxy de Internet

6.2 Monitoreo y actualización

Las instituciones financieras deben continuamente obtener y analizar la información acerca de nuevas amenazas y vulnerabilidades, ataques en otras instituciones y la efectividad de los controles de seguridad existentes. Ellos deberían entonces usar ésa información para actualizar los análisis de riesgo, estrategias y controles implementados. Ver referencia 6 de la Bibliografía.

CAPITULO VII
PRUEBAS DE SEGURIDAD

Desde que el comercio electrónico operaciones en línea de empresa a empresa y la conectividad global se han convertido en componentes vitales de una estrategia de negocio exitosa, las empresas han adoptado las mejores prácticas y procesos de seguridad para proteger su información. La mayoría de las compañías trabaja sin cansancio para mantener una política de seguridad eficiente, implementar los últimos productos y servicios para prevenir el fraude, vandalismo, sabotaje y ataques de negación de servicio. Sin embargo muchas empresas no consideran un ingrediente clave de una política de seguridad. No hacen pruebas de la red y los sistemas de seguridad para comprobar que estén funcionando como se esperaba.

Las pruebas de seguridad que aseguran la disponibilidad de los sistemas incluyen las pruebas de continuidad de negocio que cada institución financiera debe ejecutar regularmente. Se discutirán brevemente éstas pruebas al final del capítulo.

La prueba de penetración de red (Network penetration testing) – usa herramientas y procesos para escanear el entorno de red por vulnerabilidades, ayuda a la empresa a refinar sus políticas de seguridad y asegura que la implementación de seguridad realmente provee la protección que la empresa requiere y espera. Realizar tests periódicamente ayuda a una entidad financiera, por ejemplo, descubrir las debilidades en seguridad de una red que puede llegar a comprometer a la información o los equipos debido a ataques de virus, troyanos, ataques de negación de servicio entre otras intrusiones. Las pruebas también exponen las vulnerabilidades que pueden ser introducidas por parches y actualizaciones o por errores de configuración en servidores, Routers y Firewalls.

Es también conocido el término Ethical Hacking para realizar éste tipo de pruebas. En general el termino Ethical Hacking y Penetration Testing (pruebas de penetración) se usan indistintamente y significa lo mismo.

7.1 Prueba de penetración

El objetivo global de un Test de penetración es descubrir áreas de la red de la empresa donde un intruso puede explotar vulnerabilidades en la seguridad. Diferentes pruebas de penetración son necesarias para diferentes tipos de dispositivos de red. Por ejemplo, un test de seguridad de un Firewall es diferente a un test de una PC de usuario típica. Inclusive un test de penetración de los dispositivos en la DMZ (zona desmilitarizada) es diferente de realizar un escaneo para ver si la penetración a la red es posible. El tipo de prueba de penetración debe ser evaluado en función del valor de la información del dispositivo siendo testeada y la necesidad de conectividad con un servicio dado.

El proceso de una prueba de penetración tiene 3 componentes principales:

- Definir el alcance.
- Realizar la prueba de penetración.
- Emitir el reporte y los resultados entregables.

7.1.1 Paso 1: Definir el alcance

Antes que un test de penetración pueda ser ejecutado, la entidad financiera debe definir el alcance de la prueba. Este paso incluye determinar la extensión de la prueba, que se va a testear, desde donde se va a testear y por quien.

7.1.1.a Escala completa vs. prueba orientada

Una entidad financiera debe decidir si conduce una prueba completa de la totalidad de la red o a dispositivos específicos de la misma, como un firewall. Usualmente es mejor realizar ambas para poder determinar el nivel de exposición a la infraestructura pública, así como también los objetivos de seguridad individuales. Por ejemplo, las políticas de un Firewall son usualmente escritas para permitir a ciertos servicios pasar a través de él. La seguridad para ésos servicios es puesta en el dispositivo realizando dicho servicio y no en el Firewall, por tanto, es necesario realizar un test de seguridad de esos dispositivos así como en el Firewall. Algunos de los dispositivos específicos que deben ser considerados

para las prueba de penetración son los Firewall, Routers, Servidores Web, Servidores de Correo, Servidores FTP y Servidores DNS, entre otros servidores que alojan servicios críticos para el banco.

7.1.1.b Dispositivos y sistemas

Definiendo el alcance del proyecto, la empresa debe también decidir del rango de la prueba. Por ejemplo, ¿esta buscando solo vulnerabilidades que pueda combatir el compromiso de un dispositivo, o está además buscando susceptibilidades de ataques de negación de servicio?

7.1.1.c Pruebas locales vs remotas

Seguidamente, la empresa debe decidir si la prueba será realizada desde una ubicación remota a través de la Internet o dentro de la empresa en la red local o intranet. La decisión es tomada en gran medida por los objetivos que sean seleccionados a ser testeados y las implementaciones en seguridad actuales de la empresa. Por ejemplo, una prueba remota de un dispositivo detrás de un Firewall que esconde la red interna por NAT (Networ Address Translation) fallará si el Firewall previene apropiadamente el acceso al dispositivo, sin embargo, testear el mismo Firewall para ver si éste protegerá las PCs de usuarios de un escaneo remoto será exitoso.

7.1.1.d Pruebas por Staff o por terceros

Después de que en alcance de la prueba sea determinado, el equipo de Seguridad de la Información y de Tecnología debe decidir si el test será realizado por personal de la entidad financiera o por alguna tercera empresa. Si bien es recomendable que una empresa especializada realice dicha tarea crítica y especializada, es necesario considerar capacitar al personal de la entidad financiera respecto a éstas pruebas y el uso de las herramientas y la metodología correctamente, así, la empresa ahorrará costos y su personal estará correctamente capacitada para realizar ésta tarea que se debe realizar regularmente.

Para los sistemas con Internet Banking y Servidores Web, es decir servidores de cara a Internet, las empresas especializadas cuentan con los últimos equipos y experiencia para poder realizar las pruebas, así en éstos casos de equipamiento de cara a Internet, es decir, mucho mas riesgosos, es recomendable la contratación de éstos servicios, siempre bajo la atenta supervisión del personal designado de la entidad financiera para resguardar la confidencialidad de la información del banco.

Algunas de las empresas con mas experiencia para realizar éstos tipos de pruebas son: Netcraft, KPMG, PriceWaterHouseCoopers, entre otras. **Figura 7.1**.

Fig. 7.1 Empresas auditoras de red

7.1.2 Paso 2: Realizando la prueba de penetración

La metodología apropiada es esencial para el éxito del test de penetración. Esto incluye obtener información para luego testear el entorno del objetivo.

El proceso de la prueba empieza obteniendo tanta información como sea posible acerca de la arquitectura de la red, topología, hardware y software para poder encontrar todas las vulnerabilidades en seguridad posibles. La investigación de la información pública tales como periódicos, revistas, información en la web, patentes entre otros, no sólo provee a los ingenieros de seguridad con información base, sino que les da una idea de que un Hacker

puede obtener y tener para encontrar vulnerabilidades. Las herramientas tales como ping, traceroute y nslookup pueden ser usadas para obtener información del entorno del objetivo y ayuda a determinar la topología de la red, proveedor de servicio de Internet y la arquitectura. Las herramientas tales como escaneadotes de puerto, NMAP, SNMPC y NAT ayudan a determinar el hardware, sistema operativo, nivel de parches y los servicios corriendo en cada dispositivo objetivo.

Una vez que la información acerca de todos los objetivos han sido colectadas, los ingenieros de seguridad la usan para configurar las herramientas comerciales de escaneo como ISS, Internet Scanner, NAI's Cybercop Scanner y otras herramientas de uso libre como Nessus y Satan especializadas para buscar vulnerabilidades.

El uso de éstas herramientas comerciales y libres agiliza tremendamente el proceso de escaneo. Después que el escaneo de vulnerabilidad se ha completado, la salida es examinada por falsos positivos y falsos negativos. Cualquier sospechosa vulnerabilidad de ser falsa es re-examinada o testeada usando otras herramientas o Scripts customizados.

Para testear por nuevas vulnerabilidades que no han sido actualizadas dentro de las herramientas comerciales o libres, los ingenieros de seguridad realizan pruebas adicionales y corren exploits recientemente realizados. Esto es necesario por que nuevos exploits son liberados cada día, y esto puede ser muchas semanas o meses antes que éstas vulnerabilidades son incluidas en la base de datos de vulnerabilidades de las herramientas automatizadas de escaneo.

Una vez que el escaneo ha sido realizado, los ingenieros de seguridad puedes testear objetivos adicionales definidos en el alcance del test de penetración, incluyendo por ejemplo, vulnerabilidades de passwords y ataques de negación de servicio (DoS).

Para realizar pruebas de DoS en un entorno de producción, sin poner en riesgo el funcionamiento del dispositivo o sistema, la entidad financiera puede crear una imagen en producción y luego poner ésta imagen en un hardware similar para las pruebas.

7.1.3 Paso 3: Emitir el reporte y los resultados entregables

Después de completar el test de penetración, los ingenieros de seguridad analizan toda la información derivadas de las pruebas. Después ellos listan y priorizan las vulnerabilidades, categorizan los riesgos como altos, medios y bajos además de recomendar posibles soluciones a las vulnerabilidades encontradas. Ellos pueden también proveer recursos como links de Internet para encontrar información adicional u obtener parches para reparar las vulnerabilidades.

El reporte final puede incluir las siguientes partes:

- Un resumen ejecutivo que sumariza lo encontrado en el test de penetración y desglosa información relacionada a las debilidades y las fortalezas de los sistemas de seguridad existentes. Los puntos más importantes de lo encontrado en las pruebas también son incluidos.
- Un reporte técnico detallado de lo encontrado en las vulnerabilidades de los equipos analizados, categorizando y priorizando los riesgos además de hacer recomendaciones acerca de las reparaciones, incluyendo información técnica adicional de cómo reparar o corregir cualquier vulnerabilidad.
- Información adicional, acerca de las salidas de los escaneadotes, pantallazas, diagramas así como RFCs relevantes y papers incluidos en un apéndice.

7.2 Pruebas de plan de continuidad de negocio

La información es uno de los activos más importantes para las organizaciones, donde los sistemas de información y disponibilidad de estos juegan un rol preponderante para la continuidad de un negocio, por lo cual las organizaciones desarrollan e implementan lo que se conoce como BCP (Business Continuity Plan), con el objetivo de mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia.

Esto implica que un BCP debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

Una etapa importante de éste plan involucra las pruebas necesarias para que ése proceso sea depurado y asegure su funcionalidad en un evento real. Las etapas de las pruebas se pueden resumir en la **Figura 7.2**.

Fig. 7.2 Resumen de etapas de pruebas de BCP

CAPITULO VIII
CONCLUSIONES Y RECOMENDACIONES

1. Durante el presente informe hemos discutido los principales conceptos de la Seguridad de la Información en una institución financiera. Abarcar todos los conceptos y detallarlos sería una tarea compleja que no es el objetivo del presente informe, sin embargo hemos comentado lo que se ha considerado lo primordial y más crítico, resaltando en los puntos que he experimentado durante el transcurso de mi experiencia profesional.

2. La Seguridad de la Información se basa principalmente sobre 3 conceptos: Confidencialidad, Integridad y Disponibilidad. La confidencialidad trata sobre el aseguramiento de la información a ser visualizada. La integridad trata sobre el objetivo de evitar que la información sea modificada o alterada. Finalmente la Disponibilidad trata sobre el hecho que la información y data siempre debe estar disponible para su uso.

3. Durante el presente informe hemos discutido los procedimientos y herramientas que se deben tener en cuenta para asegurar la información, sin embargo, es importante también resaltar el "factor humano" que es vital para el objetivo de asegurar la información. Los empleados de la entidad financiera deben ser guiados correctamente para que puedan manejar y cuidar la información con prioridad alta y que sea una práctica común en su día a día. Deben tener claros los conceptos de seguridad, como por ejemplo saber que es "Ingeniería Social" en donde personas mal intencionadas pueden obtener información mediante técnicas sociales o engaños.

4. Una medida de atenuación del riesgo del factor humano en una institución financiera es contar con un programa de capacitación de personal en temas de seguridad de la información. Esto puede brindarse en los cursos de inducción cada vez que una persona ingresa a trabajar a la institución, con boletines informáticos, seminarios, publicaciones

en la intranet de la empresa, avisos educativos cada vez que un usuario hace un "log in" a su PC (o en el protector de pantalla), entre otras maneras.

5. Mencionamos durante el informe, diversas herramientas de uso actual y de calidad comprobada, tales como el Sanctuary (para evitar la fuga de información), el EnVision (para monitoreo de eventos y alertas de todos los sistemas del banco) o el PGP (usada para el cifrado de correos electrónicos para el envío seguro a terceros). Se recomienda el uso de dichas herramientas o similares para implementaciones de seguridad en cualquier empresa.

5. Comentamos sobre el procedimiento de análisis de riesgos y la forma de obtener el valor cuantitativo del mismo mediante una matriz de riesgos. El análisis de riesgo es vital para evaluar la criticidad de cualquier solución tecnológica y tener en claro el proceso para así poder implementar controles que los mitiguen. Se recomienda el uso de ésta herramienta de análisis para cualquier proceso, especialmente para ver que tan crítico puede ser. Cada nuevo proyecto de tecnología de información en una entidad financiera debe pasar por un análisis de riesgo.

6. Concluimos que la seguridad de la información es una tarea que nunca termina y que involucra a todos los miembros de la institución financiera. Se deben establecer controles, herramientas y procedimientos para su correcta implementación y seguimiento. La tecnología crece día a día por tanto las herramientas y sistemas tienen que estar actualizados al mismo nivel para prevenir cualquier nueva vulnerabilidad o tipo de ataque tecnológico interno o externo. Teniendo en cuenta la premisa de accesos a sistemas: "En seguridad menos es mas".

ANEXO A
TERMINOLOGÍA

TERMINOLOGÍA

Amenaza	Una acción o evento que puede ser perjudicial a la seguridad. Una amenaza es una violación potencial a la seguridad.
Vulnerabilidad	Existencia de una debilidad, diseño o error de implementación que puede lidiar con un inesperado e indeseable evento comprometiendo la seguridad del sistema.
Exploit	Un camino definido para quebrar la seguridad de un sistema tecnológico a través de una vulnerabilidad.
Objetivo de Evaluación	Un sistema tecnológico, producto o componente que es identificado para tener una evaluación de seguridad.
Ataque	Un asalto en un sistema de seguridad que deriva de una amenaza inteligente. Un ataque es cualquier acción que viola la seguridad.
Seguridad	Un estado de bienestar de información e infraestructura en que la posibilidad de un robo, intento y falta de disponibilidad de la información y servicios es mantenido bajo o tolerable. La seguridad se basa en confidencialidad, integridad y disponibilidad.
Confidencialidad	La ocultación de información o recursos.
Integridad	La seguridad de la información o recursos en términos de prevenir cambios inapropiados y no autorizados.
Disponibilidad	La habilidad de usar la información o recursos deseados.
Ataque a fuerza bruta	Un intento para adivinar un password probando con cualquier posible combinación de letras o números.
Negación de Servicio	Un ataque extremadamente serio que sobrecarga completamente servidores y evita el acceso legítimo de usuarios.
NMAP	Una herramienta de escaneo que ubica dispositivos en la red.
Parche	Un programa que es escrito para reparar una vulnerabilidad en una aplicación o sistema.
Ping	Una utilidad que testea conectividad de red.

Escaneador de Puerto Un programa que testea todos los puertos (65535) para ver cuales están abiertos para ser accedidos.

Falso positivo de virus Es un error por el cual un software antivirus reporta que un archivo o área de sistema está infectada, cuando en realidad el objeto está limpio de virus.

Falso negativo de virus Es un error mediante el cual el software falla en detectar un archivo o área del sistema que está realmente infectada.

ANEXO B
EVALUACIÓN DEL NIVEL DE RIESGO

EVALUACIÓN DEL NIVEL DE RIESGO

Una institución financiera puede categorizar sus riesgos para un mejor y ordenado análisis. Las categorías pueden tener a la vez varios niveles. Como en los cuadros categorizados en 3 niveles:

TABLA B.1 Categorías de Riesgos

Nivel 1	Nivel 2	Nivel 3	Codigo
Personas	Fraude de empleados / malicia (como acto delictivo)	Colusión	PER01
		Malversación, desfalco	PER02
		Sabotaje a la reputación del banco	PER03
		Lavado de dinero	PER04
		Robo físico	PER05
		Robo de propiedad intelectual	PER06
		Fraude de programación	PER07
		Ingresar virus al sistema del banco	PER08
	Actividad no autorizada / Estafas / Delitos de empleados	Uso indebido de información privilegiada (p e. transacciones bursátiles iniciadas)	PER09
		Utilizar información sobre un cliente para beneficio propio comprando antes de que se le ejecute una orden de compra de gran volumen, o vendiendo antes de que ejecute la venta	PER10
		Compra y venta de acciones con el fin de atrer corretaje y dar la impresión de actividad	PER11
		Actividad no autorizada con clientes o terceros	PER12
		Actividad con productos no autorizados	PER13
		Incumplimiento de límites de autonomía o establecidos para transacciones	PER14
		Modelos incorrectos (intencionalmente)	PER15
		Actividad fuera de las reglas de intercambio	PER16
		Actividad para fijación de precios incorrecta	PER17
		Manipulación del mercado	PER18
		Procedimientos omitidos o cortados voluntariamente	PER19
		Tácticas de venta ilegales o agresivas no permitidas	PER20
	Leyes laborales	Culminación de la relación laboral errónea	PER21
		Discriminación / oportunidades desiguales	PER22
		No adaptación a otras leyes laborales	PER23
		No adaptación a regulaciones de seguridad y salud	PER24
	Interrupción laboral	Acción industrial: sindicatos, huelgas, rebeliones, motines.	PER25
	Pérdida o falta de personal clave	Falta de empleados adecuados	PER26
		Pérdida de personal clave	PER27
Procesos	Riesgo de pago / liquidaciones / entrega	Interrupción en el proceso de pagos / liquidaciones	PRO01
		Inadecuado proceso de pagos / liquidaciones	PRO02
		Inadecuada o baja adaptación a los procedimientos / instrucciones	PRO03
		Pérdidas debidas a fallas en la conciliación	PRO04
		Errores en la aplicación de procesos de seguridad	PRO05
		Capacidad insuficiente de personas o sistemas para cubrir los vólumenes o carga de trabajo	PRO06
	Riesgo contractual o documentario	Documento no completado apropiadamente	PRO07
		Cláusulas o términos de contrato inadecuados	PRO08
		Términos contractuales inapropiados	PRO09
		Registros de venta inapropiados	PRO10
		Fallas en la valorización de la empresa (due dilligence)	PRO11
	Valuación / Determinacion de Precios	Riesgo de modelo	PRO12
		Error en los datos recibidos	PRO13
	Cumplimiento e informes internos / externos - Riesgo Contable y Riesgo de Cumplimiento	Reportes de excepción inadecuados	PRO14
		Fallas en el registro contable, contabilidad, o datos inadecuados	PRO15
		Reporte regulatorio	PRO16
		Reporte financiero	PRO17
		Reporte de impuestos (tributos)	PRO18
		Reporte de mercado de valores	PRO19
		Fallas en el cumplimiento	PRO20
		Incumplimiento de murallas chinas (relacionado a conflictos de interés)	PRO21
		Protección de datos / ley privada	PRO22
	Riesgos de Proyectos / Gestión del cambio	Planes o proyectos inadecuados	PRO23
		Riesgo de nuevo producto	PRO24
		Incumplimiento en las fechas límite del proyecto	PRO25
	Riesgos de Ventas / Mala gestion de los activos de clientes	Inapropiada selección de productos o decisiones de inversión	PRO26
		Complejidad de productos	PRO27
		Conocimiento o asesoría de bajo nivel (incluyendo títulos valores)	PRO28
		Inadecuado registro de las preferencias de inversión de los clientes	PRO29

Sistemas	**Riesgo de Inversión en Tecnología**	Arquitectura inapropiada	SIS01
		Riesgo estratégico (plataformas tecnológicas / proveedores)	SIS02
		Incompatibilidad con sistemas existentes	SIS03
		Inapropiada definición de requerimientos de negocio	SIS04
		Desarrollo / desiciones de compra incorrectas	SIS05
		Obsolescencia de hardware	SIS06
		Obsolescencia de software	SIS07
	Desarrollo e implementación de sistemas	Inadecuada gerencia de proyectos	SIS08
		Costo / tiempo mayor al planificado	SIS09
		Errores de programación interno / externo	SIS10
		Fallas en la integración / migración con o desde sistemas existentes	SIS11
		Falla de sistemas para consolidar requerimientos de negocio	SIS12
		Inadecuados procedimientos de operaciones (sin seguimiento)	SIS13
	Fallas en los sistemas	Fallas en la red	SIS14
		Fallas en el hardware	SIS15
		Fallas en el software	SIS16
	Violación de la seguridad de sistemas	Violación de la seguridad externa	SIS17
		Violación de la seguridad interna	SIS18
		Virus	SIS19
	Capacidad de sistemas	Falta de una adecuada planificación de la capacidad de sistemas	SIS20
		Software inadecuado	SIS21

Eventos externos	**Obligaciones públicas / legales**	Incumplimiento de ley de patente	EXT01
		Incumplimiento de la gestión del medio ambiente	EXT02
		Incumplimiento fiduciario / pago de impuestos	EXT03
		Interpretación de leyes	EXT04
		Litigios	EXT05
	Actividades delictivas	Fraude externo / fraude de cheques / falsificación	EXT06
		Vandalismo	EXT07
		Cuentas fraudulentas abiertas por clientes	EXT08
		Chantaje	EXT09
		Robo	EXT10
		Lavado de dinero	EXT11
		Terrorismo	EXT12
		Guerra civil / huelgas	EXT13
		Incendio provocado	EXT14
		Ataques a los sistemas de e-banking incluyendo el fraude de phishing, fraude subsecuente, y software malévolo recibido a través de Spams, como virus, spyware	EXT15
	Riesgo de tercerización / proveedores	Quiebra de proveedores	EXT16
		Incumplimiento de responsabilidad (mal uso de datos confidenciales)	EXT17
		Riesgo del proceso de contraparte por contratos con terceros	EXT18
		Incumplimiento de acuerdos de niveles de servicio	EXT19
		Fallas en la recepción del servicio	EXT20
		Fallas tecnológicas en sistemas de proveedores	EXT21
		Inadecuada administración de proveedores / proveedores de servicios	EXT22
		Fraude de programación	EXT23
	Riesgo de internalización	Incumplir con acuerdos de niveles de servicio al prestar servicios de tercerización a otras empresas	EXT24
	Desastres naturales o fallas humanas que dañan la infraestructura	Incendio	EXT25
		Inundación	EXT26
		Terremotos, Fenómenos metereológicos	EXT27
		Desastre civil	EXT28
		Fallas de transporte	EXT29
		Fallas en la energía	EXT30
		Fallas en las telecomunicaciones externas	EXT31
		Interrupción del aprovisionamiento de agua	EXT32
		Indisponibilidad del local (edificio)	EXT33
	Riesgo regulatorio	Riesgo regulatorio	EXT34
	Riesgo de gobierno / político	Guerra	EXT35
		Expropiación de activos	EXT36
		Negocios bloqueados	EXT37
		Cambio en régimen tributario	EXT38
		Otros cambios en las leyes	EXT39

B.1 Criterios de Evaluación Cualitativa

El concepto básico para realizar el análisis cualitativo del riesgo es el de encontrar los valores de los parámetros necesarios, para tal son necesarios 3 items:

1. Impacto
2. Probabilidad
3. Exposición

B.1.1 Impacto

El nivel de impacto de riesgo absoluto es el daño potencial o consecuencia, lo cual puede generar pérdida financiera, afectar el valor de los accionistas y/o afectar la eficiencia.

TABLA B.2 Impacto

NIVEL		FACTORES QUE INFLUYEN EN EL VALOR DE LOS ACCIONISTAS						
		Servicio al Cliente	Actitud de los Medios	Acción Regulatoria	Acción Legal	Personal del Banco	Crimen	Pérdida Directa
INSIGNIFICANTE	1	Sin impacto para el Cliente, no se entera del problema	Reputación muy alta, se ve al Banco como un proveedor de calidad	Reconoce altos estándares de cumplimiento	Amenaza de acción legal	Sin efecto	Altos estándares del Banco son reconocidos públicamente	Hasta los US$ 7,500.00
MENOR	2	Algunos Clientes se enteran pero el impacto es insignificante (poco tiempo perdido en el servicio)	Noticia "rutinaria" en la Prensa o difundida por Internet sobre el funcionamiento del Banco	Comentarios verbales del Regulador	Acción legal limitada en contra de las decisiones del Banco	Daño menor o imposición de trabajar fuera del horario normal	Fracaso en intentar acceder a los sistemas operativos; pérdida de información de menor importancia	Hasta los US$ 37,500.00
MODERADO	3	Número significativo de Clientes conocen el problema y encuentran algunos inconvenientes	Críticas en prensa o TV. Críticas públicas del Regulador o de la Industria. Críticas en foros de Internet o en titulares de Internet	Hallazgos y observaciones en los informes de evaluación regulatoria (visita de la SBS)	Inicio de proceso judicial o litigio	Daño requiere tratamiento médico para más de un empleado. Reducción de personal local	Intrusión física o lógica dentro de los sistemas operativos del Banco	Hasta los US$ 150,000.00
MAYOR	4	Pérdida prolongada del servicio durante las últimas 24 horas	Múltiples medios relatan la noticia y/o la TV local la prioriza por más de un dia	Sanciones por violaciones múltiples o repetitivas	Litigio llevado contra el Banco por violación legal con baja oportunidad de negociación	Daños significativos, muerte potencial. Reducción significativa de personal	Investigación policial iniciada; datos operativos o sistemas de control pueden estar comprometidos	Hasta el US$ 1,500,000.00
MASIVO	5	Muchos Clientes sufren problemas en su trabajo que les causa inconvenientes mayores	Fiscalizadora o comparable a una repercusión política. Pérdida pública de confidencialidad	Acciones contra el Banco realizadas por violación significativa, genera ceses / renuncias, multas / penalidades grandes	Litigio en contra del Banco por violación legal significativa	Muertes y/o daño mayor en la vida del personal. Amplia reducción del personal a todo nivel	Fraude realizado exitosamente para obtener fallas significativas en los sistemas	Superior al US$ 1,500,000.00

B.1.2 Probabilidad

La probabilidad de ocurrencia de un evento de riesgo indica la frecuencia con que puede ocurrir. Las gerencias de línea evalúan la probabilidad utilizando el criterio profesional basado en su conocimiento y experiencia del negocio / proceso.

TABLA B.3 Probabilidad

NIVEL		Probabilidad	Estado de la Regulación	Ejemplo de frecuencia de evento de pérdida
RARO	1	Insignificante - podría ocurrir solo en circunstancias excepcionales	Sin cambios en la regulación	Cada 30 años o menos
IMPROBABLE	2	Podría ocurrir alguna vez	Cambios insignificantes en la regulación	Una vez cada 10 años
POSIBLE	3	Debería ocurrir alguna vez	Cambios moderados en la regulación	Una vez cada 3 años
PROBABLE	4	Probablemente ocurre alguna vez	Cambios significativos en la regulación	Anualmente
ESPERADO	5	Ocurrirá en varias circunstancias	Cambios complejos importantes en la regulación	Al menos una vez al mes

B.1.3 Exposición

El nivel de exposición mide el grado en que se tiene mitigado el riesgo, considerando efectividad y relevancia de los controles y acciones de mitigación.

TABLA B.4 Exposición

NIVEL		FACTORES QUE INFLUYEN EN LA EXPOSICIÓN AL RIESGO						
		Procedimientos / Pruebas	Efectividad del control	Cambios en el negocio	Diseño de control	Clientes / Terceros	Contingencias	Mitigación externa
MINIMA	1	Procedimientos que incluyen acciones de control han sido actualizados y probados durante el último año	Probado cuidadosamente para todos los problemas principales	Constante por algunos años con cambios mínimos para actualizar los procesos existentes	Roles y responsabilidades detalladas cubren la segregación de funciones. Controles automatizados y preventivos	El perfil con quien se hace negocio no genera riesgo a la transacción	Planes aseguran que el trabajo puede continuar con una pequeña interrupción	Riesgo totalmente transferido a un tercero con una mínima exposición (residual)
BAJA	2	Procedimientos cubren todas las áreas clave, algunas detalladamente, actualizados en los últimos 12 meses	Soporta la gestión pero utilizado por diferente personal (no por todos los que deberían aplicarlo)	Pocos cambios en los deberes operativos en los siguientes seis meses	Roles y responsabilidades claros para las funciones. Controles automatizados y preventivos mayormente	El perfil con quien se hace negocio es improbable que genere riesgo a la transacción	Planes permiten una recuperación total en 24 horas	Riesgo transfendo en gran parte a terceros
MEDIA	3	Cubre la mayoría de las áreas claves. Algunos probados pero con brechas	Inclusión incompleta en su aplicación (no se aplica como debería)	Nuevos proyectos afectan que la operatividad sea implementada	Trabajos definidos en términos genéricos. Algunos problemas no tienen seguimiento. Controles automatizados y manuales, preventivos y detectivos	El perfil con quien se hace negocio es posible que genere riesgo	Planes permitirán una recuperación en pocos días	Riesgo transfendo parcialmente a terceros
SIGNIFICATIVA	4	Solo los elementos principales son probados. Algunas áreas clave no son cubiertas en los procedimientos	Nivel de soporte a la gestión no es clara	Cambios fundamentales en los métodos de trabajo, productos / servicios o reestructuración del negocio	Acciones correctivas en términos amplios no son implementadas	El perfil con quien se hace negocio solo está definidio parcialmente y es probable que genere riesgo	Poca atención o pruebas a los planes	Mínimo nesgo transfendo a terceros
MAYOR	5	Pocos o inexistencia de procedimientos	Se aplican controles "de palabra", verbalmente. Se tiene escrito pero no es usado ni actualizado	Cambio rápido en curso y/o incertidumbre	No se tiene niveles de control y responsabilidad definidos	El perfil con quien se hace negocio no está bien comprendido y es altamente probable que genere riesgo	No se tienen planes y no hay eficacia en la contingencia	Ningún nesgo transferido a terceros

Basados en los valores obtenidos definimos el riesgo absoluto:

Nivel de Riesgo Absoluto = Impacto * Probabilidad **(B.1)**

De donde finalmente obtenemos el nivel de vulnerabilidad del riesgo de la matriz de riesgos:

TABLA B.5 Matriz de Riesgos

NIVEL DE RIESGO ABSOLUTO	NIVEL DE EXPOSICIÓN				
	1	2	3	4	5
> 10	C	B	B	A	A
8 - 10	C	C	B	B	A
5 - 7	C	C	C	B	B
3 - 4	D	C	C	C	B
1 - 2	D	D	C	C	C

B.1.4 Definiendo la criticidad

A: Riesgo Alto

B: Riesgo Medio

C: Riesgo Medio-Bajo

D: Riesgo Bajo

De un análisis de riesgo, los resultados con resultado de nivel "**A**" deben ser resueltos en el menor tiempo posible ejecutando planes de acción con fechas definidas, se debe hacer un seguimiento constante del mismo.

ANEXO C
DISPONIBILIDAD EN UN DATACENTER

CLASIFICACIÓN DE LA INFRAESTRUCTURA DE DATACENTER – TIA 942

Un Data Center no sólo es construcción, hardware, software y telecomunicaciones. La infraestructura física de un Data Center la componen una serie subsistemas como el de climatización, el eléctrico, el sistema de protección contra incendios y otros. Adicionalmente se deben tomar en cuenta otros aspectos como los recursos humanos y los procesos asociados que deben generar la capacidad de mantenerse en funcionamiento aunque existan accidentes o desastres naturales.

El standard **TIA-942 (Telecomunication Infrastructure Standard for Data Centers)** incluye un Anexo informativo sobre los Grados de Disponibilidad (**Tier**) con los que pueden clasificarse los Datacenters. Estos Tiers están basados en información desarrollado por el **Uptime Institute**, un consorcio dedicado a proveer a sus miembros las mejores prácticas y benchmarks para mejorar la planificación y gerenciamiento de Datacenters. Para cada uno de los cuatro Tiers el anexo describe detalladamente las recomendaciones para la infraestructura edilicia, de seguridad, eléctrica, mecánica y telecomunicaciones. A mayor número de Tier mayor grado de disponibilidad. Ver **Tabla C.1**.

TABLA C.1 Comparativa según nivel de disponibilidad

	Tier I	Tier II	Tier III	Tier IV
Building Type	Tenant	Tenant	Stand-alone	Stand-alone
Staffing	None	1 Shift	1 + Shifts	"24 by Forever"
Useable for Critical Load	100% N	100% N	90% N	90% N
Initial Gross Watts per Square Foot (W/ft^2) (typical)	20-30	40-50	40-60	50-80
Ultimate Gross W/ft^2 (typical)	20-30	40-50	100-150[1,2,3]	150+[1,2]
Uninterruptible Cooling	None	None	Maybe	Yes
Support Space to Raised-Floor Ratio	20%	30%	80-90%[2]	100+%
Raised-Floor Height (typical)	12"	18"	30-36"[2]	30-36"[2]
Floor Loading lbs/ft^2 (typical)	85	100	150	150
Utility Voltage (typical)	208, 480	208, 480	12-15 kV[2]	12-15 kV[2]
Single Points-of Failure	Many + human error	Many + human error	Some + human error	None + human error
Annual Site-Caused IT Downtime (actuals)	28.8 hours	22.0 hours	1.6 hours	0.4 hours
Site Availability	99.671%	99.749%	99.982%	99.995%
Months to Implement	3	3-6	15-20	15-20
Year First Deployed	1965	1970	1985	1995
Construction Cost (±30%)[1,2,3]				
Raised Floor	$220/ft^2	$220/ft^2	$220/ft^2	$220/ft^2
Useable UPS Output	$10,000/kW	$11,000/kW	$20,000/kW	$22,000/kW

Tier I: Datacenter Básico

Un Datacenter Tier I puede admitir interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía, pero puede no tener piso técnico, UPS o generador eléctrico. Si los posee pueden tener varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del Datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Errores de operación o fallas en los componentes de su infraestructura causarán la interrupción del Data Center. La tasa de disponibilidad máxima del Datacenter es **99.671%** del tiempo.

Tier II: Componentes Redundantes

Un Datacenter con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos Datacenters cuentan con piso falso, UPS y generadores eléctricos, pero está conectado a una sola línea de distribución eléctrica. Su diseño es (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura, pueden causar una interrupción del servicio. La tasa de disponibilidad máxima del Datacenter es **99.741%** del tiempo.

Tier III: Mantenimiento Concurrente

Las capacidades de un Datacenter de este nivel le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planeadas incluyen mantenimiento preventivo, reparaciones o reemplazo de componentes, agregar o eliminar componentes, realizar pruebas de sistemas o subsistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua, significa doble conjunto de tuberías. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea y mientras que la otra atienda la totalidad de la carga. En este nivel,

actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura pueden todavía causar una interrupción del Datacenter.
La carga máxima en los sistemas en situaciones críticas es de 90%.
Muchos Datacenters Tier III son diseñados para actualizarse a Tier IV, cuando los requerimientos del negocio justifiquen el costo.
La tasa de disponibilidad máxima del Datacenter es **99.982%** del tiempo.

Tier IV: Tolerante a Fallas

Un Datacenter de este nivel provee capacidad para realizar cualquier actividad planeada sin interrupciones en el servicio, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aún ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración System+System. Eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones críticas es de 90%. Persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos.

La tasa de disponibilidad máxima del Datacenter es **99.995%** del tiempo.

BIBLIOGRAFIA

1. Federal Financial Institutions Examination Council, "Information Security", Julio 2006.

2. HSBC Bank, “Group IT Security Standars”, UK 2006-2008.

3. Álvaro Gómez, “Enciclopedia de la Seguridad Informática”, Madrid 2006.

4. Tony Northrup & Orin Thomas, “Security in a Microsoft Windows Server 2003 Network”, USA 2004.

5. Victor Barahona, “Intrusion Detection System”, Madrid 2008.

6. Rsa Security Inc, “Resumen de la plataforma RSA EnVision”, www.rsa.com 2008.

7. Information Security Forum, “Security Audit of Networks”, United Kingdom 2001.

8. Baquia, Publicación Web, http://www.baquia.com/ 2009.