TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PLATAFORMA DE BANCA VIRTUAL EN UNA ENTIDAD FINANCIERA

Presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de Especialista en
Comunicaciones y Redes de Comunicación de Datos
Por el Ing. Samanta Andreina De Pablo Arias

Caracas, Septiembre del 2007

TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PLATAFORMA DE BANCA VIRTUAL EN UNA ENTIDAD FINANCIERA

TUTOR ACADÉMICO: Prof. Vincenzo Mendillo

Presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de Especialista en
Comunicaciones y Redes de Comunicación de Datos
Por el Ing. Samanta Andreina De Pablo Arias

Caracas, Septiembre del 2007

DEDICATORIA

A Dios y a mi Madre por estar presentes en todo momento

A mi hermano Santiago por estar siempre apoyándome incondicionalmente

A mi amiga Helen quien me enseñó que siempre vale la pena luchar por nuestros sueños, cueste lo que cueste alcanzarlos

AGRADECIMIENTOS

A Dios por acompañarme en todo momento y darme la fuerza para perseverar en mis objetivos

A mi madre que siempre me ha impulsado a seguir adelante y me ha guiado por el camino correcto

A mi hermano por servirme de motivación

A mi Novio Tomás por impulsarme a terminar este trabajo y contar siempre con su cariño, apoyo y preocupación

Al Profesor Vicenzo Mendillo quien me brindó su apoyo y conocimiento

A la Universidad Central de Venezuela por brindarme la oportunidad de incrementar mi desarrollo profesional

A todos los que de una u otra forma colaboraron en mi formación, y que me han ayudado aunque sea con una simple oración…

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA
POSTGRADO DE ESPECIALIZACIÓN EN COMUNICACIONES
Y REDES DE COMUNICACIÓN DE DATOS

EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PLATAFORMA DE BANCA VIRTUAL EN UNA ENTIDAD FINANCIERA

AUTOR: Ing. Samanta De Pablo
TUTOR: Prof. Vicenzo Mendillo
AÑO: 2007

RESUMEN

Para las organizaciones, la tecnología de información es esencial en el procesamiento electrónico de la información, mejorando altamente el desempeño en el mercado competitivo. No obstante, el uso de la tecnología introduce riesgos adicionales a la gestión del negocio, los cuales se relacionan al manejo, integridad, confidencialidad y disponibilidad de la información, como principal activo para la toma de decisiones.

La Entidad Financiera ABC conciente de los riesgos que en tecnología de información se expone, permitió el desarrollo del presente trabajo que permitiría la identificación de riesgos en una de las plataformas más críticas de la Organización, como lo es la Banca Virtual. Como resultado, se propusieron soluciones a las diferentes oportunidades de mejoras identificadas, en función de reducir los riesgos implícitos en la utilización de tecnologías y sistemas de información, así como alcanzar un nivel de seguridad aceptable que les permita hacer frente a las nuevas amenazas informáticas.

INTRODUCCIÓN

Uno de los cambios de mayor importancia hoy en día en las organizaciones ha sido la automatización de sus procesos mediante la tecnología de información, y la influencia que ésta tiene sobre las empresas, convirtiendo su uso en un factor estratégico más que en una necesidad. En este sentido, uno de los primeros retos de las organizaciones, es el enfrentar la seguridad de la información bajo una perspectiva de tecnología por ser un factor fundamental que habilita los procesos de negocio.

Para muchas organizaciones, la información y la tecnología de información que la apoya, representan los activos más valiosos del negocio, por lo cual, un elemento crítico para el éxito de las mismas, no es tan sólo aplicar una administración efectiva de la información y de la tecnología relacionada, sino también velar porque los controles asociados a minimizar los riesgos en estas áreas, estén debidamente aplicados.

Es por esta razón que la seguridad de información posee un papel significativo, sobre todo cuando las amenazas a que se exponen las redes de comunicaciones y datos pueden afectar las operaciones de los negocios, dada su dependencia en la tecnología de información, ocasionando situaciones tales como:

- Imposibilidad para prestar parcial o totalmente sus servicios.
- Pérdidas económicas debido a que no se puedan efectuar sus operaciones financieras (servicio al cliente, operaciones de tesorería, entre otras).
- Pérdidas económicas directas, producto de ataques o fraudes contra las operaciones financieras.
- Perjuicios legales ante la incapacidad de cumplir con obligaciones contractuales.

En este sentido, la compañía en estudio, consciente de la necesidad de ahondar en los aspectos relacionados a la creación de actitudes proactivas, planteó sus necesidades de evaluar la seguridad en sus ambientes tecnológicos más críticos, en función de iniciar la planificación estratégica de seguridad integral.

El objetivo de la evaluación estará orientado a la prestación de servicios especializados, con el fin de identificar situaciones de riesgo y establecer acciones para su minimización, como estrategia para la obtención de un modelo de seguridad de activos de información adaptado a las necesidades de la compañía.

Los resultados alcanzados en este trabajo, se han estructurado en cinco capítulos. El capítulo I indica el planteamiento del problema, el cual plantea de forma clara y precisa los lineamientos y objetivos (generales y específicos) del trabajo realizado, así como un breve estudio de la factibilidad de la investigación; el capítulo II resume los conceptos y aspectos relevantes que teóricamente requieren conocerse para el desarrollo y entendimiento del trabajo realizado; el capítulo III se describe el marco metodológico, el tipo de investigación y metodología empleada para desarrollar el proyecto; el capítulo IV muestra los resultados de la evaluación incorporando el esquema de recomendaciones, finalmente en el capitulo V se muestra el procedimiento de análisis realizado para la implantación de recomendaciones.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1. Confidencialidad de la información

Debido a la importancia de la información manejada en este proyecto, existen políticas de confidencialidad de información que impiden revelar el nombre de la compañía en estudio. Por esta razón, en el desarrollo de la tesis de grado, se utilizará como nombre “Entidad Financiera ABC”.

2. Planteamiento del problema

Durante los últimos años ha crecido significativamente el uso de la tecnología de información, hasta el punto que ha llegado a ser un pilar fundamental en el manejo de los negocios transformando la forma de llevar a cabo los procesos productivos.

Esta tecnología ha sido aprovechada por las organizaciones para el apoyo de sus actividades administrativas y para ofrecer a sus clientes servicios eficientes. Sin embargo, su utilización conduce a ciertas exposiciones de riesgo, hasta tal punto que incluso encierra dependencia de las actividades del negocio hacia la referida tecnología.

En términos de seguridad de información, los riesgos más importantes a los que está sujeta la información son: revelación, manipulación y accesos no autorizados. En tal sentido, el impacto de estos riesgos para una organización puede afectar la confianza, oportunidad y confiabilidad de la información manejada, así como la calidad de los servicios prestados

La Entidad Financiera ABC no escapa ante esta realidad, ya que hace uso de la tecnología de información para optimizar las operaciones y procesos del negocio. En consecuencia, existen riesgos y brechas de seguridad que pueden existir en los sistemas e infraestructura tecnológica, y que eventualmente puedan ser

utilizadas por personas no autorizadas, pudiendo afectar las operaciones de la Institución.

Por tal motivo, la Entidad Financiera ABC solicitó la evaluación de seguridad de información para la plataforma de Banca Virtual, ya que este es uno de sus servicios más críticos, en función de conocer sus actuales brechas de seguridad que pudieran ser utilizados por personas no autorizadas para tener acceso a la información crítica o confidencial, o bien tratar de interrumpir sus operaciones.

3. Justificación del servicio

Los ataques informáticos ocurren diariamente: simplemente se conecta una computadora a Internet y alguien tratará de penetrar la misma una, dos, tres o decenas de veces al día buscando víctimas vulnerables y con mucha más razón si estas computadoras son utilizadas con fines comerciales, militares o educacionales. En la Figura 1 se puede observar el porcentaje de incidentes en páginas web reportados en el año 2006.

Fuente: Computer Security Institute
CSI/FBI 2006 Computer Crime and Security Survey

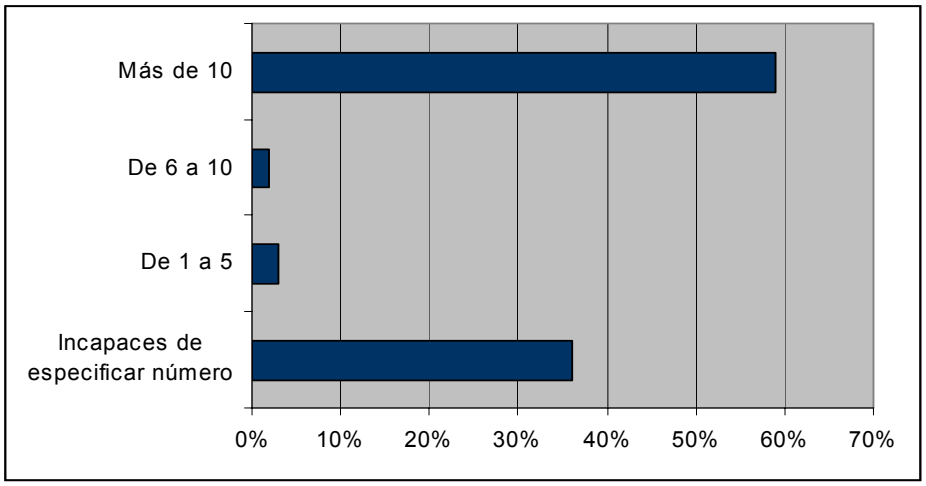


Figura 1. Porcentaje de incidentes reportados en páginas web por organizaciones en U.S.A.

Al estar inmersos en un mundo globalizado en donde Internet es, no sólo una herramienta, sino un medio de comunicación vital, las computadoras se vuelven

más vulnerables a ataques que desean obtener y/o destruir información vital para la organización, o simplemente afectar las operaciones de la misma.

Es por esto que la mayoría de las organizaciones tienen diariamente incidentes de seguridad provocados por distintos factores como denegación de servicios, virus, usurpación de identidades (phishing), captura de contraseñas (sniffing), etc, produciendo pérdidas significativas a nivel monetario, tal y como se puede observar en la Figura 2.

Fuente: Computer Security Institute
CSI/FBI 2006 Computer Crime and Security Survey

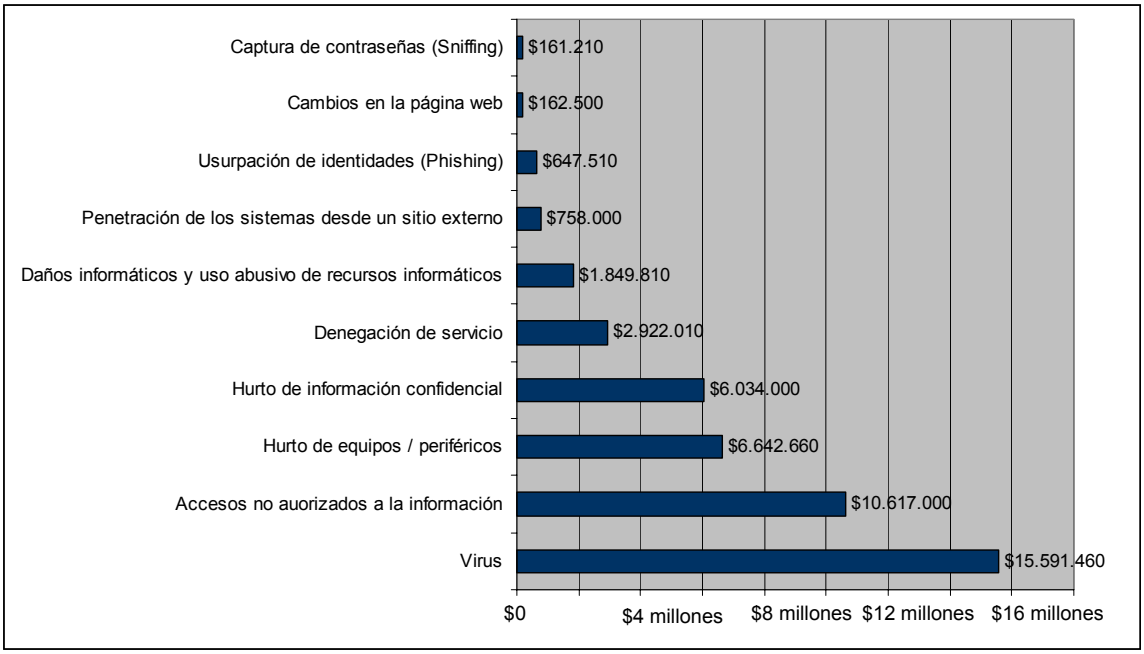


Figura 2. Pérdidas en dólares por tipo de ataques reportados por organizaciones en U.S.A.

Aun nado a esto, las organizaciones tienen que enfrentar la realidad no solamente de los ataques externos, sino de los internos, ya que no pueden subestimar las vulnerabilidades de los sistemas de información, equipos portátiles y desktops. En la Figura 3 se puede observar que en un estudio realizado a las empresas venezolanas, el origen del peor incidente de seguridad de información reportado fue interno.

Fuente: Espiñeira, Sheldon y Asociados
Prácticas de seguridad de activos de información en las empresas en Venezuela - 2004

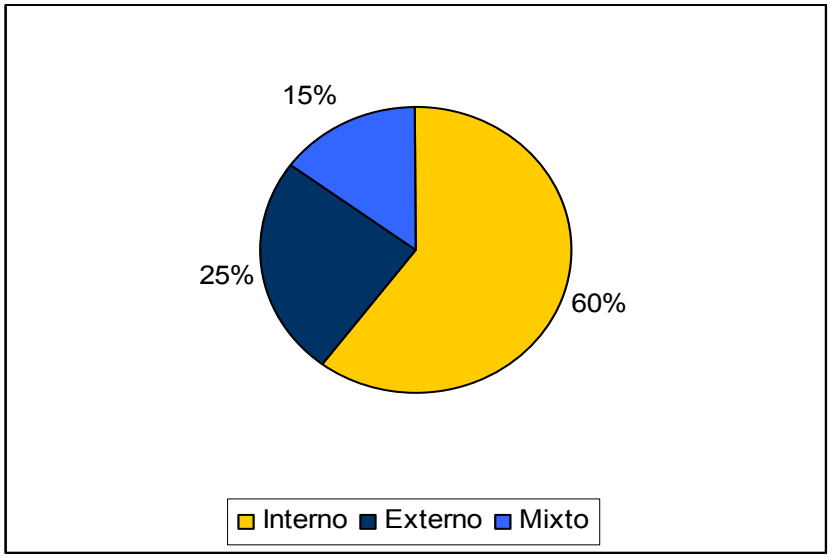


Figura 3. Origen del peor incidente de seguridad de información reportado en organizaciones venezolanas en el año 2004

En este sentido y tomando en cuenta lo explicado anteriormente, la Entidad Financiera ABC decidió evaluar los controles de seguridad implantados en su plataforma tecnológica de Banca Virtual, con el fin de conocer si sus activos de información están protegidos contra posibles accesos no autorizados por personas internas o externas a la Institución.

Es importante resaltar que por medio de este servicio la Entidad Financiera ABC puede proteger sus recursos de red y de información, lo que mitigaría el riego de ataques informáticos que pudiesen ocasionar fallas en los sistemas, así como pérdidas monetarias por interrupción de las operaciones.

4. Objetivos

4.1. Objetivo General

Evaluar y probar los controles establecidos en la plataforma tecnológica que respalda la Banca Virtual, así como proponer soluciones para la reducción de riesgos del negocio implícitos en la utilización de tecnologías de información de la Entidad Financiera ABC.

4.2. Objetivos Específicos

- Realizar un levantamiento de información exhaustivo en conjunto con la Gerencia de Sistemas, sobre la arquitectura de los activos de información, a fin de alcanzar la familiarización necesaria con los procesos generales y tecnología que soportan la aplicación de Banca Virtual.

- Revisión de los controles generales del área de sistemas que están relacionados con la protección de los activos de información.

- Evaluación de la seguridad de activos de información que componen la plataforma de Banca Virtual, con el objeto de prevenir accesos no autorizados, manipulación indebida de los activos de información, y la alteración de la configuración de los equipos.

- Presentar los riesgos asociados a las debilidades detectadas durante la evaluación de seguridad de activos de información en la plataforma de Banca Virtual, haciendo énfasis en los niveles de riesgos (alto, medio y bajo).

- Sugerir las alternativas que contribuyan a solventar o minimizar las vulnerabilidades detectadas.

5. Alcance del servicio

Para el cumplimiento de los objetivos propuestos en la realización de este trabajo, el alcance estuvo limitado a las siguientes actividades:

- Levantamiento de información relacionado a los procesos de Banca Virtual, así como la plataforma tecnológica que los apoya.

- Evaluación de seguridad de información de la siguiente infraestructura tecnológica:

  - Evaluación del esquema y controles de seguridad implantados a nivel del sistema operativo Linux del servidor donde residen los componentes principales del servicio de Banca Virtual.
  - Revisión del esquema y controles de seguridad implantados a nivel del sistema operativo Windows 2000 del servidor donde reside la base de datos Oracle.
  - Revisión del esquema y controles de seguridad implantados a nivel de la base de datos Oracle, donde reside la información de autenticación de los clientes jurídicos y naturales.

- Elaboración del plan de acción recomendado para mitigar los riesgos de negocio existentes.

- Discusión de resultados obtenidos con diferentes niveles gerenciales de la Entidad Financiera ABC.

6. Análisis de factibilidad

6.1. Factibilidad Técnica

La Entidad Financiera ABC posee una infraestructura tecnológica actualizada con los últimos adelantos tecnológicos en materia de redes y prestación de servicios vía Internet, en la cual apoya sus procesos de negocio más críticos. Por esta razón, técnicamente es factible evaluar los controles de seguridad que tienen implantados actualmente en función de conocer los riesgos a los que se exponen contra posibles intentos de acceso no autorizados a sus activos de información.

6.2. Factibilidad Económica

En el plan de adaptación, fortalecimiento y mejoramiento de la infraestructura tecnológica que desarrolla la Entidad Financiera ABC, y de acuerdo a los planes de crecimiento e incorporación de servicios de valor agregado al cliente, existe la factibilidad económica para el desarrollo del proyecto, considerando el hecho que se aportarían recomendaciones para mejorar el entorno de control del negocio.

6.3. Factibilidad Operativa

Con la realización de este proyecto, la operatividad del entorno informático no será afectada y por ende las acciones recomendadas tendrán un efecto mínimo sobre los usuarios finales, más sin embargo algunas políticas de seguridad definidas pueden impactar mientras se difunde la cultura de seguridad en la organización.

CAPÍTULO II

MARCO TEÓRICO

Las bases teóricas brindan todos aquellos conocimientos relacionados con el trabajo presentado, las cuales sirven como punto de apoyo para llevar a cabo el mismo. Estas se tomaron de acuerdo a la relación que se tiene como apoyo en las recomendaciones para evaluar, diseñar e implantar controles de seguridad que mitiguen los riesgos de accesos no autorizados e interrupción de la continuidad operativa, tanto desde Internet como en la red interna de la entidad financiera estudiada; se consideraron los conceptos de sistemas, de seguridad, de políticas y procedimientos, riesgos y vulnerabilidades en plataformas tecnológicas, etc., todo esto con la finalidad de aplicar el enfoque de la especialización a la situación dada.

1. Seguridad de Información

Entendemos por *seguridad de información* el conjunto de actividades y medidas orientadas a la protección de la información contenida en los sistemas e instalaciones informáticas frente a su posible destrucción, modificación, utilización y difusión indebidas.

1.1. Conceptos básicos relacionados a Seguridad de Información

- **Sistema de información.** Son los recursos informáticos (físicos y lógicos) y activos de información de que dispone la empresa u organización para su correcto funcionamiento y la consecución de los objetivos propuestos por su Dirección.

- **Amenaza.** Cualquier evento que pueda provocar daño en los sistemas de información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista.

- **Vulnerabilidad.** Cualquier debilidad en los sistemas de información que pueda permitir a las amenazas causarles daños y producir pérdidas. Generalmente se producen por fallos en los sistemas lógicos, aunque también corresponden a defectos de ubicación e instalación.

- **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto en la empresa. Evidentemente el riesgo es característico para cada amenaza y cada sistema, pudiéndose disminuir tomando las medidas adecuadas.

- **Incidente de seguridad.** Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un sistema de información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza, pues como no existe el riesgo cero siempre es posible que una amenaza deje de ser tal para convertirse en una realidad.

- **Impacto.** Es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles tales como la calidad del servicio y la imagen de la organización.

- **Defensa.** Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste. Muchas veces se la conoce como *medida de seguridad o prevención*. Su objetivo es reducir el riesgo o el impacto.

- **Defensa activa o medida de seguridad activa.** Cualquier medida cuyo objetivo sea anular o reducir el riesgo de una amenaza como la instalación de un programa antivirus o el cifrado de la información.

- **Defensa pasiva o medida de seguridad pasiva.** Cualquier medida cuyo objeto sea, si se produce un incidente de seguridad, reducir el impacto. El ejemplo típico es el uso de las copias de seguridad de la información.

- **Recurso de recuperación.** Recurso necesario para la recuperación de las operaciones en caso de desastre, como las cintas magnéticas de salvaguarda o los equipos de respaldo.

- **Acción de contingencia.** Acción a realizar en caso de un incidente de seguridad. Por ejemplo cambiar el servidor de la red a otro equipo.

1.2. Principios de la Seguridad de Información

- **Confidencialidad.** Permite proteger la información de acceso por personas no autorizadas. Este objetivo de la seguridad busca asegurar que únicamente personas que requieren acceso a cierta información sean las que lo posean.

- **Integridad.** Asegura que la información no ha sido alterada, es decir que los datos almacenados son exactamente los mismos a los introducidos inicialmente o modificados por última vez. La pérdida de integridad puede ser causada por errores humanos y/o actitudes intencionadas.

- **Autenticidad.** Permite proteger la información de acceso por parte de personas no autorizadas. Se busca asegurar que la persona identificada sea la persona verdadera.

- **Disponibilidad.** Asegura que la información no será negada a los usuarios autorizados, previene la desaparición o inaccesibilidad de recursos, brindando protección y recuperación en caso de siniestros. La mayoría de los ataques intencionados a sistemas informáticos persiguen imposibilitar el acceso a datos o robo de información; sus razones son diversas, y van desde simples motivaciones políticas a intereses económicos.

- **Identificación.** Refiere la correcta identificación de personas cuando solicitan el acceso.

- **Control.** Los procedimientos y políticas de control de uso, limitan las acciones que personas puedan realizar una vez que tenga acceso a datos o recursos del sistema.

- **Auditabilidad.** Poder llevar a cabo la auditoría mediante registros históricos de los eventos.

1.3. Aspectos a considerar en una evaluación de Seguridad de Información

Existen múltiples puntos de vista con los que se puede acometer el estudio de la seguridad en los entornos informáticos, así como una gran variedad de intereses, elementos afectados y tipos de medidas a adoptar. En general se adopta el punto de vista del usuario, informático o final, que es el que resulta más afectado por cualquier fallo en la seguridad del sistema. El grado de integridad en el tratamiento de los problemas de seguridad en un sistema determinado dependerá de las medidas que se adopten, pero siempre habrán de tenerse en cuenta los aspectos específicos informáticos involucrados con la seguridad.

Cada instalación y cada sistema informático es diferente, por lo que, al estudiar su seguridad, deberá previamente tenerse en cuenta una serie de aspectos básicos como:

- La existencia o no de un entorno hostil (zona de tormentas, campos magnéticos, desiertos, zona de conflictos laborales, terrorismo, etc.) que aconsejen el incremento o no de las defensas.

- La necesidad de asegurar un funcionamiento continuo (cajeros bancarios, control de tráfico aéreo, etc.), o si, por el contrario, el sistema puede funcionar de forma discontinua con interrupciones.

- El grado de sensibilidad o privacidad de los activos de información contenidos o elaborados por el sistema. En algunos casos, como los datos personales deben protegerse por imperativo legal.

Estos aspectos anteriores han de tenerse en cuenta en todos los estudios y planes de seguridad, ya que obligan a ser más o menos exhaustivos en la elección de las defensas.

1.4. Fases de una evaluación de seguridad

Para abarcar todos los aspectos de la seguridad han de tenerse en cuenta las siguientes cuatro fases consecutivas que se relacionan con:

- La *identificación* de las amenazas que puedan afectar al sistema; en especial las de mayor riesgo y mayor impacto.

- Las *defensas* o medidas de prevención a implantar para dificultar o evitar los incidentes de seguridad.

- Los medios de *detección* de indicios de situaciones no deseadas.

- Los *recursos de recuperación y acciones de contingencia* necesarias para reducir los trastornos y/o repercusiones económicas de los incidentes de seguridad.

1.5. Actitudes frente al riesgo

Frente al problema de la seguridad de información se puede adoptar una de las tres actitudes siguientes:

- **Aceptar el riesgo**, bien por su baja probabilidad de ocurrencia, bien por su bajo impacto.

- **Transferir el riesgo**, mediante la contratación del correspondiente seguro, aunque pueden existir pérdidas irreparables como la del recurso información.

- **Mitigar el riesgo**, mediante la elaboración y puesta en marcha de *un Plan Estratégico de Seguridad de Información* que contengan medidas preventivas y de recuperación.

2. Amenazas e Impacto

La diversidad de elementos de un sistema informático que pueden ser atacados origina que las amenazas puedan deberse a muy diversas causas. A principios de los años ochenta un estudio del gobierno sueco identificó 800 diferentes amenazas, aunque evidentemente con mayor o menor probabilidad de riesgo y con impactos muy variables. Además, la evolución de la tecnología informática y el creciente número de jóvenes expertos, incrementa continuamente su número. Por ello la identificación de las posibles amenazas y el intento de tipificarlas es una labor muy ardua. Adicionalmente, la labor de clasificación de las mismas, se ve complicada debido a que en la realidad, el ataque a un sistema se suele producir mediante amenazas combinadas y con un propósito definido, en la mayoría de los casos, de obtener algún beneficio de tipo económico.

2.1. Tipos básicos de amenazas

Las amenazas que se ciernen sobre los recursos informáticos, los activos de información y el personal son, básicamente, de cuatro tipos diferentes: interceptación, modificación, interrupción y generación:

- **Interceptación:**

  La Interceptación se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema. Ejemplos: acceso a una base de datos, entrada a través de la red en un sistema informático ajeno, etc.

- **Modificación**

  La Modificación intenta, además de la interceptación, cambiar en todo o en parte el funcionamiento del sistema. Es el tipo de amenaza más peligroso ya que puede ocasionar grandes daños en el sistema. Ejemplos: cambios en el contenido de una base de datos, cambios en los datos de una transferencia bancaria, etc.

- **Interrupción**

  La Interrupción puede ser temporal o permanente e incluye la posibilidad de destrucción de recursos y activos. Es la más sencilla de detectar y la que presenta mayor dificultad para luchar contra ella, ya que muchas veces son accidentes naturales. Ejemplos: interrupción de suministro eléctrico, incendios, errores de operación que afectan la operatividad del negocio.

- **Generación**

  La Generación se refiere a la adición de campos o registros en los activos, en la adición de líneas de código en los recursos lógicos, o a la introducción en el sistema de programas completos. Ejemplos: virus informáticos, caballos de Troya, transacciones electrónicas falsas, introducción de datos en una base, etc.

2.2. Impacto

Cuando se produce un incidente de seguridad, es decir, cuando se materializa una amenaza, se produce una pérdida para la organización que es necesario valorar. Interesa también clasificar la naturaleza de las posibles pérdidas derivadas de un incidente en orden a su importancia con el objeto de seleccionar las medidas preventivas a adoptar en cada caso.

- **Tipificación de las pérdidas**

  La importancia de las pérdidas depende de los casos, llegándose a producir daños irreparables en las organizaciones. Las pérdidas ocasionadas pueden ser de muy diferente naturaleza, tales como:

  - Físicas (muertos, heridos, incapacidades laborales, enfermedades profesionales, etc.)
  - Materiales (daños e inutilización de instalaciones y recursos informáticos, robos de los mismos, etc.)
  - Alteraciones de la normalidad (interrupciones y retrasos en los procesos de producción, pérdidas de ingresos, etc.).
  - Pérdidas de integridad (alteraciones de los archivos y programas, etc.)
  - Fugas indeseadas (de datos e informaciones, de programas, etc.)

  La fuerte interdependencia entre los daños materiales, lógicos y humanos hace que la anterior tipificación no sea única, por lo que también se utilizan otras clasificaciones en base a la magnitud de las pérdidas, los activos afectados, etc. La utilización de estas otras clasificaciones depende fundamentalmente de las prioridades de seguridad de cada organización u organismo.

- **Valoración económica**

  La valoración económica de las pérdidas o *impacto* exige tener en cuenta tanto las económicas tangibles (costo de reparaciones, de reposición de recursos, responsabilidad civil, etc.) como las intangibles.

  Ejemplos típicos de pérdidas intangibles son: pérdida de imagen por errores o retrasos, disminución de ingresos potenciales por salida de información a la competencia, pérdida de posición competitiva en el sector, etc.

  Debe de hacerse un esfuerzo especial en intentar valorar económicamente estas pérdidas intangibles, aunque sea aproximadamente, ya que en muchas ocasiones sobrepasan sensiblemente a las pérdidas tangibles.

3. Defensas y acciones de recuperación

La vulnerabilidad y la seguridad en un ambiente informático están íntimamente ligados y conjuntamente justifican la decisión de adoptar diversas medidas para prevenir riesgos o, al menos, aminorar sus consecuencias.

La seguridad de los sistemas informáticos presenta aspectos comunes con los de cualquier otra instalación que tiene equipos para sus procesos de producción. Pero además presenta aspectos específicos como son los derivados de los programas, datos e informaciones. Los incidentes de seguridad que se producen en un sistema de información pueden perturbar en mucho mayor grado el funcionamiento normal de una empresa que la simple avería, parada o inutilización de una máquina. Por ello, las medidas de seguridad industrial tradicionales son insuficientes para los entornos informáticos. Los aspectos generales de la seguridad admiten un tratamiento industrial; no así los aspectos específicos, que requieren un tratamiento especial.

La vulnerabilidad de los sistemas informáticos se acrecienta principalmente por la continua evolución de la tecnología que obliga a frecuentes cambios de los

recursos físicos y lógicos. Por consiguiente, la prevención ha de ser dinámica y revisar y actualizar continuamente las defensas o medidas de seguridad adoptadas y anticiparse a las nuevas posibles amenazas.

3.1. Tipos de defensa

Las defensas o medidas de seguridad a establecer en un sistema de información se agrupan en cuatro tipos: legales, administrativas u organizativas, físicas y lógicas.

- **Defensas Legales**

  El personal encargado de la seguridad de información debe conocer la *legislación* vigente, que a veces impone obligaciones de seguridad, para conocer que tipos de amenazas deben ser prevenidas especialmente y que tipos de impactos pueden ser perseguidos legalmente. En algunos casos la referencia es a modo de recomendación; en otros, la norma es un imperativo legal. Esto es especialmente importante cuando los activos a proteger contienen datos de carácter personal, los que afectan al honor, a la intimidad personal y familiar, así como a la propia imagen.

  En este sentido, en Venezuela se aprobó en febrero del 2001 la Ley Especial contra los Delitos Informáticos, la cual constituye un adelanto importantísimo en materia de seguridad, ya que no sólo sirve como base legal para combatir y sancionar los actos delictivos, sino que contribuirá en gran medida con la disminución de los mismos y en el proceso de estandarización de mecanismos de seguridad.

  En términos generales, la Ley Especial contra los Delitos Informáticos, persigue lo siguiente:

  - Preveer y sancionar delitos cometidos contra sistemas o cualesquiera de sus componentes.
  - Preveer y sancionar delitos cometidos mediante el uso de tecnologías.

Asimismo:

- Define que los actos delictivos cometidos fuera del territorio de la República con efectos internos podrán ser sancionados si el sujeto no ha sido juzgado o condenado por el mismo en tribunales extranjeros.
- Define los tipos de sanciones a aplicar por cada delito informático.
- Establece las responsabilidades por delitos cometidos a ser imputados a una persona jurídica o dependientes de la persona jurídica que han actuado en nombre o representación de ésta.
- Define varios de los términos utilizados en el resto del documento, sobre tecnología de información.

La Ley Especial contra Delitos Informáticos se conforma por los siguientes capítulos:

- **Capítulo I - DE LOS DELITOS CONTRA LOS SISTEMAS QUE UTILIZAN TECNOLOGÍAS DE INFORMACIÓN.** Este capítulo hace referencia a las sanciones que serán aplicadas a delitos informáticos cometidos contra sistemas que usan tecnologías de información. Estas sanciones podrán tener multas que van desde 10 a 1.000 unidades tributarias, así como prisión de 1 a 10 años. Entre los delitos penados se encuentra accesos indebidos, sabotaje o daño a sistemas, acceso indebido o sabotaje a sistemas protegidos, posesión de equipos o prestación de servicios de sabotaje, espionaje informático, falsificaciones de documento.

- **Capítulo II - DE LOS DELITOS CONTRA LA PROPIEDAD**. En este capítulo se mencionan las sanciones que serán aplicadas a delitos informáticos cometidos contra la propiedad. Estas sanciones podrán tener multas desde 10 a 1.000 unidades tributarias, así como prisión de 1 a 10 años. Entre los delitos penados, se consideran el hurto, fraude, obtención indebida de bienes y servicios, manejo fraudulento de tarjetas inteligentes o

instrumentos análogos, apropiación de tarjetas inteligentes o instrumentos análogos, provisión indebida de bienes o servicios, posesión de equipo para falsificaciones.

- **Capítulo III - DE LOS DELITOS CONTRA LA PRIVACIDAD DE LAS PERSONAS Y DE LAS COMUNICACIONES.** Este capítulo está referido a las sanciones que serán aplicadas a delitos informáticos cometidos contra la privacidad de datos, información o comunicación personal y la revelación de la misma. Estas sanciones podrán tener multas que van desde 200 a 600 unidades tributarias, así como prisión de 2 a 6 años. Entre los delitos que serán penados por esta Ley, se consideran violación de la privacidad de datos o información de carácter personal, violación de privacidad en las comunicaciones, revelación indebida de datos o información de carácter personal.

- **Capítulo IV - DE LOS DELITOS CONTRA NIÑOS, NIÑAS O ADOLESCENTES.** Este capítulo menciona las sanciones que serán aplicadas a delitos informáticos cometidos por difusión o exhibición de material pornográficos a niños, niñas o adolescentes. Estas sanciones podrán tener multas que van desde 200 a 800 unidades tributarias, así como prisión de 2 a 8 años. Entre los delitos que serán penados por esta Ley, se consideran la difusión o exhibición de material pornográfico, exhibición pornográfica de niños o adolescentes.

- **Capítulo V - DE LOS DELITOS CONTRA EL ORDEN ECONÓMICO**. Este capítulo hace referencia a sanciones que serán aplicadas a delitos informáticos cometidos por la apropiación de propiedad intelectual o cualquier oferta engañosa realizada mediante el uso de tecnologías de información. Estas sanciones podrán tener multas que van desde 100 a 500 unidades tributarias, así como prisión de 1 a 5 años.

- **DISPOSICIONES COMUNES**. Adicionalmente a las sanciones que se han mencionado en los capítulos I al V, podrán ser agravantes a las penas señaladas, si para la realización de delitos descritos en esta Ley, se está haciendo uso de contraseñas ajenas obtenidas de manera indebida, si los delitos en cuestión fueran cometidos mediante el abuso de acceso. Asimismo, se considerarán penas accesorias a sanciones ya mencionadas el decomiso de equipos o cualquier otro objeto utilizado para la comisión de delitos, entre otras.

Es importante resaltar, que las leyes no evitan los delitos, por lo que este tipo de defensa es realmente intimidatorio. Pueden utilizarse para perseguir a los infractores y para resarcirse de los daños producidos

- **Defensas Administrativas**

  La verdadera primera forma de defensa y prevención es la adopción de medidas de carácter *administrativo u organizativo,* como la creación de una infraestructura de seguridad informática en los distintos niveles (Comité de Dirección, Comité de Seguridad Informática, Responsable de Seguridad, etc.), políticas, procedimientos, normativas, modelos, planes de seguridad y contingencias.

- **Defensas Físicas**

  El siguiente nivel de protección es el *físico***.** Sin entrar en detalles, este nivel abarca la construcción y control de acceso a los Centros de Procesameinto de Datos, las medidas de protección contra fuegos, fallos de energía eléctrica o falta de aire acondicionado, los armarios de almacenamiento de la cintas de back-up, la protección durante el transporte de los soportes de almacenamiento, las llaves de disqueteras, las defensas contra las amenazas electromagnéticas y cósmicas, etc.

- **Defensas Lógicas**

  En el nivel más cercano a los activos de información se encuentran las medidas de protección *lógicas* o *técnicas*: identificación, autorización y autentificación de usuarios, contraseñas (password), claves, cortafuegos (firewalls), cifrado, antivirus, etc.

  - **Firewall, Muro de Seguridad o Cortafuego**

    Se puede definir de una forma simple un firewall, como aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre dos redes. También se puede decir que es un mecanismo de protección de una red segura (interna) contra una que no lo es (generalmente Internet). Entre sus propiedades podemos mencionar:

    √ Todo el tráfico interno – externo en ambos sentidos pasa a través de él.
    √ Solamente el tráfico autorizado, el cual es definido por las políticas de seguridad local, es permitido pasar a través de los firewalls.
    √ El sistema en sí mismo es altamente resistente a penetraciones.

    El propósito fundamental de los firewalls es mantener a los intrusos fuera del alcance de los activos de información. Entre las clasificaciones encontradas de firewalls, se puede decir que conceptualmente hay tres tipos:

    √ ***Firewalls a nivel de red***: generalmente toman las decisiones basándose en la fuente, dirección destino y puertos, todo ello en paquetes individuales IP. Un simple router es un “tradicional” firewall a nivel de red, particularmente desde el momento que no puede tomar decisiones sofisticadas. Los modernos firewalls a nivel de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellas, los contenidos de algunos datagramas y más cosas.

- √ ***Firewalls a nivel de aplicación***: son generalmente host que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellos. Los firewalls a nivel de aplicación se pueden usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los actuales firewalls tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto es lo que hace diferenciarse de los firewalls a nivel de red.

- √ ***Firewalls por inspección de paquetes***: son combinaciones de los dos anteriores con la finalidad de controlar las capas más bajas y habilitar aplicaciones. Ellos no solo filtran los paquetes, sino también consideran el contenido y la dirección. Los firewalls de este tipo utilizan un módulo de inspección, aplicable a todos los protocolos que integra las funcionalidades de los filtros de paquetes con los de aplicación en un simple punto de inspección. De esta forma se abarca desde la capa de red hasta la de aplicación, lo cual los hace más efectivos en el rendimiento respecto a los firewalls de aplicación.

- **Redes Privadas Virtuales (VPN – por sus siglas en inglés)**

  Las VPN proveen medios para establecer conexiones seguras entre localidades utilizando Internet como red de transporte y basándose en cifrado de información. El cifrado de paquetes en la transmisión evita que posibles intrusos utilicen herramientas (“sniffer”) para capturar la información que atraviesa la red, manteniendo la confidencialidad.

  La VPN puede ser utilizado en la mayoría de tecnologías de transporte disponibles: en la red pública de Internet, en las redes de un Proveedor de Servicios de Internet (ISP por sus siglas en inglés), Frame Relay, así como

las de Modo de Transferencia Asíncrona (ATM por sus siglas en inglés). La funcionalidad de VPN está definida por el equipo instalado en los límites de la red, y no por el protocolo de transporte de la red WAN.

- **Acceso Remoto VPN**

  Las VPN para acceso remoto extienden la red de la corporación a usuarios móviles y oficinas remotas. Permite a los usuarios conectarse a la intranet o extranet a cualquier hora y momento. Existen dos tipos de VPN de acceso remoto: la que utiliza un cliente en su computador del usuario y la que utilizan NAS (del inglés Network Attached Storage).

  El usuario remoto establece un túnel cifrado a través de Internet y del ISP hasta la intranet de la corporación por medio de un software o una aplicación instalada en su equipo y un equipo VPN ubicado en los límites de la empresa. En la Figura N° 4 se muestra el esquema de conexión utilizando aplicaciones VPN. Se puede observar, que el usuario establece una conexión con el NAS del ISP y luego se establece el túnel sobre la PSTN.

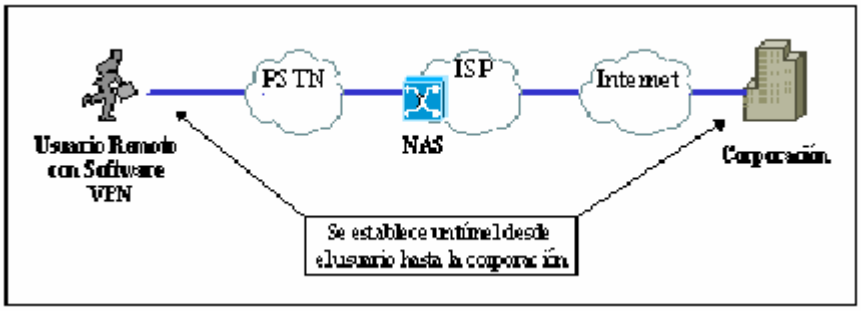


Figura 4. Esquema de conexión utilizando aplicaciones VPN

- **Filtrado IP**

  Cualquier dispositivo en redes TCP/IP - Protocolo de Control de Transmisión (TCP por sus siglas en inglés) y Protocolo de Internet (IP por sus siglas en inglés), se identifica con una dirección IP única. El filtrado IP

es un mecanismo de acceso y control que filtra el tráfico de la red basado en las direcciones IP y servicios solicitados. Esto lo hace utilizando lista de control de acceso (ACL, Access Control List), de las cuales existen 2 tipos:

- √ ACL basadas en el usuario, las cuales describen el servicio al cual se permite o niega el acceso para cada usuario o red.
- √ ACL basadas en el servicio, las cuales describen los usuarios o redes a los cuales se les permite o niega el acceso para cada servicio.

- **Proxy**

  Un proxy es un sistema de software que permite la conexión de una LAN entera al exterior con sólo una dirección IP de salida, es decir, al configurar en el servidor principal de la red un modem, tarjeta de red, entre otros, e instalamos el proxy (configurando también las aplicaciones cliente en terminales), obtendremos acceso al exterior de todos y cada uno de los equipos con una sola cuenta de acceso a Internet. Un proxy es un intermediario para las solicitudes de un usuario a través del firewall. El usuario debe establecer primero una conexión con el firewall, luego ingresar a la aplicación proxy sobre el mismo. La aplicación proxy determina si la petición es permitida, basada en información reunida sobre el usuario y la petición. Si el proxy aprueba la petición, este establecerá una conexión separada desde el firewall hasta el destino de la petición. El proxy entonces recibe la información del usuario y la transmite hacia su destino. El punto impedir que paquetes sean transmitidos directamente a través de las redes; de esta manera el proxy actúa como un intermediario.

- **Sistemas detectores de intrusos (IDS)**

  La detección de intrusos consiste en monitorear en tiempo real las actividades específicas en redes y posteriormente realizar el análisis de información para identificar vulnerabilidades y/o ataques internos o externos.

El manejo de información en tiempo real (opuesto a una revisión periódica de registros guardados o logs) puede reducir significativamente daños potenciales y costos de recuperación ante ataques al eliminar al intruso desde la red. Detectar anomalías en el comportamiento normal de sistemas requiere conocimientos previos. Una forma para determinar el comportamiento normal, es usando herramientas que monitoreen los patrones del tráfico en tiempo real y realice comparaciones con historiales del mismo.

Cuando se evalúa un sistema de detección de intrusos, se debe considerar las siguientes características básicas:

- √ Debe trabajar continuamente sin supervisión humana. El sistema debe ser lo suficientemente confiable para trabajar con el mayor nivel de detalle en el sistema observado.

- √ Debe ser tolerable a fallas, es decir, en caso de ataques o fallas en el sistema a ser observado, el IDS no debe ser impedimento para el restablecimiendo de funciones en el sistema.

- √ No debe introducir retardos elevados.

- √ Debe detectar desviaciones en el comportamiento normal y producir señales de alerta.

- √ Debe acoplarse a los cambios en el comportamiento del sistema para mantenerse actualizado sobre las nuevas aplicaciones.

- √ El IDS debe ser seguro y no abierto a ser comprometido de cualquier forma.

Debido a la cantidad de ataques existentes y en constantes aparición, el uso de herramientas automatizadas es fundamental. Muchos IDS están basados en combinaciones de estadísticas y métodos basados en reglas:

√ El método de análisis estadísticos mantiene historiales estadísticos de cada usuario y sistema que monitorea. Este método origina señales de alarma cuando identifica que alguna actividad no coincide con el patrón del usuario. Esta diseñado para detectar intrusos que se hacen pasar por usuarios legítimos. Al mismo tiempo se detectan intrusos que han explotado vulnerabilidades no conocidas y que no pueden detectarse por otro medio.

√ Método de análisis basado en reglas, utiliza reglas que caracterizan a escenarios de ataques conocidos y crean señales de alarma al detectar comportamientos iguales a los que se encuentran en la base de datos. Este tipo de análisis es diseñado para identificar ataques sobre vulnerabilidades conocidas del sistema. También detecta a intrusos con un tipo de comportamiento conocido.

Por otra parte, existen 2 categorías de sistemas IDS, los sistemas basados en red y sistemas basados en el servidor. Los primeros son instalados sobre la red, cerca del sistema a monitorear, encargándose de examinan el tráfico de red y determinan el estado de la misma en cuanto a ataques de reconocimiento sobre los puertos, monitoreo de conexiones válidas, identificación de intentos de engaños IP de diferentes clases. El sistema basados en el servidor operan sobre el equipo o dispositivo en el cual se lleva a cabo el monitoreo, realizando monitoreos del tráfico entrante y saliente del servidor y sobre los archivos.

- **Programas Antivirus**

  Estos programas, según su forma de actuar se agrupan en las siguientes categorías:

  √ ***Vacunas***: Son los más variados, consisten en programas protectores cuyo fin es impedir que el virus ataque el sistema o se introduzca en él. Normalmente solicitan permiso para efectuar labores de escritura o formateo de disco: También en algunas ocasiones impiden que se sitúen programas residentes en la memoria del computador. Este tipo de programas son de los denominados residentes o TSR siglas del inglés *Terminate and Stay Resident* (Termina y Permanece Residente).

  √ ***Detectores***: son aquellos que detectan la existencia de algún tipo de virus, basándose para ello en las peculiaridades de cada uno de ellos, o bien por procedimientos de almacenamiento de datos de gestión del disco y operaciones de control, detectan alteraciones indeseables del disco (checksum, CRC – Control de redundancia cíclica, etc.).

  √ ***Antivirus***: son los programas dirigidos a destruir virus, eliminándolos de la memoria del computador y de los discos infectados.

  √ ***Chequeadores***: son aquellos que permiten chequear programas desconocidos, para medir su peligrosidad; son de utilidad relativa, ya que cualquier programa puede efectuar operaciones de escritura en disco, pero informaciones de sobreescritura del área del sistema o de formateo y de escritura de sectores absolutos, pueden alterar al usuario.

  Algunas formas de protección no requieren programas especializados, sino que se pueden tomar con las facilidades que proporciona e propio sistema

operativo o sus utilidades más difundidas. Veamos una serie de medidas fáciles de tomar:

- √ Tener siempre copias de seguridad de los archivos de datos o de texto.
- √ Los diskettes deben estar siempre protegidos con la pestaña (los de 31/2") excepto para operaciones de escritura.
- √ Buen número de virus se alojan en archivos ejecutables (.COM, .EXE, .BAT) o similares (.OVL, .ZIP); afortunadamente estos archivos casi nunca se deben modificar, por lo que resulta fácil marcar todos estos archivos como de sólo lectura (read only).
- √ Utilice programa antivirus.

3.2. Actitudes hacia la aplicación de defensas

Independientemente de su tipo, se suele distinguir entre dos grupos de defensas o medidas de seguridad a adoptar para prevenir, contrarrestar o reducir las amenazas: las defensas activas y las defensas pasivas.

- **Seguridad activa**

  La seguridad activa está formada por el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. También pueden denominarse *medidas de prevención*.

  Son comparables, por ejemplo, a los frenos de un automóvil o a la barra antirrobo. Un ejemplo típico de defensa activa informática es un antivirus residente.

- **Seguridad pasiva**

  La seguridad pasiva está formada por las defensas que se implantan para, una vez producido el incidente de seguridad, facilitar la recuperación. Este tipo de seguridad no anula o reduce el riesgo del incidente, sólo intenta paliar sus

consecuencias o corregir los daños ocasionados. A veces se conocen estas defensas como *medida de corrección*.

En el caso del automóvil, las defensas pasivas serían, una vez producido el accidente que no han podido evitar los frenos, el airbag para las personas o el seguro a todo riesgo para los daños sufridos por el vehículo. Caso de defensa pasiva informática sería un antivirus que limpiara los archivos infectados por un virus.

4. Acciones de contingencia

La situación ideal es que las defensas neutralicen las amenazas. Pero esto no es siempre posible, bien por no conocerse la amenaza, bien por no considerarse probable y no existía la defensa adecuada o simplemente por el fallo de la protección. En estos casos se produce el incidente de seguridad afectando a recursos y activos.

Lo importante es recuperar la normalidad lo más rápidamente posible. Para ello es necesario disponer de recursos de respaldo y de un plan de contingencia o de recuperación del negocio.

- **Recursos de respaldo**

  Los recursos de respaldo permiten sustituir a los equipos dañados, recuperar programas o archivos afectados. Pueden ser tanto físicos como lógicos.

  Entre los físicos hay que destacar la duplicación de equipos o la existencia de equipos de reserva. Entre los lógicos destacan los programas para restaurar archivos o las copias de seguridad.

  En general, los recursos de respaldo se utilizan como medios de seguridad pasiva.

- **Plan de contingencia**

  Al plan de contingencia también se le suele denominar Plan de recuperación de negocios, ya que su objetivo es que la empresa vuelva a funcionar normalmente en el menor tiempo posible para que los negocios no queden afectados.

  El Plan de contingencia está formado por una lista de acciones a tomar en caso de incidentes de seguridad. Recoge las respuestas a los diferentes problemas que puedan surgir en forma de planes unitarios. Cada plan contendrá, al menos, dos bloques: plan de emergencia y plan de recuperación.

  El *plan de emergencia* contiene las acciones a realizar inmediatamente después de un incidente o fallo, reflejando las responsabilidades de cada miembro de la plantilla.

  El *plan de recuperación* indica las acciones a emprender para reiniciar las acciones interrumpidas por el incidente.

  Una vez que se ha vuelto a la normalidad es necesario replantearse el plan de seguridad, porque pudiera ser que las defensas y acciones existentes no fueran las adecuadas y el incidente pudiera haber sido evitado. También pudiera deducirse que el incidente era inevitable o que por su baja probabilidad no valga la pena cambiar el plan.

5. Riesgos de los equipos informáticos

La amplia variedad de amenazas que afectan a los equipos informáticos siempre se cristalizan en una única consecuencia: el sistema deja de funcionar.

La paralización del sistema puede conllevar otro impacto aún mayor: la destrucción o desaparición de la información almacenada, que muchas veces es casi imposible de recuperar, o lo es con unos costos muy elevados.

Entre los diversos riesgos podemos examinar los siguientes:

- **Obsolescencia de los soportes de almacenamiento**
  La rápida evolución de las tecnologías de almacenamiento (tarjetas perforadas, cintas magnéticas, casetes, discos magnéticos, discos compactos, etc.) implica que al pasar el tiempo, la información grabada en un determinado soporte sea prácticamente irrecuperable al no disponerse de los periféricos de lectura adecuados. El traspasar enormes cantidades de información de un tipo de soporte a otro implica una gran cantidad de tiempo de sistemas y elevados costos económicos, por lo que muchas veces no se realiza.

  Medida de seguridad: actualización periódica de las bases de datos.

- **Amenazas naturales**
  Las instalaciones de procesos de datos se encuentran sometidas a todo tipo de amenazas y catástrofes (terremotos, inundaciones, tormentas, incendios, etc.) que pueden provocar la interrupción del funcionamiento y, en muchos casos, la destrucción del sistema. Las estadísticas indican que un elevado número de empresas u organizaciones que han tenido un incidente de seguridad de este tipo han quebrado o desaparecido en un breve lapso de tiempo.

  Medida de seguridad: equipo alternativo o plan de contingencia.

- **Problemas eléctricos y electromagnéticos**
  Los fallos del suministro eléctricos y las radiaciones electromagnéticas pueden alterar el funcionamiento de los equipos y los datos almacenados de forma magnética.

  Medidas de seguridad: sistemas antifallo de alimentación continua y normativas de protección.

6. Riesgos de los sistemas de información

Este tipo de riesgo suele ser uno de los más peligrosos y difíciles de detectar, ya que al alterar el funcionamiento normal del sistema y no detectarse a tiempo puede provocar daños irreparables a la información, a los usuarios e incluso al sistema físico.

- **Software malintencionado**

  Abarca un conjunto diverso de programas (virus, gusanos, caballos de Troya, etc.) cuyos objetivos es adueñarse del control del sistema operativo con el fin de provocar, en la mayoría de los casos, la destrucción de la información u otros tipos de daños a los sistemas informáticos.

  Las características de los principales tipos de software malintencionados son las que se explican en los siguientes párrafos, aunque lo normal es que no existan tipos puros, sino programas que reúnen las características de varios de los tipos básicos.

  - **Virus.** Son programas que modifican otros programas o alteran los archivos. Antes se propagaban a través de programas en disquetes que al introducirse en los PC, se liberaban y realizaban sus comandos. Hoy día se propagan principalmente a través del correo electrónico, de ahí su gran poder de propagación debido al desarrollo de los e-mails. Se les denomina así debido a su parecido con los virus biológicos ya que necesitan para vivir un cuerpo vivo, el sistema informático y la red en funcionamiento. Además son capaces de reproducirse y de morir, mediante la utilización del software adecuado. Hay dos tipos de virus. Los benignos y los malignos. Los primeros sólo producen efectos molestos como la superposición de mensajes, movimiento de figuras o transposición de los caracteres de la pantalla. Los malignos pueden borrar archivos de datos o alterar el funcionamiento de los programas. Los más conocidos son Blaster,

MyDoom, Beagle, Passer entre otros. Hay que destacar que el primer virus de la historia fue construido por el investigador informático Fred Cohen cuando trabajaba en conseguir programas inteligentes que pudieran automodificarse, dando lugar a una rama de la informática, de inquietante futuro, la Informática Evolutiva o Vida Artificial.

- **Caballos de Troya o troyanos.** Son comandos introducidos en la secuencia de instrucciones de otros programas legales (de ahí su nombre) y que realizan funciones no autorizadas, destruyen archivos o capturan información mientras simulan efectuar funciones correctas. Un caso particular de los troyanos son los *salami*, generalmente utilizados en instituciones financieras, realizan asientos de pequeñas cantidades, como los redondeos de operaciones de cálculo de intereses, par que no se detecten por su importancia y al final se transfieren a una cuenta bancaria particular.

- **Bombas lógicas.** Son programas que se activan en determinadas condiciones tales como una fecha determinada (Viernes 13) o la presencia o ausencia de un determinado dato en un archivo. Se ha detectado que su uso más común es como elemento de venganza de algún empleado. Caso típico es la bomba que se activa cuando un determinado empleado, su autor, no aparece en el archivo de nómina, por haber sido despedido. El efecto de una bomba es liberar un virus o un troyano. Una bomba lógica puede estar inactiva durante años.

- **Remailers**. Son programas relacionados con la administración y gestión del correo electrónico, que pueden generar órdenes de envío de correos desde un origen a diversos destinatarios y a su vez, utilizando su libreta de direcciones, reenviarlos a estos nuevos destinatarios, creando una cadena de envíos. Actualmente es la manera más común de propagar virus. Johan Helsingius fue el primer conductor de un remailer anónimo

- **Electronic Mail Bombs.** Son también programas relacionados con el correo electrónico y permiten generar órdenes de envío de correos desde uno o varios orígenes a un solo destinatario, generándole una gran cantidad de órdenes y mensajes, con el fin de bloquear su funcionamiento e impidiéndoles, por ejemplo, atender pedidos o responder consultas. A este efecto se le conoce como *negación de servicios.*

- **Worms o gusanos.** Deben a su origen a los investigadores Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky, desarrolladores de un juego de estrategia denominado Corewar (Guerra de la Memoria), que consistía en que ganaba el jugador que era capaz de ocupar más cantidad de memoria. El gusano no necesita, a diferencia de los virus otro programa para funcionar y simplemente se va duplicando y ocupando memoria hasta que su tamaño desborda al sistema informático en que se instala, impidiéndole realizar ningún trabajo efectivo.

- **Recuperadores de elementos borrados.** Cuando se da la orden de borrar un archivo, ya sea de datos o de programas, realmente lo que se hace es declarar, en el directorio que controla el soporte, que el espacio que antes estaba ocupado queda libre para almacenar otra información. Por consiguiente, la información antigua permanece en ese lugar, no se ha borrado físicamente, pero es inabordable por los sistemas normales. La información sólo desaparece cuando otra ocupa su lugar. Los programas recuperadores permiten obtener esa información siempre que no se haya superpuesto otra; de esta manera se obtiene informaciones teóricamente destruidas.

- **Puertas falsas o Back Doors.** Está técnica permite introducirse en los programas por puntos que no son los estándares o normales. En principio eran utilizados por los programadores para facilitar el proceso de pruebas,

evitando tener que procesar todo el programa o sistema para probar sólo un trozo. Si estas puertas falsas se mantienen en la versión operativa, bien de forma intencionada o por descuido, se crean agujeros en la seguridad de la aplicación.

- **Sniffers o Rastreadores.** Son programas que se ejecutan en una red informática y rastrean todas las transacciones que viajan por ella para volcarlas en un fichero. El estudio de este archivo permite encontrar claves, números de tarjetas de crédito, etc., que pueden ser utilizados de forma fraudulenta. En general los programas están escritos en lenguaje C y pueden encontrarse disponibles en algunos foros de debate de Internet.

Medidas de seguridad: antivirus y cortafuegos (firewalls), así como otros tipos de software de protección y de rastreo de cadenas de bits identificables como de operaciones peligrosas y programas de análisis del log del sistema para detectar transacciones no autorizadas.

- **Copias ilegales**

Cada vez más circulan por la red todo tipo de programas que permiten la copia de otros programas, música, tarjetas de TV, Discos Compactos (CD por sus siglas en Inglés), películas, etc. Todo ello ocasiona un fraude a los derechos de autor y a los beneficios de empresas editoras, cinematográficas, discográficas, de TV, etc., que se elevan a miles de millones anuales, y que ponen en peligro el futuro de algunos sectores económicos dedicados al ocio.

Medidas de protección: Cambio periódico de los sistemas de protección de los diferentes soporte. Estas medidas son muy poco eficaces, ya que en plazos muy breves aparecen sistemas de desprotección.

- **Negación de servicios**

  Consiste en el envío de mensajes masivos a un servidor, mediante los programas ya comentados, con el único fin de saturarlo y bloquearlo, impidiendo el normal funcionamiento del sistema.

  El riesgo es muy importante en servidores y hosts que administran servicios importantes como el tráfico aéreo, ferroviario, distribución eléctrica, o seguridad nacional por las graves consecuencias que para el normal funcionamiento de los correspondientes servicios tendría la negación de los mismos.

  Medidas de protección: Separar el servidor de correo electrónico o de páginas web de la red local o de la Intranet del usuario. Muchas veces esto es imposible por la propia configuración del sistema. Además en los entornos de la Seguridad Informática, existe el aforismo de que *el único computador seguro es el que se encuentra aislado en una habitación con las correspondientes medidas de seguridad física y sin estar conectado a ninguna fuente de suministro eléctrico*.

7. Función de Seguridad de Activos de Información (FSAI)

El propósito de establecer el alcance de la seguridad de la información dentro de una organización es establecer un único punto de responsabilidad en materia de seguridad en tecnología, las políticas de la organización y los servicios que se prestarán. Adicionalmente, la organización de la seguridad debe estar posicionada en un lugar tal que exista un compromiso se seguridad con cada una de las áreas de la organización y bajo el patrocinio de la alta gerencia.

El impacto de centralizar la definición y administración de las políticas de seguridad es crítico, ya que afecta en todas las áreas de la organización. El Gerente de Seguridad CISO del inglés *Chief Information Security Officer*, quien lidera la FSAI, será quien regularmente actualizará las políticas. Estas

actualizaciones incluyen cambios en las políticas y otras informaciones de seguridad.

En cuanto al lugar de ubicación de la FSAI dentro de la organización, el mismo debe ser en un nivel suficientemente alto para aumentar al máximo su efectividad. Una práctica muy usada en las organizaciones, es colocar al Gerente de Seguridad (Chief Information Security Officer, CISO) al mismo nivel staff que soporte todos los procesos referentes al área de tecnología, lo cual ayuda a asegurar una visión integral y la independencia de criterio que debe prevalecer en una gerencia de esta naturaleza.

7.1. Misión y metas de la FSAI

La misión de la FSAI es proveer una efectiva y apropiadas políticas de seguridad en tecnología para todas las áreas que comparten información, proveen servicios o administran negocios a través de Internet. Las metas específicas de la organización incluyen:

- Desarrollo e implementación de políticas y estándares de seguridad de activos de información.
- Proveer soporte técnico y asistencia para la implantación de políticas y estándares de seguridad.
- Monitoreo y medida de los procesos de seguridad de las áreas de la organización e implementación de tecnología.
- Coordinación y administración de reportes de incidentes de seguridad y análisis de vulnerabilidades, así como la comunicación con las áreas afectadas.
- Desarrollo de entrenamientos de seguridad para ejecutivos, gerentes, técnicos y personal administrativos.

7.2. Funciones de la FSAI

La misión y metas de la organización deben estar reflejadas en la estructura organizacional de la unidad encargada de administrar la seguridad de tecnología de la compañía. Cada área funcional debe tener objetivos definidos, los cuales deben ser consistentes con los objetivos del negocio de la organización. El grado en que esto ocurre afecta la percepción, aceptación y efectividad de esta unidad.

En cuanto a las funciones de FSAI un factor importante es la aptitud y habilidad técnica del equipo que la conforma, ya que con una estructura de reporte apropiada esta unidad recibe el enfoque y autoridad para llevar a cabo las medidas de seguridad.

El próximo paso en el proceso de definición de la FSAI es construir el conjunto de herramientas necesarias para dirigir varias áreas de seguridad dentro de la organización. Dependiendo de las necesidades esto puede involucrar varios talentos diversos. La organización de seguridad debe poder entonces manejar algunas de las siguientes áreas:

- Políticas de seguridad.
- Operación técnica de sistemas o seguridad de base de datos.
- Herramientas y paquetes de seguridad.
- Aplicación de niveles de seguridad.
- Procedimientos o integridad de procesos.
- Seguridad física.
- Conocimientos de programas de seguridad.
- Procedimientos de auditoría.

Por consiguiente, el conjunto de habilidades incluidas dentro de la FSAI debe ser amplio. Se necesitan habilidades técnicas relacionadas con la seguridad de información, asimismo se necesitan habilidades de administración del riesgo para el negocio o los procesos relacionados con seguridad de activos de información.

Por esa razón, dentro de esta estructura organizativa, deben estar definidos los programas de entrenamiento y desarrollo de estas habilidades.

La estructura organizacional de la FSAI no sólo debe tratar de seguridad en tecnología, ya que implica tanto aspectos técnicos como aspectos de riesgo. El propósito de crear un equipo de seguridad multidisciplinario es administrar la seguridad en todos los aspectos. Esto llevará a la organización a un alto grado de cooperación con las funciones de Auditoría Interna y/o el departamento de Seguridad Física.

En este sentido, aunque el objetivo es crear un equipo multidisciplinario de diversos profesionales, es también extender el alcance de seguridad en otras áreas de la organización.

CAPÍTULO III

MARCO METODOLÓGICO

1. Método de investigación

El método de investigación utilizado fue la investigación proyectiva, también conocida como proyecto factible. Este método define el enfoque de la investigación, y por ende la forma de presentar el cumplimiento de los objetivos y resultados finales del trabajo.

Según la Universidad Pedagógica Experimental Libertador (UPEL) (1990), "El proyecto factible consiste en la elaboración de una propuesta de un modelo operativo viable, o una solución posible a un problema de tipo práctico, para satisfacer necesidades de una institución o grupo social" (p.7).

2. Área de investigación

El desarrollo de la investigación se llevó a cabo en la Gerencia de Banca Virtual de la Entidad Financiera ABC, la cual se encuentra ubicada en la oficina principal, lugar donde lugar reside la infraestructura principal de comunicaciones y redes de datos.

3. Descripción de la metodología

Para el desarrollo de este proyecto, se consideró el estándar de seguridad ISO 17799 publicado por la Organización Internacional de Normas en diciembre de 2000, el cual es un código de buenas prácticas para gestionar la seguridad de la información de una organización, de tal forma que le permita en todo momento garantizar la confidencialidad, integridad y disponibilidad de la información que maneja. La creación de esta norma responde a la necesidad de proporcionar una base común a las organizaciones desde la triple óptica técnica, organizativa y jurídica, y cuyo cumplimiento implique que dicha organización mantiene una

infraestructura y un esquema de funcionamiento que garantizan la seguridad de la información.

3.1. El origen de ISO 17799

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI por sus siglas en inglés) y la Organización Internacional de Normas Técnicas (ISO por sus siglas en inglés) han brindado parámetros globales a normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de información.

Finalmente en 1995, el BSI publicó la primera norma técnica de seguridad, BS (por sus siglas en inglés) 7799, la cual se redacta para abarcar los asuntos de seguridad relacionados con el "e-commerce", sin embargo no tuvo la aceptación esperada debido a que no despertó interés de la comunidad. Cuatro años después, en mayo de 1999, el BSI intentó nuevamente publicar su segunda versión de la norma BS 7799, siendo una revisión más amplia y mejorada de la primera publicación. En este momento, la ISO se percató de cambios y comenzó a trabajar en la revisión de la norma técnica BS 7799.

En diciembre de 2000, la ISO adoptó y publicó la primera parte de la norma BS 7799 bajo el nombre de ISO 17799. Alrededor de la misma época, se adoptó un medio formal de acreditación y certificación para cumplir con la misma. La adopción por parte de ISO de la Parte 1 de los criterios de la norma técnica de BS 7799, recibió gran aceptación por parte del sector internacional y fue en este momento que un grupo de normas técnicas de seguridad tuvo amplio reconocimiento.

La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy día es una compilación de recomendaciones de las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada

intencionalmente para que fuese flexible y nunca indujo a cumplir soluciones de seguridad específicas. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes. Por ejemplo, la norma discute la necesidad de contar con firewall, pero no profundiza sobre los 3 tipos de firewall y cómo se utilizan, lo que conlleva a que contrarios de la norma opinen que ISO 17799 es general y tiene una estructura muy imprecisa y sin valor real.

La flexibilidad e imprecisión de ISO 177999 es intencional, por cuanto es difícil encontrar una norma que funcione sobre una variedad de entornos de tecnología de información y sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 177999 simplemente ofrece un conjunto de reglas a un sector donde no existían.

3.2. Las diez áreas de control del ISO 17799

La norma define la seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información, siendo necesario para ello no solo medidas técnicas sino también políticas y organizativas. Para alcanzarla define diez áreas de control, las cuales se detallan a continuación.

- **Políticas de Seguridad**

  El objetivo principal es la elaboración de un documento de políticas de seguridad publicado por el máximo nivel directivo de la organización, con una declaración apoyando sus objetivos y principios. En este documento se describirán brevemente las políticas, principios y normas que en materia de seguridad se consideren esenciales y se establecerá la jerarquía de responsabilidades en la gestión de la seguridad indicando claramente quien se hace responsable de los activos. Incluirá referencias a la legislación aplicable y a los documentos de detalle donde se encuentran desarrolladas las normas.

Se debe asegurar que se comunica esta política a todos los usuarios del sistema y que es fácilmente comprensible por todos ellos, ya que es el medio de dar a conocer la implicación de la Dirección en las políticas de seguridad además de su contenido.

- **Organización de la Seguridad**

  Se trata de desarrollar el documento gerencial de políticas de seguridad desde tres puntos de vista distintos, cuando los sistemas son gestionados por la propia organización, cuando existen accesos de terceras partes (asistencia técnica, por ejemplo) y cuando todos los sistemas de información están externalizados por medio de un outsourcing.

  En el primer caso debe haber un comité de dirección encargado de impulsar, hacer el seguimiento y revisar las políticas de seguridad, independientemente de que exista un responsable de seguridad encargado de la misma. Para la implementación de los controles puede ser conveniente la existencia de otro foro con representantes de áreas ajenas a las tecnologías de la información y que acuerde funciones, metodologías, revisiones o como realizar la difusión en materias relacionadas con la seguridad de la información. Deben definirse los responsables, en general los propietarios de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos ni solapamientos. Es de resaltar la importancia de tener correctamente establecido el protocolo de actuación ante la instalación de nuevos sistemas de información, ya que esta no se debe llevar a cabo sin el pertinente estudio del impacto que producirá en la seguridad y, en su caso, de las medidas suplementarias al plan de seguridad establecido.

  En el caso de la contratación de terceros que desarrollarán su labor dentro de la organización o de contratación de un outsourcing total, es esencial tener un modelo de contrato, validado por el departamento jurídico si hiciera falta, que

contenga todos los requerimientos de seguridad para asegurar el cumplimiento de las políticas y normas de la organización. Además debe ser lo suficientemente claro para que no puedan surgir malentendidos entre la organización y el proveedor.

- **Clasificación y control de activos de información**

  Para mantener una adecuada protección de los activos hay que identificar claramente cuales son y asignarles un grado de protección según su sensibilidad y criticidad, indicando en cada caso como ha de ser tratado y protegido.

  Lo primero será contar con un exhaustivo inventario de activos que incluirá los recursos de información de todo tipo, recursos software y hardware, servicios informáticos y de comunicaciones y aquellos otros recursos que nos afecten como climatización, suministro eléctrico, etc. Una vez realizado se le asignará a cada recurso un grado de protección que marcará las medidas de seguridad que le serán aplicables y el tiempo durante el cual estarán vigentes siendo responsable de esta asignación el dueño o responsable del activo. Por último es conveniente manejar esta información de una manera organizada incluyendo algún tipo de clasificación sistemática que ayude a su mantenimiento y control.

- **Seguridad del personal**

  En cuanto al personal la seguridad se basará en tres pilares básicos, la seguridad inherente al puesto desempeñado, la formación en materia de seguridad y la respuesta ante incidentes.

  La seguridad del puesto deberá enfocarse a evitar que personal malintencionado utilice los medios de la organización para provocar fallos de seguridad y se evitan con una adecuada política de selección de personal, tanto propio como contratado temporalmente, e incluyendo condiciones y

términos en los contratos que indiquen claramente las responsabilidades y las obligaciones. El trabajo de todo el personal debe ser periódicamente revisado y nuevamente aprobado por un superior jerárquico.

La formación en materia de seguridad implica que ningún usuario desconozca la política general de seguridad ni las normas específicas que le afectan en el desarrollo de sus funciones. Para ello se promoverán cursos de formación y actualizaciones periódicas de los conocimientos, así como todas aquellas medidas de difusión que se consideren oportunas.

Es esencial para minimizar el numero de incidentes de seguridad y su alcance establecer un sistema de comunicación de incidencias hardware, software o de cualquier tipo, que todos los usuarios puedan utilizar y que sirva para reaccionar con rapidez ante cualquier amenaza o para evitarla antes de que se produzca. También habrá que disponer de un procedimiento establecido de respuesta a incidentes que establezca las acciones a realizar ante un aviso de incidente. Este sistema servirá también para actualizar las políticas de seguridad de la organización teniendo en cuenta los incidentes más habituales o graves. Por último se habrá de establecer y difundir las sanciones disciplinarias cuando sean los propios empleados los que provoquen los incidentes.

- **Seguridad física y del entorno**

  Un primer objetivo será impedir el acceso a las áreas seguras de personal no autorizado. Estas zonas habrán de estar claramente delimitadas pero no de forma claramente visible sino de una manera formal, con un perímetro permanentemente controlado. Se pueden definir varios tipos de zonas seguras dependiendo del tipo de sistema informático que contengan y de su grado de criticidad y, por lo tanto, las medidas de seguridad en cada tipo serán acordes a dicho grado. Las medidas para evitar accesos no autorizados y daños en los sistemas suelen ser barreras físicas y de control de cualquier tipo, pero

también la ausencia de información sobre lo que contiene un área segura y la falta de signos externos que puedan hacer adivinar su contenido.

Deberá tenerse en cuenta cuando se diseñe el sistema de información que la ubicación e infraestructuras del mismo sean las adecuadas para reducir el riesgo de amenazas naturales como incendios, vibraciones, inundaciones, etc. También se pondrán medios para atajar aquellas no directamente relacionadas con el sistema de información pero que pueden afectar a su funcionamiento como pueden ser el suministro de energía incorporando un sistema de alimentación ininterrumpida de capacidad suficiente, proteger contra cortes o intrusiones el cableado de suministro de datos y energía, facilitar un adecuado mantenimiento de los equipos y establecer unas normas de seguridad para el equipamiento que contenga datos sensibles y que salga fuera de la organización y nunca permitir su salida sin autorización. Se debe asegurar que los soportes susceptibles de contener información sensible son físicamente destruidos o sobrescritos antes de desecharlos.

Es conveniente establecer políticas de escritorios sin papeles para evitar el robo o destrucción de datos y de pantallas limpias, no dejando en la misma ningún dato sensible al dejar el puesto sin atención.

- **Gestión de comunicaciones y operaciones**

  Los procedimientos operativos, cualquiera que sea su tipo, deben estar perfectamente documentados por su política de seguridad, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes. Asimismo se ha de dar especial importancia a los cambios en los sistemas o instalaciones ya que son fuente frecuente de fallos del sistema y de seguridad.

Se debe establecer una serie de procedimientos de manejo de los incidentes para responder lo más rápida y eficazmente posible, estableciéndose como mínimo procedimientos para todos los tipos de incidentes probables, tratando de identificar las causas, indicando el modo de auditado del sistema afectado e incluyendo protocolos detallados de las acciones de recuperación.

Para reducir el riesgo de mal uso del sistema se deben separar las tareas de gestión de las de ejecución impidiendo que haga una misma persona todo el proceso. También se separaran las áreas de desarrollo de la de producción para evitar errores por incorrecciones en los sistemas o fallos forzados.

Cuando el sistema de información se encuentra en una instalación externa los controles deben ser los mismos pero deben encontrarse claramente especificados en el contrato.

Una adecuado monitoreo del uso de los recursos del sistema nos permitirá detectar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación. Estas ampliaciones se realizarán cuando estén perfectamente asegurado el correcto funcionamiento en el sistema existente y su adecuación a las normas de seguridad.

En cuanto a elementos software es esencial controlar la introducción de software malicioso que pudiera degradar los sistemas o introducir vulnerabilidades, para lo cual se implementarán los controles necesarios para evitar su instalación y se promoverán medidas para concienciar a los usuarios del riesgo que suponen y para formarles en un uso seguro del sistema.

Existirá un programa de copias de respaldo para todos los datos no recuperables de la organización, que se guardarán en una ubicación independiente con los mismos niveles de seguridad que en su emplazamiento

original y por un periodo de tiempo que dependerá de la naturaleza y sensibilidad de los datos. Se realizarán ensayos de recuperación para comprobar la viabilidad del protocolo y validez del programa.

Se mantendrá un registro de actividades del personal de operación así como de los errores del sistema detectados, revisándolos para verificar la resolución de los fallos y que las medidas que se tomaron para ello estaban dentro de las normas.

La administración de las redes de datos deben incluir los controles necesarios para garantizar la seguridad de los datos y la protección de los servicios contra el acceso no autorizado. Se tomarán medidas adicionales, principalmente cifrado, cuando los datos sean especialmente sensibles. Cualquier medio susceptible de almacenar datos ha de ser tenido en cuenta dentro de las políticas de seguridad y especialmente los soportes removibles como discos o papel, estableciéndose procedimientos operativos para protegerlos contra robo, daño o acceso no autorizado y procedimientos para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo. La documentación del sistema debe ser también protegida ya que suele contener información valiosa y que puede ser utilizada para vulnerar el sistema.

Un apartado especial tienen los intercambios que se realizan entre distintas organizaciones que debido a la variedad de formatos implicados (correo electrónico, comercio electrónico, mensajero, fax, teléfono, etc.) exigen un control cuidadoso. Se establecerán acuerdos (preferiblemente escritos) con las otras organizaciones que respeten por una parte la política de seguridad de la organización y por otra la legislación aplicable, solo se utilizarán medios de transmisión que sean seguros y se establecerán normas para que el propio envío (datos, paquetes, etc.) incluya todas las medidas de seguridad consideradas adecuadas a su naturaleza. Respecto al correo electrónico se elaborará una política clara para todos los usuarios respecto al uso de anexos

y almacenamiento de los mismos, el uso responsable de tal manera que no se comprometa a la organización y técnicas de cifrado para proteger la confidencialidad y la integridad. En definitiva se promoverá entre el personal de la organización una actitud activa por la seguridad formando sobre actos cotidianos que la comprometen y que son fáciles de evitar como intentar no ser escuchado al hablar por teléfono, no usar contestadores o el envío de fax con información sensible a números equivocados.

- **Control de accesos**

  Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Está política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos. Por otra parte las reglas que se definan deberán ser preferiblemente restrictivas (no permitir el acceso nunca excepto cuando se necesite mejor que permitirlo siempre excepto cuando exista riesgo) y modificables solo por el administrador.

  Se implementará un procedimiento formal que cubra todo el ciclo de vida del registro de un usuario, desde su alta donde se verificará que los accesos otorgados sean los adecuados a las necesidades y que exista un permiso de uso de los recursos accedidos, la cancelación inmediata de permisos ante cambios en las tareas del usuario, verificaciones periódicas de consistencia de los permisos y usuarios del sistema o utilización de identificadores únicos.

  Es importante limitar todo lo posible la asignación de privilegios que permitan evitar los controles de acceso estándar ya que son la principal vulnerabilidad de un sistema, por lo que deberán estar perfectamente identificados, asignarse sobre la base de la necesidad de uso y evento por evento y a un identificador de usuario distinto al de uso habitual. Los derechos de acceso serán revisados

a intervalos regulares y tras cada cambio en un usuario y los privilegios con una mayor frecuencia.

La asignación de contraseñas se controlará a través de un procedimiento formal que impida su almacenamiento o envió sin la debida protección y que incluya reglas para impedir su captura o adivinación.

En entornos especialmente sensibles se proveerán sistemas de identificación más fuertes como huellas, candados hardware u otros. Por otra parte se informará a los usuarios de buenas prácticas en el uso de contraseñas, como no compartirlas ni tenerlas escritas o cambiarlas regularmente y usar contraseñas robustas. Es conveniente bloquear por contraseña las sesiones de terminal o PC cuando el usuario se ausente del puesto.

Es esencial para la organización la protección de los servicios de red para impedir que sean interrumpidos o accedidos ilegalmente. Las normas para su protección, que han de ser coherentes con la política de control de accesos, se plasmarán en un documento de política de uso de los servicios de red. Todo usuario externo o nodo automático que intente acceder al sistema ha de ser autentificado preferiblemente con técnicas fuertes como el cifrado. Es recomendable la definición de caminos forzados entre terminales de usuario y los servicios del sistema así como la división de la red en subredes lógicas y aisladas. Todos los accesos a la red deben ser validados contra las reglas de control de accesos e incluir un control de origen y destino de la conexión, independientemente de las validaciones de seguridad que cada servicio del sistema incluya.

Es importante vigilar el acceso al sistema operativo ya que su control supone el dominio de una parte importante del sistema, por lo que se usarán todas las medidas de seguridad que incluya destacando la identificación y verificación segura de los usuarios, aplicaciones y terminales y el registro de los intentos

de conexión al sistema. Se dispondrá de un sólido sistema de administración de contraseñas y se establecerán reglas sobre limitación del horario de uso y desconexión automática por inactividad.

El acceso a las aplicaciones estará limitado a los usuarios autorizados basándose en las normas de control de accesos y estará claramente documentado para cada aplicación su nivel de sensibilidad, aplicando las medidas de seguridad indicadas a dicho nivel.

Es esencial para preservar la seguridad del sistema la supervisión y seguimiento de todas las incidencias que se produzcan lo que permitirá la detección temprana de incidentes y la validación de la bondad de los controles de seguridad adoptados. Se guardará un registro de los eventos de seguridad como accesos con o sin éxito a aplicaciones o a datos, usuarios que han accedido y por cuanto tiempo, alarmas del sistema y otros que se consideren necesarios para la recolección de evidencias de incidentes. Regularmente este registro debe ser revisado en busca de evidencias que indiquen algún compromiso de la seguridad.

Cuando en el sistema exista la posibilidad de teletrabajo o de computación móvil será necesario estudiar la sensibilidad de los sistemas desplazados e implementar las medidas de seguridad acordes con la misma y, al mismo tiempo, se dictarán normas especificas para este tipo de sistemas como por ejemplo sobre la seguridad física de los equipos contra robo o rotura o sobre el uso en público de los mismos.

- **Desarrollo y mantenimiento de sistemas**

  Se trata de asegurar que todos los requerimientos de seguridad que se han definido son incluidos en el sistema de información, ya que es en el momento del desarrollo de los sistemas cuando más económico es implementarlos. Las aplicaciones se deben diseñar para que incluyan los controles de acceso necesarios así como para que dejen registro de actividad. Se validarán los datos de entrada y de salida y se verificara la integridad y autenticidad de los mismos según se considere necesario.

  Se deben utilizar técnicas de cifrado para preservar la confidencialidad, autenticidad e integridad de la información que, tras una evaluación de los riesgos, sea considerada como especialmente sensible. Esta política en materia de cifrado tendrá en cuenta la legislación aplicable así como los estándares técnicos y las necesidades de la organización. También incorporará los casos y condiciones de uso de la firma digital o de servicio de no repudio. Es esencial la gestión de las claves de cifrado por lo que se establecerán normas y procedimientos para su administración, tanto en el caso de técnicas de clave secreta como de clave pública.

  En el entorno de producción se controlará el acceso al software de sistema así como a los datos de prueba que se haya podido utilizar y a las bibliotecas de código fuente ya que contienen información interna sensible sobre el funcionamiento del sistema. En el entorno de mantenimiento se verificará que todos los cambios que se realicen en las aplicaciones están autorizados y existirá un procedimiento para llevarlos a cabo, al igual que las revisiones técnicas del sistema operativo o los cambios en los paquetes comerciales de software; todos los cambios han de quedar perfectamente documentados y tener una verificación previa de conformidad con las normas de seguridad.

- **Gestión de la continuidad**

  Toda organización ha de contar con un plan de actuación ante contingencias que permita identificar y reducir los riesgos de que se produzcan interrupciones en el servicio, atenuar en lo posible las consecuencias de los incidentes y asegurar que se reanuda la actividad lo antes posible.

  La implementación de un proceso controlado para el mantenimiento de la actividad debe incluir una identificación clara de los eventos que pueden provocar su interrupción, evaluando el riesgo de ocurrencia y calculando el impacto que tendría sobre la organización, y esto para cada proceso de la organización. En base a esto se documentaran los procedimientos de actuación ante incidencias y se formará al personal que deba llevarlos a cabo, realizando las pruebas necesarias y actualizando los procedimientos cuando se produzcan cambios en el sistema o cuando las pruebas de reevaluación indiquen fallos. Estos planes contendrán como mínimo las causas de activación, el personal implicado y los procedimientos de actuación y de recuperación con sus diagramas de tiempos correspondientes, y debe tener un propietario o responsable del mismo. Asimismo se realizará el mantenimiento periódico del plan de continuidad para garantizar que es eficaz y que se encuentra vigente.

- **Cumplimiento**

  Dentro de los controles de la conformidad se incluirán la conservación de aquellos archivos o registros que determine el marco legal, el uso adecuado por parte del personal de los recursos de la organización y el uso que se hace de las técnicas de cifrado. Es conveniente mantener un registro de evidencias que, desde un punto de vista legal, pudiera ser utilizado en un tribunal, por lo que deberán cumplir todos los requisitos para su admisión como son la validez general a través del cumplimiento de estándares, la calidad con copias fieles y la totalidad de la prueba, conservando todo el registro de la acción.

La política de seguridad de la información debe estar en permanente revisión para, por una parte, vigilar que se esté produciendo un adecuado cumplimiento de la misma por todas las áreas de la organización y por otra mediante el uso de verificaciones técnicas para comprobar que el sistema es seguro ante las incidencias que se puedan prever. Se proveerán herramientas de auditoria que deben estar separadas del resto de sistemas de información y cuyo uso estará limitado y controlado por un acuerdo donde se indique el alcance de las verificaciones y los procedimientos a llevar a cabo.

CAPÍTULO IV

SITUACIÓN ACTUAL

1. Entidad Financiera ABC

La Entidad Financiera ABC es una organización que ofrece servicios financieros integrales para personas naturales y jurídicas en las regiones de Guayana, Oriente, Centro, Occidente e Insular, con presencia estratégica nacional.

Su sede principal se encuentra ubicada en la ciudad de Puerto Ordaz y cuenta con aproximadamente 100 puntos de atención entre agencias, taquillas bancarias, taquillas externas y autobancos, distribuidos en los estados Bolívar, Anzoátegui, Monagas, Nueva Esparta, Delta Amacuro, Sucre, Miranda, Aragua, Carabobo, Cojedes, Mérida, Trujillo, Barinas, Portuguesa, Táchira, Zulia y el Distrito Capital.

Entre los servicios ofrecidos se pueden mencionar los siguientes:

- **Servicios Electrónicos**

  - *Banca OnLine:* Banca por Internet que le permite al cliente realizar sus operaciones financieras a través de un computador conectado a Internet, las 24 horas del día, los 365 días del año .
  - *Centro de atención telefónica*: Centro de atención que sirve como alternativa a los clientes para efectuar transacciones puntuales vía telefónica.
  - *Tarjetas de Débito*: Plástico intransferible, que permite realizar operaciones a través de los cajeros automáticos, Centro de Atención Telefónica y Puntos de Ventas.
  - *Cajeros automáticos*: Dispensador de dinero en efectivo en forma automática. Adicionalmente, permite realizar consultas de saldos y hacer

transferencias entre cuentas de un mismo cliente asociadas a la Tarjeta de Débito.

- *Afiliación a comercios (Puntos de ventas electrónicos):* Relación comercial a través de la cual el banco adquirente permite al comercio recibir, como forma de pago, tarjetas de crédito VISA y MasterCard y tarjetas de débito Maestro, nacionales e internacionales, servicio por el cual el banco le cobra al comercio una comisión sobre las ventas canceladas con dichos medios de pago

- **Servicios Financieros**

  - *Taquillas externas*: Taquillas de atención que permiten a los clientes realizar transacciones rápidas fuera del horario convencional de atención al público.
  - *Cheques de gerencia*: Título valor nominativo o a la orden, emitidos y respaldos por la Entidad Financiera ABC.
  - *Recepción de pagos de servicios básicos*: Recepción y pagos de servicios (Eleoriente y CANTV)

2. Servicio de Banca Virtual

El acceso al servicio de Banca Virtual de la Entidad Financiera ABC denominada *BANCA On Line*, se presta diferenciando a los clientes naturales y jurídicos. En el caso de las personas naturales se utilizará el número de tarjeta de débito con la cual accede normalmente a cajeros automáticos y puntos de ventas, utilizando una clave o pin, diferente a la usada para estos servicios, la cual el cliente establece al momento de su registro como se describe más adelante. Las personas debidamente autorizadas por las empresas y grupos económicos para acceder al servicio y manejar sus cuentas, utilizarán un dispositivo de seguridad,

RSA SecurID (The Security Division of EMC Corporation - conocida también por RSA Security-) y una identificación o código de usuario.

Los clientes Naturales y Jurídicos accederán al servicios mediante un link ubicado en la página institucional de la Entidad Financiera ABC www.entidadfinancieraABC.com.ve

En la pantalla de inicio de sesión el cliente según sea su condición, Persona o Empresa, selecciona el acceso al servicio.

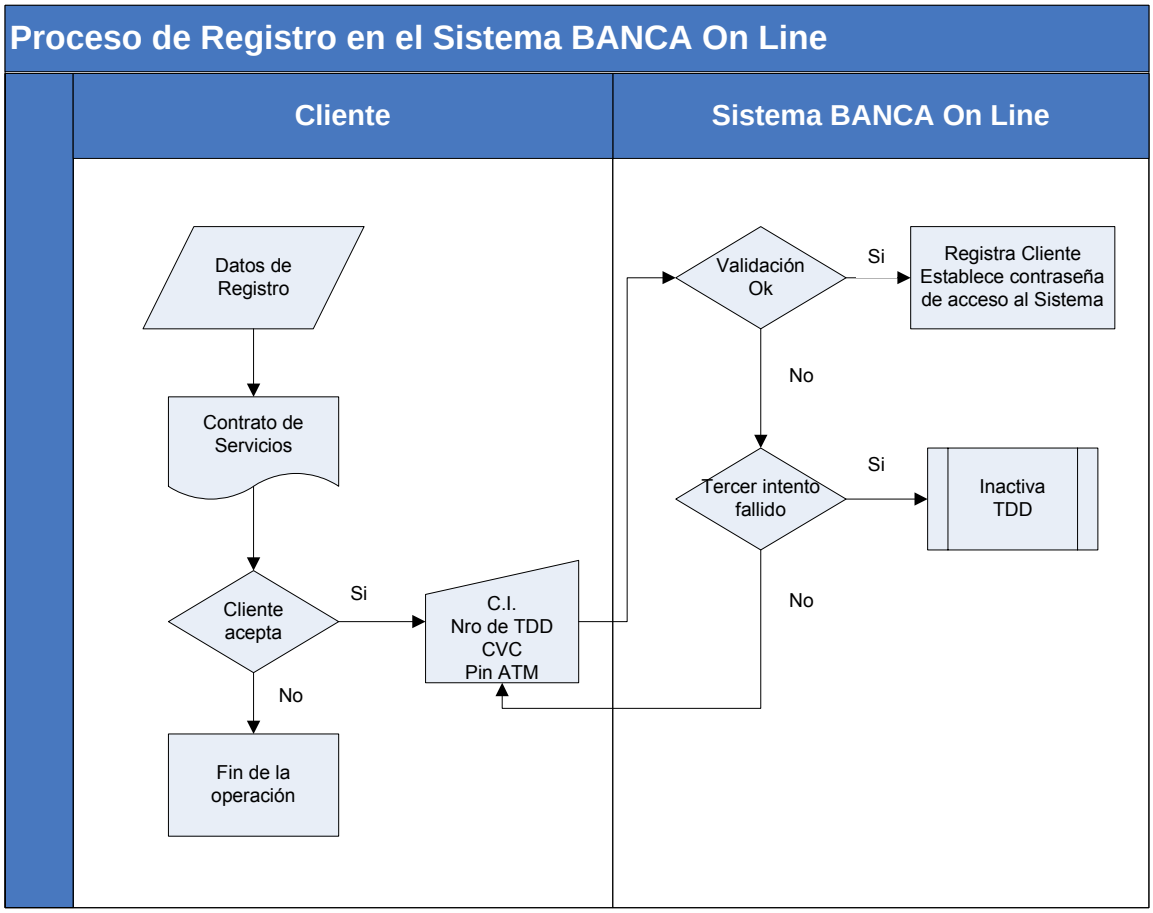
- **Personas Naturales**

El cliente para acceder al servicio, deberá registrarse por única vez a éste, haciendo clic a un link que lo envía a la pantalla con el formato de registro.

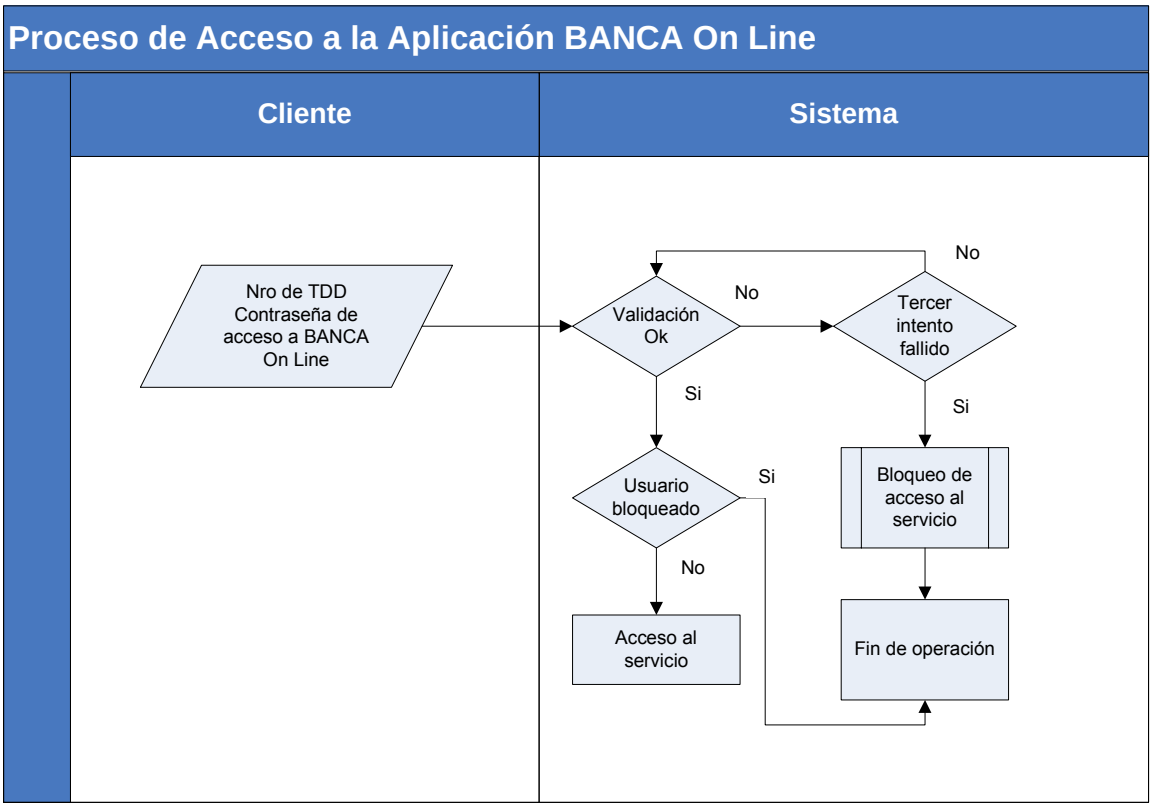
En la pantalla de registro, el cliente coloca sus datos personales y socio económicos. La Identificación del cliente en el servicio se obtiene sometiendo a validación, la Cedula de Identidad, Número de la Tarjeta de Débito, la contraseña utilizada para los servicios de Cajero Automático y Punto de Ventas y el código de seguridad CVC (del inglés *Card Verification Code*) ubicado en el reverso de la tarjeta, a partir de ello, el cliente establece la contraseña que será de uso exclusivo para futuros accesos al servicio.

A continuación los flujos del proceso de acceso a la aplicación del cliente Persona Natural.

- *Flujo del Proceso de Registro*



- *Flujo del Proceso de Acceso a la Aplicación BANCA On Line*



Es importante mencionar que las contraseñas de acceso al servicio *BANCA On Line* viajan de forma cifrada en SSL (del inglés Secure Sockets Layer) a 128 Bits y dentro de la red con encriptación 3DES.

- **Personas Jurídicas**

El esquema definido para que las personas autorizadas por los clientes Jurídicos (empresas o grupos económicos), puedan acceder y manejar las cuentas y demás productos que poseen en la Entidad Financiera ABC, por medio del servicio *BANCA On Line,* consiste en la entrega de un usuario generado en el módulo de

administración de la aplicación “Back Office” y la clave de acceso que utilizarán será compuesta por dos partes, una es el conjunto de dígitos que aleatoriamente y por cada sesenta (60) segundos despliega el dispositivo RSA SecurID, y la otra es una clave que define el usuario, las cual sólo él debe conocer, lográndose así lo que se denomina doble factor de autenticación para el acceso al Servicio *BANCA On Line.*

- *Proceso de asignación del dispositivo RSA SecurID al cliente*

1. El cliente se dirige a la oficina o es contactado por un ejecutivo de Banca de Empresa para solicitar la afiliación del servicio. Para ello, el cliente debe llenar los datos requeridos en la planilla de solicitud del servicio *BANCA On Line.*
2. El Ejecutivo de Cuenta en la Región o funcionario de la oficina envía un correo electrónico a la Gerencia De Banca Virtual, notificando la intención que tiene determinada empresa o grupo económico de solicitar acceso al servicio y por fax transmite los documentos exigidos para tal fin, al igual que copia de la solicitud.
3. Una vez que se determina la veracidad de los datos de la empresa, la Gerencia De Banca Virtual, extrae del stock de securID existentes en la bóveda de la unidad, el número del o los SecurID que serán asignados, dependiendo de la cantidad de usuarios autorizados para acceder al servicio.
4. La Gerencia De Banca Virtual solicita a la Gerencia De Seguridad de Información por medio de un requerimiento a Service Desk, que cree los usuarios requeridos en el módulo de administración “Back Office” y les asocie los SecurID en el sistema de autenticación, enviándole para ello una relación de usuarios y seriales de los SecurID a ser asignados. La Gerencia De Seguridad de Información, una vez concluida la actividad envía por el mismo medio que ya fue realizada dicha actividad.

5. La Gerencia De Banca Virtual envía por valija especial de valores los SecurID a la persona responsable de la Agencia de la Entidad Financiera o Ejecutivo de Cuenta en la región que atiende a la empresa solicitante del servicio.
6. Una vez que el funcionario de la agencia o ejecutivo de cuenta recibe los SecurID, este contacta a la empresa solicitante, le hace firmar la planilla de solicitud de afiliación al servicio y le entrega los securID.
7. El funcionario de la agencia envía la planilla de solicitud de afiliación firmada por el cliente y copia de los demás recaudos exigidos, a la Gerencia De Banca Virtual y ésta lo archiva generando un expediente particular por cada empresa o grupo económico.
8. La Gerencia De Banca Virtual solicita por Service Desk a la Gerencia De Seguridad de Información que active los SecurID.
9. La Gerencia De Seguridad de Información una vez recibida la confirmación del paso anterior, le envía a cada usuario autorizado por la empresa en la solicitud, un correo electrónico de confirmación con el usuario de acceso al servicio de BANCA On Line y la notificación de activación del dispositivo SecurID.

Es importante resaltar, que previo a la entrega del dispositivo al cliente, se realiza una sincronización de los dispositivos con el sistema de autenticación, y luego cuando se certifica la recepción del SecureID por parte del cliente, el mismo es activado. Por otro lado, en el momento de la autenticación, el servidor donde reside la aplicación BANCA On Line ejecuta un programa agente que sólo permite el acceso al servicio cuando el servidor de autenticación de RSA “ACE/SERVER” verifica que un usuario definido y su contraseña para un determinado instante coinciden, con la que este ha generado.

3. Descripción de la infraestructura tecnológica que soporta el Servicio de Banca Virtual

La infraestructura tecnológica que apoya al servicio de Baca Virtual se puede observar en la siguiente figura:

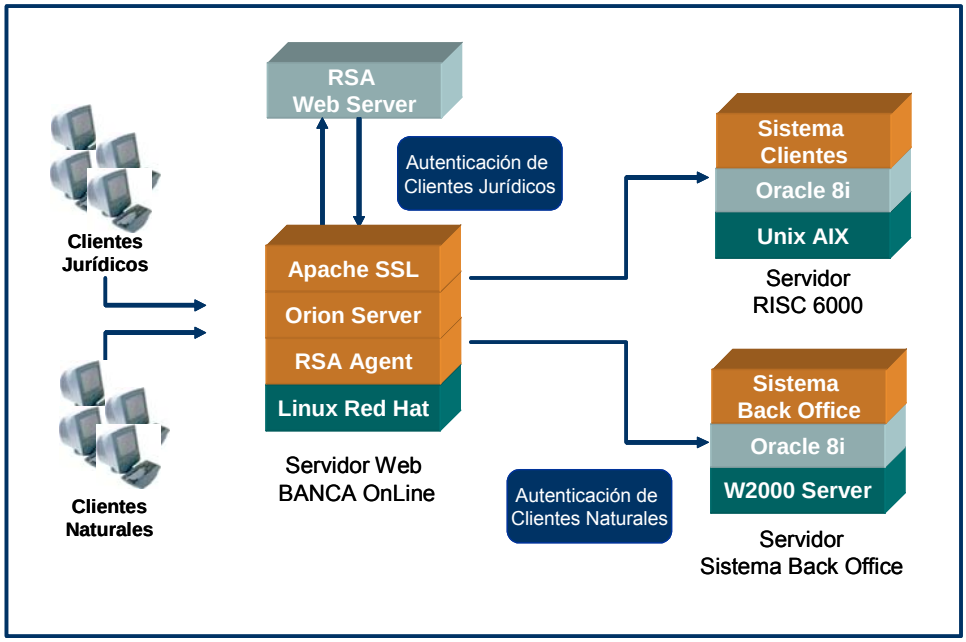


Figura 5. Infraestructura tecnológica del servicio BANCA On Line

- **Servidor Web**
  - Nombre: Webprod1
  - Sistema Operativo: Linux Red Hat
  - Aplicaciones: Apache, Orion y RSA Agent
  - Descripción: Servidor Web, el cual se encuentra instalado en una Zona Desmilitarizada DMZ (por sus siglas en inglés) y gestiona la conexión hacia el resto de los sistemas requeridos tanto para la autenticación de los usuarios como para la gestión de la información de los clientes (Tipos de cuentas, monto, etc.) y sus operaciones.

- **Servidor Sistema Back Office**
  - Nombre: Boprod2
  - Sistema Operativo: Windows 2000
  - Aplicaciones: Sistema Back Office
  - Descripción: Este servidor apoya a la aplicación Back Office, la cual contiene la información tanto de los clientes naturales como jurídicos para su autenticación al servicio BANCA On Line.

- **Servidor RISC 6000**
  - Nombre: Riscprod1
  - Sistema Operativo: Unix AIX
  - Aplicaciones: Sistema Clientes
  - Descripción: Este servidor apoya a la aplicación Sistema Clientes, la cual contiene toda la información bancaria de los clientes y sus productos asociados.

Basados en la figura 5, se puede explicar el flujo de la transferencia de información para la autenticación de los clientes jurídicos y naturales:

- **Autenticación Clientes Jurídicos**

A continuación se detalla el proceso de comunicación durante el proceso de autenticación de los usuarios jurídicos, el cual se puede resumir en las siguientes operaciones:

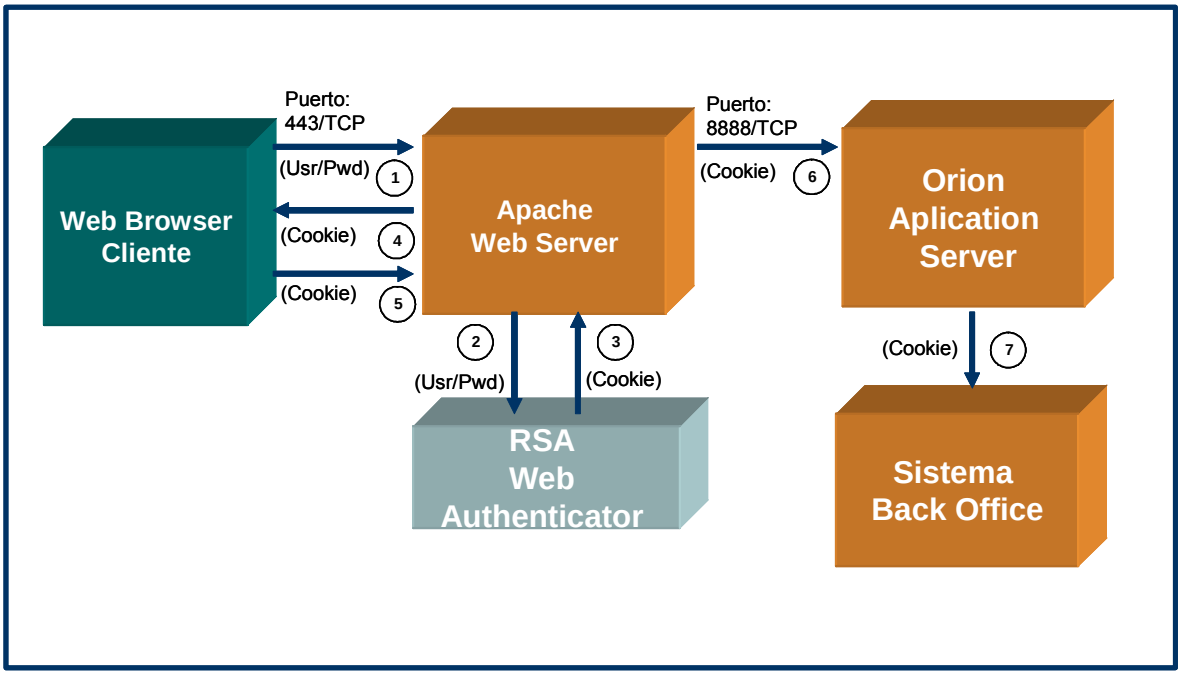


Figura 6. Proceso de autenticación de los clientes jurídicos

1. El usuario envía su usuario y contraseñas dinámica y estática por el puerto 443 (https) al servidor Apache. Este tráfico se encuentra cifrado.
2. El servidor Apache canaliza la autenticación con el Web Authenticator
3. El Web Authenticator genera un “cookie” de autenticación si la misma es exitosa.
4. El “cookie” es enviado al cliente.
5. El cliente envía el “cookie” de autenticación al servidor Apache.
6. El servidor Apache reenvía este “cookie” en texto claro por el puerto 8888 al servicio “Orion”.
7. El servidor “Orion” entrega el “cookie” a la aplicación Back Office, la cual valida el cookie.

- **Autenticación Clientes Naturales**

Los clientes naturales se autentican al sistema BANCA On Line introduciendo el número de la tarjeta de débito (TDD) y una clave, la cual es validada en el Sistema BackOffice. El proceso se detalla en la Figura 7 y la descripción de las operaciones efectuadas es la siguiente:

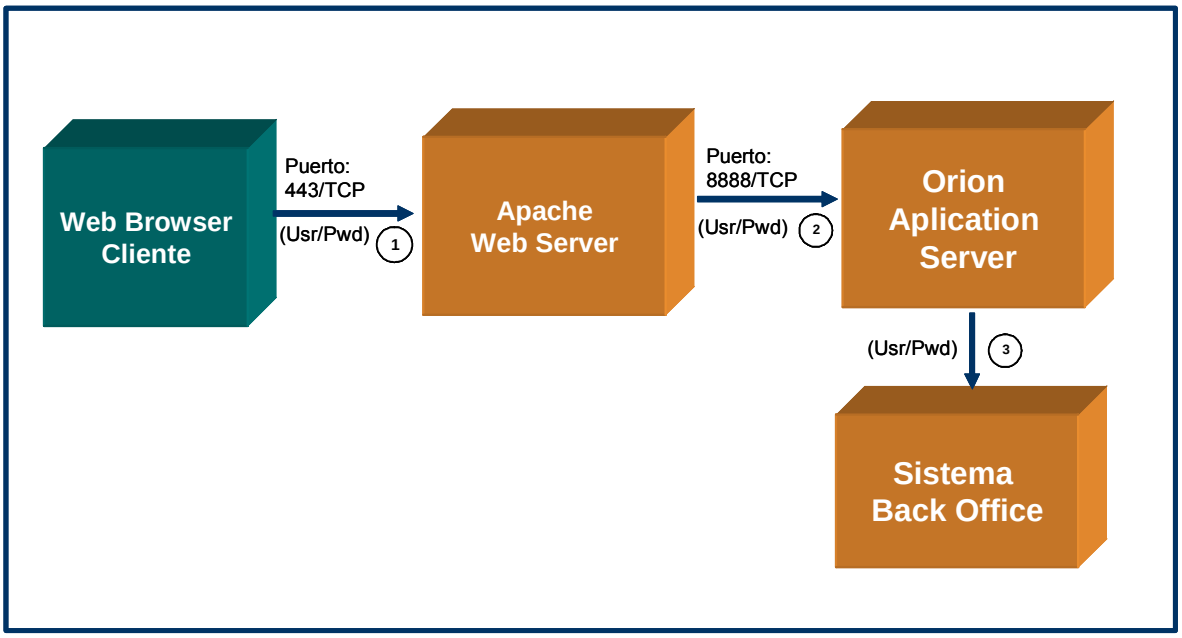


Figura 7. Proceso de autenticación de los clientes naturales

1. El usuario envía su número de TDD y contraseña por el puerto 443 (https) al servidor Apache. Este tráfico se encuentra cifrado.
2. El servidor Apache reenvía la información sin cifrar al puerto 8888 del servicio “Orion” en el mismo servidor.
3. “Orion” envía estos datos a la aplicación Back Office para que procese la autenticación.

4. Evaluación y diagnóstico de Seguridad de Información de la plataforma tecnológica que soporta al sistema BANCA On Line

Los objetivos de evaluación de Seguridad de Información de la plataforma Banca Virtual de la Entidad Financiera ABC, se orientaron a la identificación y evaluación de los controles de seguridad definidos en el sistema BANCA On Line. A los fines de cumplir con este objetivo, los procesos realizados fueron los siguientes:

- Revisión de los controles generales de cómputo.
- Evaluación del esquema y controles de seguridad implantados a nivel del sistema operativo Linux del servidor “Webprod1”, donde residen los componentes principales del servicio BANCA On Line.
- Evaluación de la configuración y controles de seguridad implantados en el servidor web “Apache” del servidor “Webprod1”.
- Evaluación de la configuración y controles de seguridad implantados en el servidor de aplicaciones “Orion” del servidor “Webprod1”.
- Revisión del esquema y controles de seguridad implantados a nivel del sistema operativo Windows 2000 del servidor “Boprod2”, donde reside la base de datos y la aplicación Back Office.
- Revisión del esquema y controles de seguridad implantados a nivel de la base de datos Oracle de la aplicación Back Office.

Los resultados de la evaluación y diagnóstico de los componentes de la infraestructura tecnológica de la Entidad Financiera ABC que soportan el servicio de BANCA On Line, se presentan a continuación en tablas de resultados que contienen la siguiente información:

- Situación identificada
- Riesgo
- Nivel de riesgo

Es importante mencionar que para el desarrollo de la evaluación no se utilizaron herramientas automatizadas por requerimiento de la Entidad Financiera ABC, en su defecto se utilizaron comandos e instrucciones propias por cada ambiente revisado. Los resultados de la evaluación se presentan a continuación.

Tabla 1. Evaluación de Seguridad: Controles generales de la plataforma Banca Virtual

Nro	Situación Identificada	Nivel de riesgo	Riesgo
Esquemas de contingencia			
1	Aún cuando existen mecanismos de control que permiten solventar eventos de bajo impacto, como por ejemplo un esquema de respaldos para la plataforma de Banca Virtual, la Entidad Financiera ABC, no tiene documentado un plan a seguir que permita proveer la continuidad y recuperación de sus operaciones y servicios, ante la ocurrencia de siniestros o accidentes graves que puedan afectar los principales equipos e instalaciones que conforman el ambiente de producción.	**A**	La situación antes planteada trae como consecuencia, que en caso de presentarse un siniestro se dificulte la realización de una coordinación eficaz en los pasos a seguir para restablecer los procesos operativos en función al evento presentado, requiriendo improvisar soluciones que pudieran entorpecer o retrasar la reanudación de las operaciones del negocio o inclusive la paralización total de las mismas, lo cual puede redundar en pérdidas financieras y de imagen para la Entidad.
Respaldo y recuperación			
2	Actualmente la Entidad Financiera ABC contempla dentro de sus procesos operativos la realización de respaldos, sin embargo, se detectaron las siguientes situaciones: - El procedimiento de respaldo y restauración de la información no se encuentra formalmente documentado. - No se realizan pruebas periódicas de restauración de la información a partir de las cintas de respaldo.	**M**	El hecho de no contar con controles adecuados y procedimientos debidamente documentados y actualizados para el proceso de respaldos, puede dificultar la recuperación de la información en caso que se produzcan fallas en el sistema y que requiera hacer uso de las cintas que almacenan la información respaldada. Por otra parte, la existencia de la documentación, reduce la dependencia del personal encargado de realizar estas actividades.
Control de Cambio			
3	Actualmente la Entidad cuenta con información general a ser tomada en cuenta en la gestión de control de cambios, sin embargo, no se ha desarrollado un procedimiento formal que abarque la incorporación de nuevas funcionalidades y mantenimiento de los programas en la plataforma de Banca Virtual.	**M**	La carencia de documentación de políticas y procedimientos para el control de cambios, incrementa el riesgo de que los mismos se realicen sin tomar en consideración el impacto que pueda tener para el negocio o se efectúen a criterio del personal a cargo del área de informática. Asimismo, no asegura la correcta documentación y seguimiento a los cambios, dificultando la solución de problemas en caso de presentarse fallas operativas o de seguridad.

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td colspan="4">Control de acceso</td></tr>
<tr><td>4</td><td>En los archivos de configuración del servidor “Orion” en los cuales se definen los usuarios y contraseñas de acceso a las bases de datos de los sistemas “Back Office” y “Clientes”, se evidenció que dicha información se encuentra en texto claro y además las contraseñas son secuencias de dígitos de fácil deducción.

Es importante resaltar que los directorios y archivos en los cuales se encuentran la configuración de la aplicación poseen privilegios de acceso inadecuados, brindando la posibilidad a todos los usuarios del servidor “Webprod1” a leer y ejecutar el archivo en donde se encuentran almacenadas las contraseñas de conexión a las bases de datos de los sistemas “Clientes” y “Back Office”. Los archivos bajo la situación descrita se muestran a continuación:

<table><tr><th>Archivo</th><th>Privilegios</th></tr><tr><td>/usr/orion/applications/backoffice</td><td>rwxr-xr-x</td></tr><tr><td>/usr/orion/applications</td><td>rwxrwxr-x</td></tr><tr><td>/usr/orion/config</td><td>rwxrwxr-x</td></tr></table></td><td>A</td><td>Esta situación incrementa el riesgo que información confidencial de los clientes del Banco se vea comprometida.</td></tr>
<tr><td>5</td><td>Los controles sobre las contraseñas de acceso al de Banca Virtual para persona natural, presentan funcionalidades que pudieran ser optimizadas:

- Aunque la contraseña del sistema BANCA On Line es independiente al resto de los canales de atención al cliente, la longitud de la clave de acceso al sistema es de cuatro (4) dígitos, y ésta sólo admite en su construcción caracteres numéricos.

- Las contraseñas de los clientes naturales del sistema Banca Virtual no tienen definido tiempo de caducidad, lo cual permite la permanencia de una misma clave de acceso durante un período indefinido.</td><td>M</td><td>Las situaciones antes planteada podrían traer diversas consecuencias, las cuales se detallan a continuación:

- El hecho de que la clave de acceso al sistema de BANCA On Line sea de cuatro (4) digitos, facilita la identificación de los datos de acceso por parte de terceros y la obtención de accesos no autorizados al sistema, lo cual se traduce en una pérdida de privacidad de la información financiera del cliente.

- El que las claves de los clientes naturales no tenga configurado tiempo de caducidad, podría traer como consecuencia la pérdida de confidencialidad de la contraseña, facilitando en caso de que se obtuvieran</td></tr>
</table>

Nro	Situación Identificada	Nivel de riesgo	Riesgo
	- No se cuenta con una funcionalidad para el cambio de claves, así como una facilidad que le permita al usuario recordar la contraseña de su cuenta si la misma ha sido olvidada.		el resto de los datos requeridos para el acceso a BANCA On-Line por parte de las personas naturales, un posible acceso irrestricto a información confidencial, como estados de cuenta, transacciones efectuadas, entre otras. - El hecho de que el sistema no presente una opción para el cambio de contraseña en caso de olvido, trae como consecuencia un aumento en las actividades planificadas para el personal del Centro de Atención Telefónica, ya que en ambos casos el usuario deberá notificar la situación con el fin de que le sea eliminada la cuenta y realizar nuevamente el proceso de registro, además podría generar incomodidad entre los clientes y el incremento en la oportunidad del personal del centro de atención telefónica en la incursión de operaciones fraudulentas, traduciéndose en un impacto negativo en el uso del sistema BANCA On-Line.
6	Se carece de un mecanismo de control para evitar el inicio de sesiones simultáneas a la aplicación de Banca Virtual, permitiendo de esta manera la posibilidad que los clientes puedan establecer dos (2), o más sesiones en el sistema con el mismo perfil de usuario.	**M**	Dicha situación hace posible que un tercero pueda obtener información confidencial referente a saldos bancarios de todas las cuentas asociadas a la tarjeta de débito del cliente, lo cual pone en riesgo la integridad personal del mismo como consecuencia de haberse revelado información que podría ser utilizada en contra de sus intereses.
Auditoría			
7	Se evidenció la carencia de políticas, procedimientos y herramientas de monitoreo de los eventos de seguridad del servicio BANCA On Line	**A**	El no contar con un procedimiento formal que norme las acciones a seguir en el ambiente del servicio BANCA On Line para verificar los registros de auditoría, dificulta aplicar acciones preventivas que permitan actuar oportunamente ante irregularidades y así disminuir los

Nro	Situación Identificada	Nivel de riesgo	Riesgo
			riesgos de accesos inadecuados y manipulación, revelación y/o destrucción de datos.
Manejo de errores			
8	No se están manejando adecuadamente los eventos de borde o validación de errores en la aplicación, ya que luego de realizar varias suscripciones fallidas en el módulo de Banca Personal, BANCA On Line emite un error de código e inmediatamente se cierra la aplicación.	**B**	Esta situación evidencia un problema de programación de la aplicación de Banca Virtual y una gestión inapropiada de los errores a presentar a los usuarios, lo cual puede repercutir en desconfianza de los clientes sobre el servicio prestado a través de este canal, y divulgación sobre detalles en el desarrollo de la aplicación.

Tabla 2. Evaluación de Seguridad: Sistema Operativo Linux Red Hat del servidor "Webprod1"

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td colspan="4">Políticas de contraseñas</td></tr>
<tr><td>9</td><td>Los parámetros de control de contraseñas de usuario presentan valores que pudieran ser optimizados:
<table>
<tr><th>Parámetro</th><th>Descripción</th><th>Valor Actual</th></tr>
<tr><td>PASS_MAX_DAYS</td><td>Permite definir la duración máxima de días de la contraseña.</td><td>99999</td></tr>
<tr><td>PASS_MIN_LEN</td><td>Permite definir la longitud mínima de la contraseña.</td><td>5</td></tr>
<tr><td>INACTIVE</td><td>Permite configurar el número de días en que una cuenta puede estar en desuso antes de ser deshabilitada.</td><td>-1</td></tr>
</table></td><td>A</td><td>La situación antes planteada podría traer diversas consecuencias, las cuales se detallan a continuación:

- La no caducidad de contraseñas de usuarios, incrementa la posibilidad de que las mismas pierdan su confidencialidad debido al tiempo que pueden permanecer sin cambiarse, lo cual puede generar accesos no autorizados en caso que las contraseñas asociadas a estas cuentas puedan ser descifradas o conocidas por personas no pertenecientes a la comunidad de usuarios.

- El hecho de que la longitud mínima de caracteres requeridos para las contraseñas esté definido en un</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td></td><td></td><td></td><td>valor de cinco (5) facilita la identificación de los datos de acceso por parte de terceros y la obtención de accesos no autorizados al sistema, lo cual se traduce en una pérdida de privacidad de la información financiera del cliente.

- La no configuración del tiempo de inactividad de una cuenta, brinda la posibilidad de que cuentas en desuso se mantengan activas, incrementando el riesgo de que personas con conocimientos de las contraseñas de las cuentas habilitadas, puedan obtener accesos no autorizados a información del Banco.</td></tr>
<tr><td colspan="4">Administración de usuarios</td></tr>
<tr><td>10</td><td>La seguridad relacionada con el control de acceso al servidor “Webprod1” debe contemplar una adecuada administración de usuarios en la plataforma tecnológica de la Entidad, a fin de minimizar las posibles brechas de accesos no autorizados. En tal sentido, se detectaron las siguientes situaciones:

- Existen cuentas de usuarios que no han establecido sesión con el servidor por más de treinta (30) días. Los usuarios bajo la situación descrita, se muestran a continuación:

<table><tr><th>Usuario</th><th>Ultima fecha que inició sesión</th></tr><tr><td>Soporte</td><td>30/11/2003</td></tr><tr><td>ftp</td><td>02/01/2004</td></tr></table>
- Existen perfiles de usuario que son utilizados como cuentas genéricas. Los casos identificados se presentan en la siguiente tabla:</td><td>M</td><td>Las situaciones antes planteadas podrían traer diversas consecuencias, las cuales se detallan a continuación:

- El hecho de que existan cuentas en desuso podría ocasionar que se produzcan accesos no autorizados en el sistema, al descifrar las contraseñas de algunas de estas cuentas, sin que esta situación sea advertida de manera oportuna por el personal encargado de administrar los accesos en este ambiente.

- La existencia de cuentas genéricas o perfiles utilizados por más de un usuario, implica que la clave pierda su privacidad y se torne pública, pudiendo ser utilizada por posibles intrusos para ingresar a la red y efectuar actividades en contra de los intereses del Banco. Asimismo, esta situación dificulta que puedan establecerse responsabilidades sobre operaciones inadecuadas.</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td></td><td><table><tr><th>Cuentas Genéricas</th><th>Usuarios</th></tr><tr><td>Security</td><td>Personal del área de Seguridad de Información</td></tr><tr><td>Operador</td><td>7 Operadores</td></tr><tr><td>Soporte</td><td>Administrador</td></tr></table></td><td></td><td></td></tr>
<tr><td colspan="4">Privilegios de acceso</td></tr>
<tr><td>11</td><td>El usuario “operador” puede iniciar sesión en el servidor evaluado mediante el shell (/bin/bash).

El shell “bash” permite a los usuarios la ejecución de funciones privilegiadas tales como, trasladarse a otros directorios, ejecutar comandos en directorios diferentes al propio, cambiar el valor de la variable “PATH”, entre otros.</td><td>M</td><td>Esta situación facilita a un atacante que obtenga acceso a algunas de estas cuentas, intentar elevar sus privilegios dentro del sistema mediante la ejecución de comando y la búsqueda de vulnerabilidades de seguridad o fallas del sistema (exploits).</td></tr>
<tr><td>12</td><td>Se detectó que el valor por defecto del parámetro “umask” es “022”, lo cual permite que la totalidad de los usuarios puedan leer y ejecutar todos aquellos archivos creados por los usuarios, a los cuales no se les haya cambiado de forma manual los privilegios de acceso.

El valor “umask” define la reducción de privilegios de acceso que se aplicará sobre los archivos creados por los usuarios. De este modo, cuando un usuario crea un archivo, el sistema operativo asigna por defecto los privilegios de acceso producto de la diferencia del valor de la permisología máxima (“rwxrwxrwx”) el cual es 777, menos el valor definido por el “umask”.</td><td>M</td><td>Esta situación puede ocasionar la pérdida de confidencialidad de archivos creados, así como también la disponibilidad de los mismos, ya que estos pueden ser eliminados, incrementando adicionalmente la posibilidad que puedan ser ejecutadas aplicaciones generadas por usuarios privilegiados cuyo “umask” no restrinja adecuadamente los permisos de lectura y ejecución a la totalidad de usuarios, lo cual representa un riesgo de manipulación o divulgación de información de forma no autorizada por parte de usuarios con acceso a la línea de comando</td></tr>
<tr><td>13</td><td>Existen archivos y directorios que poseen privilegios “world writable” o “group writable”, lo cual permite que la totalidad de los usuarios o aquellos que pertenezcan al grupo propietario, puedan alterar dichos archivos.</td><td>M</td><td>Las consecuencias de esta situación pueden ser muy variadas, desde la manipulación y pérdida de la confidencialidad e integridad de la información, hasta afectar la disponibilidad de la misma.</td></tr>
<tr><td>14</td><td>Actualmente todos los usuarios definidos en el servidor evaluado tienen la posibilidad de crear tareas programadas mediante los comandos “crontab” y “at” debido a la ausencia de los archivos de configuración que permiten restringir la utilización de dichos comandos.</td><td>M</td><td>Esta situación incrementa la posibilidad que usuarios autorizados al sistema, planifiquen la ejecución de programas maliciosos en contra de los intereses de la Entidad Financiera ABC o que personal no autorizado tenga acceso a información sensible que pudieran divulgar, dado que la ejecución de programas bajo este</td></tr>
</table>

Nro	Situación Identificada	Nivel de riesgo	Riesgo
	Los comandos de planificación, permiten ejecutar en momentos específicos comandos y programas, por lo cual la ejecución de estos comandos debe ser controlada. En este sentido, los archivos "cron.deny" y "at.deny", permiten agrupar aquellas cuentas de usuarios que no tienen capacidad para ejecutar el "cron", mientras que los archivos "cron.allow" y "at.allow" agrupan aquellas cuentas de usuario que si pueden ejecutar el comando "cron".		planificador es efectuada con atributos del usuario "root".
Auditoría			
15	No se están utilizando las facilidades de Linux para la generación y administración de registros de eventos de auditoría.	**M**	El no tener activas estas facilidades ni definidos los pasos a seguir para verificar los registros de auditoría del servidor, dificulta la detección de actividades inusuales que se produzcan en el ambiente, así como la aplicación oportuna de las acciones correctivas pertinentes.
Contraseñas de fácil deducción			
16	En el servidor "Webprod1" se identificaron que las cuentas "root" y "soporte" poseen contraseñas de fácil deducción. Las contraseñas de usuarios representan un elemento importante que contribuye a preservar la integridad y privacidad de los activos de información de la Entidad Financiera ABC. En tal sentido, la definición de las mismas debería estar enmarcada bajo criterios que permitan producir claves con características robustas. Cabe destacar, que la estructura de las contraseñas triviales, generalmente está basada en patrones de fácil de deducción, como por ejemplo: - Contraseñas iguales a los perfiles de usuarios, o iguales a los perfiles más un prefijo o sufijo básico. - Palabras triviales o comunes al entorno, como por ejemplo: Entidad Financiera ABC, Banca, Puerto Ordaz, etc.; nombres propios, objetos, etc. - Contraseñas cortas y constituidas sólo por caracteres numéricos o alfanuméricos. - Contraseñas con secuencias comunes del teclado.	**A**	La ausencia de mecanismos para la creación de contraseñas robustas facilita su identificación, permitiendo el ingreso al sistema y a sus recursos por parte de personas no autorizadas.

Tabla 3. Evaluación de Seguridad: Sistema Operativo Windows 2000 del servidor "Boprod2"

Nro	Situación Identificada	Nivel de riesgo	Riesgo
Políticas de contraseñas			
17	En la revisión de las políticas de cuentas definidas para el control de acceso al servidor, se determinaron las siguientes situaciones: - La propiedad de bloqueo de la cuenta de usuario y el contador de reinicialización del contador de intentos fallidos, se encuentran definidos en noventa (90) minutos, considerándose como un valor no óptimo. - Las contraseñas de los usuarios no caducan. - La duración mínima de contraseña tiene asignado el valor cero (0).	**B**	Las situaciones antes planteadas podrían traer diversas consecuencias, las cuales se detallan a continuación: - El hecho de que la propiedad de bloqueo de la cuenta de usuario y el contador de reinicialización del contador de intentos fallidos, se encuentran definidos en noventa (90) minutos, permite que usuarios no autorizados intenten en reiteradas oportunidades adivinar la contraseña de un usuario válido y ganar acceso al sistema. - Los cambios poco frecuentes de contraseñas facilitan la identificación de las mismas por personas no autorizadas, incrementando la posibilidad de que se produzcan accesos indebidos que puedan comprometer la confidencialidad de la información y la continuidad de las operaciones. - El hecho de que la duración mínima de la contraseña se encuentre configurado con valor cero (0), permite que los usuarios puedan cambiar la contraseña inmediatamente después de haber sido definida, y realizar un ciclo de contraseñas en un período corto, hasta que sus contraseñas originales se eliminen de la lista del historial, saltando por tanto el control de seguridad establecido por el parámetro "Historia de Contraseña".

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td colspan="4">Administración de usuarios</td></tr>
<tr><td>18</td><td>La seguridad relacionada con el control de acceso al servidor “Boprod2” debe contemplar no sólo la asignación de parámetros de configuración de cuentas adecuados, sino también una adecuada administración de usuarios en la plataforma tecnológica, lo cual minimiza las posibles brechas contra accesos no autorizados. En tal sentido, se detectaron las siguientes situaciones:

- El grupo “Domain Users” tiene acceso local a este servidor. Es importante resaltar que en este grupo se encuentran cuentas en desuso, las cuales se muestran a continuación:

<table><tr><th>Cuentas en desuso</th></tr><tr><td>Auditor01</td></tr><tr><td>Auditor02</td></tr><tr><td>Auditor03</td></tr><tr><td>auditor04</td></tr></table>
- Existen usuarios que pertenecen al grupo “Administrator”, los cuales por sus funciones dentro de la Compañía no deberían poseer tales privilegios administrativos. Los casos identificados se presentan en la siguiente tabla:

<table><tr><th>Cuentas con privilegios administrativos</th></tr><tr><td>asesor.asi03</td></tr><tr><td>luis.garcia</td></tr></table></td><td>A</td><td>Las situaciones antes planteadas podrían traer diversas consecuencias, las cuales se detallan a continuación:

- El hecho de que se le otorgue acceso al grupo “Domain Users” a este servidor, puede generar inconvenientes asociados a la existencia de perfiles inactivos, lo cual puede ocasionar que personas con conocimientos de las contraseñas de las cuentas habilitadas, puedan obtener accesos no autorizados a información de la Compañía

- La segregación inadecuada de las funciones de los usuarios, incrementa la posibilidad de que no se disponga de algún control efectivo para la verificación sobre las acciones realizadas en la red.</td></tr>
<tr><td>19</td><td>La cuenta “Administrator” creada automáticamente por el sistema operativo Windows 2000 al momento de su instalación, no ha sido renombrada.</td><td>M</td><td>Este estándar es conocido públicamente, por lo cual una de las primeras acciones de las personas que desean obtener acceso no autorizado a los sistemas, es realizar ataques e intentos de acceso con estos perfiles, ante la certeza de que “Administrator” es un usuario válido en este servidor.</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td colspan="4">Auditoría</td></tr>
<tr><td>20</td><td>Las políticas de auditoría facilitan el seguimiento de las actividades realizadas por los usuarios y del comportamiento del sistema en general. En tal sentido, se observó que en el servidor evaluado existen algunas políticas de auditoría que no se encuentran configuradas según las mejores prácticas de seguridad. Asimismo, no se cuenta con un procedimiento para la revisión periódica de los eventos ocurridos en el equipo evaluado por parte de la unidad responsable de los procedimientos de control de la tecnología de información de la Entidad Financiera ABC. En tal sentido, se detectaron las siguientes situaciones:

- Existen eventos que no están siendo auditados, lo cual puede traer como consecuencia que no se identifiquen oportunamente ciertas actividades inusuales en los servidores. A continuación se presenta las opciones de auditoría que no están configuradas:

<table><tr><th>Eventos\Servidor “Boprod2”</th></tr><tr><th>Eventos no auditados</th></tr><tr><td>Audit account management</td></tr><tr><td>Audit directory service access</td></tr><tr><td>Audit object access</td></tr><tr><td>Audit policy change</td></tr><tr><td>Audit privilege use</td></tr><tr><td>Audit process tracking</td></tr><tr><td>Audit system events</td></tr></table>
- Los cambios ocurridos en directorios o archivos críticos como “Winnt” y “System32”, así como las modificaciones realizadas en el registro del sistema (“registry”) a las entradas “HKEY_LOCAL_MACHINE\System” y “HKEY_LOCAL_MACHINE\Software”, no están siendo auditadas, situaciones ambas que representan la imposibilidad de hacer seguimiento a las manipulaciones en la configuración del sistema operativo.</td><td>B</td><td>Es importante mencionar, que la activación de las políticas de auditoría incluyendo la totalidad de eventos, facilitaría el proceso de monitoreo y detección de situaciones irregulares en el servidor. Asimismo, el registro de auditoría proporcionaría evidencias para ser utilizadas en la toma de acciones contra en caso que ocurra algún evento que afecte la operatividad del sistema.</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td></td><td>- Los parámetros de configuración del utilitario “Event Viewer” presentan características que impiden el adecuado registro de los eventos del sistema, ya que permite la eliminación anticipada de los eventos del sistema, limitando la oportunidad de hacer seguimiento a situaciones ocurridas con antelación a siete (7) días. A continuación se presenta la situación actual:
<table>
<tr><th colspan="3">Configuración del “Event Viewer”</th></tr>
<tr><th>Logs</th><th>Tamaño</th><th>Sobreescribir</th></tr>
<tr><td>Security</td><td>512Kbytes</td><td>7 days</td></tr>
<tr><td>System</td><td>512Kbytes</td><td>7 days</td></tr>
<tr><td>Aplication</td><td>512Kbytes</td><td>7 days</td></tr>
</table></td><td></td><td></td></tr>
<tr><td colspan="4">Servicios</td></tr>
<tr><td>21</td><td>Se identificaron debilidades relacionadas a servicios activos, las cuales se describen a continuación:

- Se encuentran activos los servicios de mensajería (Messenger y Alerter).
- Se evidenció la presencia del servicio NetBIOS, el cual provee información importante sobre el ambiente evaluado.</td><td>B</td><td>Las situaciones antes planteadas podrían traer diversas consecuencias, las cuales se detallan a continuación:

- El hecho de que se encuentren activos los servicios de mensajería permite a los usuarios comunicarse a través de las facilidades del comando de Windows 2000 “NET SEND”. Sin embargo, estos servicios no están siendo utilizado en el servidor, y además de consumir recursos de memoria, presenta algunas brechas de seguridad que podrían permitir entre otros, el ingreso de virus en la red.

- El hecho de tener activo el servicio NetBIOS podría traer como consecuencia que algún usuario malicioso pudiera utilizar esta información para atentar contra la seguridad de los activos de información de la Entidad Financiera.</td></tr>
</table>

Nro	Situación Identificada	Nivel de riesgo	Riesgo
Service Pack			
22	El "Service Pack" es un software desarrollado por Microsoft con la finalidad de distribuir las correcciones de aquellas fallas detectadas a la fecha en sus aplicaciones y sistemas operativos. Estos generalmente incluyen correcciones de fallas identificadas, componentes adicionales, nuevas características de seguridad, herramientas de administración del sistema, entre otros. En el servidor evaluado se encuentra desactualizado con respecto a los correctivos realizados al sistema operativo ya que tiene instalado el “Service Pack 3”, siendo actualmente el número cuatro (4) la última versión liberada por Microsoft para el sistema operativo Windows 2000.	**M**	El no tener una versión actualizada del "Service Pack" deja abierta la posibilidad que las brechas de seguridad que han sido detectadas sean aprovechadas por personal sin acceso al mencionado servidor, comprometiendo la seguridad y operatividad del mismo.
Registry			
23	No se ha restringido la conexión de servidores y estaciones de trabajo anónimas al dominio.	**M**	Esta situación podría originar el acceso no autorizado desde cualquier estación de trabajo anónima que no pertenezca a la red, y por tanto a información sensible almacenada en el servidor y/o en las estaciones de trabajo del dominio que no se encuentren adecuadamente protegidas, ya que esta propiedad permite la visualización de los miembros del dominio y los directorios compartidos.
24	El nombre de usuario de más reciente acceso a la red aparece en la caja de diálogo del próximo inicio de sesión en las estaciones de trabajo y servidores Windows 2000.	**M**	Es de hacer notar, que el hecho de presentar un nombre de usuario válido en el proceso de autenticación para el ingreso a la red, facilita accesos no autorizados, limitando el esfuerzo de búsqueda del atacante únicamente a la obtención de la contraseña.
25	El servidor no se oculta del resto de los computadores existentes en la red.	**M**	Esta situación implica que cualquier usuario con acceso a la red pudiera percatarse de la existencia de dicho servidor mediante el protocolo NetBIOS y por consiguiente, intentar ganar acceso no autorizado a los recursos definidos en dicho servidor.

Nro	Situación Identificada	Nivel de riesgo	Riesgo
26	No se presentan en tiempo de inicio de sesión las normativas de seguridad de activos de información.	**M**	El conocimiento y aceptación de las condiciones de uso de los activos de información por parte del usuario, debe incluir la presentación, previa al inicio de sesión, de las condiciones de uso en todos los computadores la Entidad Financiera ABC. Esta práctica permite informar al usuario sobre los aspectos legales relacionados a uso de los activos de información de la organización. De este modo, el usuario entra en conocimiento de dichas condiciones y, ante el incumplimiento de las mismas, pueden ser utilizadas como apoyo legal a sanciones o acciones posteriores.

Tabla 4. Evaluación de Seguridad: Base de Datos Oracle del Sistema Back Office – Servidor Boprod2

Nro	Situación Identificada	Nivel de riesgo	Riesgo
Auditoría			
27	El ambiente del sistema Back Office, consta de diferentes componentes tecnológicos que proveen la operatividad de dicho sistema. Cada uno de uno de estos componentes proporciona la habilitación de trazas de auditoría que permiten registrar los diferentes eventos que se produzcan en cada nivel. En este sentido, se evidenció que las facilidades de auditoría que posee el manejador de bases de datos Oracle no se encuentran activas.	**B**	Esta situación dificulta la obtención de información relacionadas a actividades sobre las tablas de la base de datos, los intentos de acceso a la misma, e incluso actividades asociadas a los distintos roles incluyendo el rol “DBA”, eventos que podrían pasar desapercibidos por el administrador, aumentando la probabilidad de que usuarios no autorizados pongan en riesgo la integridad y operatividad de la base de datos sin ser detectados.

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td colspan="4">Administración de usuarios</td></tr>
<tr><td>28</td><td>En la base de datos del sistema Back Office se observaron cuentas genéricas. Los casos identificados se presentan en la siguiente tabla:

<table><tr><th>Usuarios</th></tr><tr><td>Operadores</td></tr><tr><td>BackOffice</td></tr></table>
Adicionalmente, se evidenció que el usuario BackOffice es utilizado tanto por la aplicación BackOffice como por el administrador del ambiente, lo cual dificulta analizar la utilización de dicho perfil, al combinar las operaciones regulares con las actividades administrativas.</td><td>M</td><td>La existencia de cuentas genéricas trae como consecuencia que más de una persona pueda conocer su clave de acceso, perdiendo su privacidad, pudiendo ser utilizada por posibles intrusos para ingresar a la red y efectuar actividades en contra de los intereses de la Compañía. Asimismo, esta situación dificulta que las actividades realizadas por estas cuentas puedan ser adecuadamente auditadas y por consiguiente, no puedan establecerse responsabilidades sobre operaciones inadecuadas.</td></tr>
<tr><td>29</td><td>Todo ambiente Oracle provee un perfil de límite de recursos predeterminado denominado “Default”, y cuando se crea un usuario nuevo en la base de datos y no se le indica un perfil específico, Oracle automáticamente le asocia dicho perfil. El perfil “Default” especifica la configuración tanto para los recursos del sistema como para los recursos de contraseñas. La totalidad de los usuarios definidos en el manejador de base de datos instalado en el servidor Boprod2, tienen asignado el perfil “Default”, el cual posee todos los valores de recursos y administración de cuentas en forma ilimitada. En la siguiente tabla se presentan los parámetros asignados actualmente al perfil “Default”:

<table><tr><th>Parámetro</th><th>Descripción</th><th>Valor</th></tr><tr><td>COMPOSITE_LIMIT</td><td>Define la longitud de la contraseña y los caracteres, números y signos de puntuación que hay que utilizar al formar la contraseña</td><td>UNLIMITED</td></tr><tr><td>FAILED_LOGIN_ATTEMPTS</td><td>Cantidad de intentos fallidos de conexión antes de que la cuenta de usuario sea bloqueada.</td><td>UNLIMITED</td></tr></table></td><td>M</td><td>Aun cuando la mayoría de las cuentas definidas en el manejador de base de datos son creadas por defecto o son utilizadas para la aplicación de Banca Virtual, la configuración “UNLIMITED” en todos los parámetros del perfil “Default” arriba descritos no provee facilidades para la definición de restricciones en la administración del entorno, permitiendo situaciones de riesgo no requeridos.</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td></td><td>
<table>
<tr><td>SESSIONS_PER_USER</td><td>Número máximo de sesiones concurrentes por cada usuario de la base de datos.</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_LIFE_TIME</td><td>Tiempo (días) de vida de la contraseña.</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_REUSE_TIME</td><td>Tiempo (días) luego del cual puede reutilizarse una contraseña</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_REUSE_MAX</td><td>Cantidad de contraseñas distintas antes de volver a reutilizar alguna de ellas.</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_VERIFY_FUNCTION</td><td>Permite que se especifique un script para uso en la verificación de la fortaleza de una contraseña.</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_LOCK_TIME</td><td>Tiempo (días) en que una cuenta permanecerá bloqueada después de haber alcanzado el máximo número de intentos fallidos de sesión.</td><td>UNLIMITED</td></tr>
<tr><td>IDLE_TIME</td><td>Tiempo máximo (minutos) permitido de inactividad en la conexión de un usuario a una instancia</td><td>UNLIMITED</td></tr>
<tr><td>PASSWORD_GRACE_TIME</td><td>Tiempo de gracia (días) para cambiar la contraseña.</td><td>UNLIMITED</td></tr>
<tr><td>CONNECT_TIME</td><td>Tiempo de conexión por usuario a una instancia de base de datos.</td><td>UNLIMITED</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td colspan="4">Privilegios de acceso</td></tr>
<tr><td>30</td><td>Se evidenció que el rol “PUBLIC” tiene privilegios sobre algunas tablas críticas de la base de datos del sistema Back Office. En especial, a este rol se le ha asignado el privilegio de lectura a la vista “ALL_SOURCE”, la cual permite visualizar el código fuente presente en todos los triggers y procedimientos del sistema que son accesibles por el</td><td>M</td><td>El riesgo de esta situación radica en que los privilegios asignados a la cuenta “PUBLIC” aplican a todos los usuarios de la base de datos,</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Situación Identificada</th><th>Nivel de riesgo</th><th>Riesgo</th></tr>
<tr><td></td><td>usuario, donde se encuentra almacenada información importante del funcionamiento de los mismos.

A continuación se presentan los casos con la situación antes mencionada:

<table>
<tr><th>Cuenta</th><th>Tabla</th><th>Privilegio</th></tr>
<tr><td>PUBLIC</td><td>USER_JOBS</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_DEPENDENCIES</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_IDL_UB1</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_IDL_CHAR</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_IDL_UB2</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_IDL_SB4</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ORA_KGLR7_DB_LINKS</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>ALL_SOURCE</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE_USUARIOS_BP</td><td>ALTER</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>DELETE</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>INDEX</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>INSERT</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>SELECT</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>UPDATE</td></tr>
<tr><td>PUBLIC</td><td>BACKOFFICE _USUARIOS_BP</td><td>REFERENCES</td></tr>
</table>
</td><td></td><td>incrementando así la asignación inadecuada de privilegios sobre tablas críticas de la base de datos del Sistema Back Office.</td></tr>
</table>

CAPÍTULO V

ESTRATEGIA DE IMPLANTACIÓN

1. Propuesta de acción como alternativa de solución

Continuamente aparecen brechas de seguridad y se acrecienta el ingenio para identificarlas y utilizarlas por parte de personal no autorizado. Queda entonces claro que esperar la ocurrencia de fallas para proceder a corregirlas es precisamente en lo que se apoyan posibles intrusos para penetrar las redes. Por otro lado, pretender detectar las debilidades antes de que ocurran, puede ser una labor costosa en personal y tiempo.

El objetivo de este trabajo estuvo orientado a la identificación y análisis de riesgos en el ambiente tecnológico de la Entidad Financiera ABC, mediante la ejecución de un estudio de seguridad integral de la aplicación de Banca Virtual. En el Capitulo IV se presentaron los hallazgos de la evaluación realizada, los cuales fueron analizadas y discutida con el personal de administración y la directiva de la Institución. La propuesta de acción busca definir estrategias técnicas basadas en las mejores prácticas de seguridad, que solventarán las situaciones identificadas, sin incurrir en inversiones mayores.

En este sentido a continuación se detallan las recomendaciones generadas para cada aspecto identificado:

Tabla 5. Recomendaciones: Controles generales de la plataforma Banca Virtual

Nro	Resumen de la situación identificada	Recomendación
Esquema de contingencia		
1	No existe un plan de contingencia	Emprender las acciones necesarias para lograr el desarrollo, formalización y posterior prueba del referido plan, que pueda ser de utilidad ante eventualidades de diversas dimensiones, considerando la totalidad de recursos informáticos y tecnológicos del ambiente de Internet Banking y de ser posible integrarlo con el plan de continuidad del negocio desarrollado para todo el Banco. Asimismo, el procedimiento de contingencia debe estar orientado a responder todos los posibles niveles de interrupción en el servicio y su esquema debe contemplar en forma precisa cada uno de dichos niveles. En este sentido, algunas de las actividades que pueden ser tomadas en cuenta por la Entidad Financiera ABC, durante el desarrollo del plan de contingencia, son las siguientes: - Considerar la totalidad de los procesos que se encuentran operando en el(los) equipo(s) de producción, indicando para cada una de estos los tiempos mínimos de recuperación, así como su impacto financiero. - Considerar la totalidad de los componentes, incluyendo la plataforma de microcomputadores y los componentes de red y telecomunicaciones, así como los equipos periféricos, para lo cual es necesario determinar: • Unidades de respaldo, controladores de disco u otras interfaces, concentradores de red, UPS, equipos de soporte. • Información de los proveedores de cada uno de los equipos y contrato de mantenimiento a los mismos. - Determinación cuantificada del impacto al negocio de cada uno de los riesgos identificados, con el fin de asumir posiciones sobre cada uno de ellos. - Determinación y puesta en funcionamiento de un Centro Alterno, para una recuperación de datos en caso de contingencia, tomando en consideración los siguientes aspectos: • Tipo de Centro Alterno: Hot site, warm site o cold site. • Ubicación estratégica del Centro. • Facilidades para comunicaciones. • Espacios de almacenamiento, entre otros. - Definir y formalizar los equipos de trabajo, personal alterno y responsabilidades durante la ejecución

Nro	Resumen de la situación identificada	Recomendación
		del procedimiento de contingencias. Asimismo, el procedimiento debe incluir aspectos que abarquen acciones de logística, tales como: - Preparación de los proveedores de servicios ante la ocurrencia de una contingencia. El plan de contingencias debe cubrir la evaluación de los riesgos incurridos en la adquisición de un servicio dado por un tercero, considerando que el mismo no reaccione adecuadamente ante la ocurrencia de un siniestro. - Planificación y definición de responsabilidades en la actualización del plan de contingencias, así como políticas y procedimientos para la revisión y actualización permanente del plan.
Respaldo y Recuperación		
2	El procedimiento para la realización de respaldos debe ser mejorado	A fin de mitigar los inconvenientes asociados, se recomienda aplicar los correctivos necesarios a cada situación descrita, así como también, agilizar la documentación de los lineamientos necesarios para la realización de respaldos periódicos a los servidores, tomando en cuenta lo siguiente: - Responsables del proceso. - Tiempo de retención y rotación de cintas. - Tiempo de vida útil de las cintas. - Frecuencia y tipo de respaldo. - Lugar de almacenamiento de las cintas (tanto interno como externo). - Mantenimiento de las unidades de almacenamiento. - Rotación, reutilización y desincorporación de cartuchos, indicando el proceso de borrado y destrucción de los mismos. Adicionalmente, se recomienda planificar pruebas periódicas de restauración de información a partir de los respaldos realizados a fin de asegurar que el proceso funciona adecuadamente, y planificar pruebas en los servidores para intentar restaurar las copias de seguridad y asegurar que el proceso funciona adecuadamente.
Control de Cambio		
3	No existe un procedimiento formal para los cambios en los programas de la plataforma Banca Virtual	Agilizar los procesos de documentación y estandarización que permitan el adecuado manejo de los cambios a los sistemas o pases de programas, por lo cual se sugiere incluir los siguientes aspectos: - El requerimiento inicial debe estar en un formulario para la solicitud de cambios a los sistemas, el cual

Nro	Resumen de la situación identificada	Recomendación
		debe ser firmado y aprobado por los usuarios. - Evaluación del impacto de los cambios, para lo cual se deben identificar las áreas que podrían verse afectadas por los mismos. - Aprobación de los resultados de las pruebas por parte de los usuarios. - Documentación completa de todos los cambios a programas. - Restricción del acceso a los consultores / programadores a los recursos e información de producción. - Definición planes de ejecución para procesos de restauración de datos en caso de requerir versiones anteriores de programas o aplicaciones por motivo de falla o inconsistencias en el ambiente de producción. Asimismo, se recomienda informar sobre estos procedimientos a todos los departamentos y usuarios involucrados. Así como desarrollar y documentar procedimientos y controles para asegurar que se está llevando a cabo un plan de pruebas exhaustivo, que minimice el riesgo de fallas operativas en el ambiente de producción.
Control de acceso		
4	Existen archivos de configuración con la información de conexión a la base de datos en texto claro	Evaluar la posibilidad de cifrar la información de conexión a las bases de datos que sirven de apoyo al ambiente de Internet Banking. Entre los algoritmos de cifrado que pueden evaluarse para llevar a cabo esta recomendación se encuentran: - 3DES - AES - SkipJACK - IDEA
5	Los controles sobre las contraseñas de acceso al sistema Internet Banking para persona natural, presentan funcionalidades que pudieran ser optimizadas	Dentro de las recomendaciones a implantar están: - Evaluar la posibilidad de establecer que la contraseña esté compuesta por un mínimo de ocho (8) caracteres alfanuméricos. - Implantar un mecanismo automático que obligue al usuario a generar una nueva contraseña en un período máximo de aproximadamente noventa (90) días. Asímismo, se recomienda definir un historial de contraseñas (cinco contraseñas) para eliminar la posibilidad de que se definan iguales a las anteriores. - Desarrollar un esquema de pregunta confidencial, en el cual se le pedirá al usuario que escriba una pregunta que desea que le sea planteada en caso de que se le haya olvidado la contraseña y cuya respuesta servirá para recordar la contraseña empleada y será sólo conocida por éste.

Nro	Resumen de la situación identificada	Recomendación
		- Implementar una opción que pueda ser fácilmente accedida desde la página de autenticación que le permita al usuario la libertad de cambiar su contraseña en cualquier momento sin tener que recurrir a los servicios del Centro de Atención Telefónica ni tampoco tener que realizar nuevamente su suscripción al servicio.
6	Se carece de un mecanismo de control para evitar el inicio de sesiones simultáneas a la aplicación de Banca Virtual	Reforzar la seguridad de acceso al servicio "BANCA On-Line" evitando el establecimiento de conexiones simultáneas mediante un mismo perfil de usuario.
Auditoría		
7	Carencia de políticas, procedimientos y herramientas de monitoreo de los eventos de seguridad	Definir e implantar procedimientos y responsabilidades que normen la supervisión de los eventos ocurridos en el servicio de "BANCA On-Line", incluyendo como mínimo los siguientes aspectos: - Identificar el personal encargado de analizar los registros de auditoría en el sistema de "banca On-Line" y definir la frecuencia de revisión de los mismos. - Realizar un inventario de todos los posibles generadores de eventos en función a los componentes de servicio (Apache, Orion Server, Linux, Oracle, Windows 2000), así como también activar y configurar cada uno de ellos en función al nivel de detalle requerido para el monitoreo del ambiente. - Definir e implantar procedimientos de control, mantenimiento y seguimiento de los accesos al sistema, así como establecer procedimientos de revisión de los registros de auditoría. - Definir y documentar las revisiones periódicas de los registros de auditoría. - Definir el tipo de reportes a generar con el fin de apoyar las labores de auditoría sobre el sistema. Se sugiere que como mínimo se elaboren los siguientes reportes: • Reporte de las personas que se encuentren bloqueadas y/o suspendidas por más de tres (3) intentos de ingreso fallido, indicando el detalle de los campos en los que se ha incurrido en error, con el fin de determinar las actividades de posibles "hackers" o intrusos. • Reporte estadístico de los campos del formulario de suscripción en los que más se incurre en error, con el fin de determinar posibles fallas en el diseño o lógica del ingreso de los datos en el módulo de registro de clientes.

Nro	Resumen de la situación identificada	Recomendación
		• Reporte de casos fallidos de conexión en los que para números distintos de tarjetas de débito se repita la misma dirección IP, tambien con el fin de determinar las actividades de posibles "hackers" o intrusos en la fase de conexión. • Reporte general de casos fallidos de conexión. • Reporte que permita monitorear las actividades realizadas por el Centro de Atención Telefónica, indicando todos los eventos que un mismo funcionario realiza sobre un mismo cliente, con el fin de establecer patrones de comportamiento de los usuarios y operadores del sistema. Una vez definido el procedimiento para seguimiento de los registros de auditoría se recomienda formalizarlo e implantarlo.
Manejo de Errores		
8	No se están manejando adecuadamente los eventos de borde o validación de errores en la aplicación	Evaluar la posibilidad de diseñar pruebas de borde o validación de errores en "BANCA On-Line", con el fin de que dichos errores sean manejados a nivel de aplicación, y establecer prácticas en el desarrollo de las aplicaciones orientadas a gestionar errores irrecuperables o no controlados hacia esquemas internos de reporte, y mensajes generales al usuario que no aporten detalles sobre la programación de la aplicación.

Tabla 6. Recomendaciones: Sistema Operativo Linux Red Hat del servidor "Webprod1"

Nro	Resumen de la situación identificada	Recomendación
Esquema de contingencia		
9	Los parámetros de control de contraseñas de usuario presentan valores que pudieran ser optimizados	Modificar los valores de parámetros de configuración de cuentas de usuario, tomando en consideración lo que se detalla a continuación:

Archivo	Parámetro	Valor
/etc/default/logidefs	PASS_MIN_LEN	8
	PASS_MIN_DAYS	7
	PASS_MAX_DAYS	45
	PASS_MIN_DAYS	30
	INACTIVE	60
/etc/profile	TMOUT	900

Nro	Resumen de la situación identificada	Recomendación
Administración de usuarios		
10	La seguridad relacionada con el control de acceso al servidor “Webprod1” debe contemplar una adecuada administración de usuarios	- Implantar mecanismos de control para el diagnóstico y eliminación de aquellas cuentas que se encuentran inactivas. Asimismo, se recomienda realizar una revisión de las cuentas de usuario definidas, a fin de deshabilitar las cuentas en desuso o que son eventualmente utilizadas y eliminar aquellas que realmente no se requieran. - Evaluar la posibilidad de individualizar el uso de cuentas de usuarios para cada una de las personas que requieran obtener acceso. - Evaluar la posibilidad de eliminar los perfiles de usuario genéricos en caso de no ser actualmente requeridos.
Privilegios de acceso		
11	El usuario “operador” puede iniciar sesión en el servidor evaluado mediante el shell (/bin/bash).	Optimizar las restricciones del acceso al “shell” del servidor evaluado, a efectos que los usuarios que no requieran su uso no accedan a la línea de comandos del sistema operativo. Para ello es necesario tomar en cuenta las siguientes consideraciones: - Asignar la opción de “shell” restringido a aquellos usuarios que solo ameriten la ejecución de comandos específicos colocando “/bin/bash-r” como “shell” del usuario en el archivo “/etc/passwd”. Esto impide a los usuarios puedan realizar las siguientes acciones: • Trasladarse de su propio directorio (“home directory”), ya que el comando “cd” que permite cambiar el directorio actual, estaría desactivado. • Cambiar el valor de la variable “PATH”, de modo que podrán ejecutar comandos en el “PATH” que les proporciona el administrador del sistema. • Cambiar el valor de la variable “SHELL”. • Ejecutar comandos en directorios diferentes al directorio propio, ya que no pueden utilizar un nombre de comando que contenga un carácter “/”. • Redirigir la salida utilizando los operadores “>” o “>>”. • Utilizar comandos “exec” que permite la recepción de solicitudes para la ejecución de comandos en el servidor. Desarrollar un menú que contenga sólo las tareas que realizan los operadores e incorporar en el script principal el comando “trap "" 1 2 3”, a fin de evitar que el operador lo cancele e ingrese a la línea de comando**.**

<table>
<tr><th>Nro</th><th>Resumen de la situación identificada</th><th>Recomendación</th></tr>
<tr><td>12</td><td>Se detectó que el valor por defecto del parámetro “umask” es “022”</td><td>Elevar el valor “umask” a “027” a la totalidad de usuarios definidos en el servidor evaluado, modificando dicho valor en los archivos “.profile” globales y los referidos al usuario. Esto indicará al sistema que elimine todos los privilegios a “other” y elimine los privilegios de escritura al grupo.</td></tr>
<tr><td>13</td><td>Existen archivos y directorios que poseen privilegios “world writable” o “group writable”</td><td>Evitar accesos irrestrictos a los archivos y directorios del servidor a la totalidad de usuarios, utilizando para ello la práctica de identificar el uso de cada tipo de archivo y ajustarlo en la medida de lo posible dentro del esquema presentado a continuación:

<table><tr><th>Descripción</th><th>Privilegio de acceso</th></tr><tr><td>Directorios y programas ejecutables de acceso público</td><td>rwxr-xr-x</td></tr><tr><td>Directorios de trabajo de uso compartido para usuarios especializados (programadores o personal de operaciones)</td><td>rwxrwx---</td></tr><tr><td>Programas y directorios de uso común, en producción, sin acceso a la totalidad de los usuarios</td><td>rwxr-x---</td></tr><tr><td>Archivos de acceso público de sólo lectura</td><td>rw-r—r--</td></tr><tr><td>Archivos de uso exclusivo del sistema operativo</td><td>rw-------</td></tr></table>
Es importante indicar, que el cuadro presentado anteriormente no representa un esquema rígido, por lo cual debe considerarse como un modelo a seguir y ajustarlo con base a cada caso analizado.</td></tr>
<tr><td>14</td><td>Todos los usuarios definidos en el servidor evaluado tienen la posibilidad de crear tareas programadas mediante los comandos “crontab” y “at”</td><td>Definir en los archivos “cron.deny” y “at.deny” aquellos usuarios que no deberían tener privilegio para ejecutar los comandos de planificación, o por el contrario crear los archivos “cron.allow” y “at.allow”, y definir en ellos aquellos usuarios que tienen privilegios para ejecutar estos comandos sensitivos.</td></tr>
<tr><td colspan="3">Auditoría</td></tr>
<tr><td>15</td><td>No se están utilizando las facilidades de Linux para la generación y administración de registros de eventos de auditoría.</td><td>En función de detectar a tiempo todas aquellas acciones que eventualmente pudieran afectar la operatividad del ambiente se recomienda evaluar la posibilidad de implantar los servicios de auditoría del sistema. De igual modo, crear mecanismos que permitan monitorear los mensajes reportados por el sistema operativo. Dichos mecanismos deben garantizar que los “logs” de auditoría sean revisados regularmente, y preferiblemente de manera automática por medio de tareas programadas. En su defecto, se recomienda evaluar el uso de herramientas alternas que permitan hacer seguimiento de cierto tipo de eventos, como por ejemplo, intentos</td></tr>
</table>

Nro	Resumen de la situación identificada	Recomendación
		fallidos de acceso, modificación de privilegios de acceso sobre archivos sensibles, entre otros. Es importante resaltar que la generación de archivos de auditoría debe ser acompañado del desarrollo de procedimientos para el seguimiento de eventos, su respaldo y almacenamiento fuera de los equipos.
Contraseñas de fácil deducción		
16	En el servidor "Webprod1" se identificaron que las cuentas "root" y "soporte" poseen contraseñas de fácil deducción.	Divulgar criterios para el uso de contraseñas de difícil deducción por parte de terceros y fáciles de recordar por el usuario propietario, para ello pueden ser tomados en consideración los siguientes aspectos: - Emplear letras y números mezclando con caracteres especiales. Esto constituye un grado de complejidad aun mayor en la contraseña. - Buscar información relativa a los lineamientos a seguir en la asignación de contraseñas, en la siguiente dirección: http://www.alw.nih.gov/Security/first-papers.html. Link: "Department of Defense Password Management Guideline".

Tabla 7. Recomendaciones: Sistema Operativo Windows 2000 del servidor "Boprod2"

Nro	Resumen de la situación identificada	Recomendación
Políticas de contraseñas		
17	Existen políticas para el control de contraseñas que pudieran ser optimizadas	Optimizar la definición de las políticas de contraseñas, para ello es necesario tomar las siguientes consideraciones: - Activar el bloqueo de cuentas por intentos fallidos de conexión, en las políticas de cuenta, y asignar los siguientes valores: • Número de intentos fallidos: tres (3). • Contador de intentos fallidos: mil cuatrocientos cuarenta (1440) minutos (24 horas). - Tiempo de bloqueo: cuatro mil trescientos veinte (4320) minutos (72 horas) o hasta notificar al Administrador.

<table>
<tr><th>Nro</th><th>Resumen de la situación identificada</th><th>Recomendación</th></tr>
<tr><td></td><td></td><td>- Definir que la rotación de las contraseñas sea requerida y de carácter obligatorio, con un período no mayor a cuarenta y cinco (45) días.

- Definir el control histórico de la contraseña en un valor de diez (10), para evitar que puedan ser reutilizadas las últimas diez (10) contraseñas.

- Limitar el lapso mínimo para el cambio de la contraseña en catorce (14) días.</td></tr>
<tr><td colspan="3">Administración de usuarios</td></tr>
<tr><td>18</td><td>Se identificaron diversas situaciones relacionadas con una inadecuada administración de usuarios</td><td>- Revisar la asignación de los grupos que tienen acceso al servidor, con el fin de restringir sólo a aquellos usuarios que así lo ameriten.

- Establecer un seguimiento adecuado a las cuentas de usuarios finales con altos privilegios administrativos a efecto de mantener una segregación de funciones apropiada. En caso de que existan excepciones, se recomienda documentarlo.</td></tr>
<tr><td>19</td><td>La cuenta “Administrator” no ha sido renombrada</td><td>Tomando en cuenta que el ambiente Windows ofrece la posibilidad de cambiar el nombre a cualquier usuario sin tener que eliminarlo y volverlo a definir, se recomienda renombrar la cuenta de usuario antes mencionada, utilizando nombres difíciles de relacionar por terceros y asignarles contraseñas robustas. Asimismo, se recomienda definir una cuenta de usuario con permisos limitados, con el nombre de “Administrator” como un señuelo, a fin de detectar si existen usuarios intentando ganar acceso al sistema utilizando este perfil.</td></tr>
<tr><td colspan="3">Auditoría</td></tr>
<tr><td>20</td><td>Existen algunas políticas de auditoría que no se encuentran configuradas</td><td>En función de optimizar, acorde a las mejores prácticas, la configuración de las facilidades de auditoría en los servidores evaluados, se recomienda:

- Configurar los eventos de auditoría desde la opción “Audit Policies” del utilitario “User Manager for Domains”, de la siguiente manera:

<table>
<tr><th>Eventos a auditar</th><th>Exitos</th><th>Fallas</th></tr>
<tr><td>Audit account management</td><td>✓</td><td>✓</td></tr>
<tr><td>Audit object access</td><td></td><td>✓</td></tr>
<tr><td>Audit policy change</td><td>✓</td><td>✓</td></tr>
<tr><td>Audit privilege use</td><td>✓</td><td>✓</td></tr>
<tr><td>Audit system events</td><td>✓</td><td>✓</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nro</th><th>Resumen de la situación identificada</th><th>Recomendación</th></tr>
<tr><td></td><td></td><td>

Configurar la auditoría de los directorios y archivos críticos del sistema operativo y aplicaciones, mediante la visualización de propiedades en la pestaña “Security” presionando el botón “Advance”.
Configurar la auditoría del registro de sistema, haciendo uso de la aplicación “regedt32.exe” ubicada en el directorio “C:\Winnt\system32”.
En el menú Inicio (Start) -> Programas (Programs) -> Herramientas Administrativas (Administrative Tools) ->Event Viewer, activar las siguientes opciones:

Security log: sobrescribir después de 30 días.
System log: sobrescribir después de 30 días.
Application log: sobrescribir cuando sea necesario.

Evaluar la posibilidad de adecuar el tamaño de los archivos de registro “logs” basado en los siguientes valores:

<table>
<tr><th>Tipo de Servidor</th><th>Security Log</th><th>System Log</th><th>Application Log</th></tr>
<tr><td>Controlador de dominio</td><td>> 200 MB</td><td>> 10 MB</td><td>> 10 MB</td></tr>
<tr><td>Print Server</td><td>> 10 MB</td><td>> 10 MB</td><td>> 10 MB</td></tr>
<tr><td>Administrador de Base de datos</td><td>> 10 MB</td><td>> 10 MB</td><td>> 10 MB</td></tr>
<tr><td>Web Server</td><td>> 10 MB</td><td>> 10 MB</td><td>> 10 MB</td></tr>
</table>
Es importante indicar que el cuadro presentado anteriormente no representa un esquema rígido, por lo cual debe considerarse como un modelo a seguir y ajustarlo con base a cada caso analizado.

Restringir el acceso otorgado a los archivos que almacenan los registros de auditoría (“appevent.evt”, “secevent.evt” y “sysevent.evt”) ubicados en el directorio “C:\Winnt\System32\CONFIG\”, limitándolo unicamente al personal encargado de efectuar las labores de mantenimiento y monitoreo de los registros de eventos de auditoría.
Definir políticas de revisión de eventos de auditoría, tales que expliquen que tipos de eventos se van a revisar, personas encargadas de revisar estos eventos, acciones y decisiones a tomar, penalizaciones, respaldos, entre otros.
Definir el tipo de estadísticas que se van a generar, de acuerdo a los hallazgos encontrados.

</td></tr>
</table>

Nro	Resumen de la situación identificada	Recomendación
		Finalmente, se recomienda evaluar la incorporación de herramientas automatizadas para la consolidación y análisis de los eventos generados por los diversos componentes que conforman la plataforma tecnológica la Entidad Financiera ABC, a fin de optimizar la identificación y estudio de eventos de seguridad y control.
Servicios		
21	Se identificaron debilidades relacionadas a servicios activos	Deshabilitar los servicios de “Messenger”, “Alerter” y NetBios en el servidor evaluado
Service Pack		
22	Se identificó que en el servidor evaluado se encuentra desactualizado el Service Pack	Instalar el “Service Pack 4” en el servidor evaluado y definir procedimientos para la identificación e instalación de nuevos “Services Pack” y “Hotfix” emitidos por el proveedor del sistema operativo. Adicionalmente se recomienda evaluar la utilización de herramientas especializadas para la distribución e instalación de parches en el sistema operativo, tanto para servidores como estaciones de trabajo.
Registry		
23	No se ha restringido la conexión de servidores y estaciones de trabajo anónimas al dominio.	Para restringir el acceso de estaciones de trabajo y servidores anónimos al dominio, se recomienda asignarle el valor de uno (1) a la entrada “RestrictAnonymous”, la cual se encuentra ubicada en la ruta: Ruta: HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\ Lsa Clave: RestrictAnonymous Valor = 1 Tipo de dato: REG_DWORD
24	El nombre de usuario de más reciente acceso a la red aparece en la caja de diálogo del próximo inicio de sesión	Para ocultar el nombre de usuario del último acceso, configurar en el registro del sistema el siguiente parámetro: Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon\ Clave: DontDisplayLastUserName Valor = 1 Tipo de dato: REG_SZ
25	El servidor no se oculta del resto de los computadores existentes en la red.	Asignar el valor de uno (1) en la entrada “hidden” (tipo de dato: REG_DWORD) que se encuentra en la ruta que a continuación se menciona, de manera de mantener ocultos los servidores al explorar la red: Ruta: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services\LanmanServer\ Parameters

Nro	Resumen de la situación identificada	Recomendación
		Clave: hidden Valor = 1 Tipo de dato: REG_DWORD
26	No se presentan en tiempo de inicio de sesión las normativas de seguridad de activos de información.	Realizar la notificación sobre las condiciones de uso de los activos de información con la finalidad de informar a los usuarios que la red sólo esta disponible para usuarios autorizados y que todas las actividades esta siendo monitoreadas. Dicha notificación se puede hacer efectiva a través de la asignación de valores a los parámetros “Legal Notice Text” y/o “Legal Notice Caption” mediante la ruta del registro: Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon Clave: LegalNoticeCaption (o LegalNoticeText) Valor: Texto Tipo de dato: REG_SZ

Tabla 8. Recomendaciones: Base de Datos Oracle del Sistema Back Office – Servidor Boprod2

Nro	Resumen de la situación identificada	Recomendación
Auditoría		
27	Las facilidades de auditoría que posee el manejador de bases de datos Oracle no se encuentran activas.	Para implantar la auditoría en el ambiente Oracle, se sugiere considerar la selección de las opciones que se muestran a continuación: - Habilitar el inicializador de parámetros “AUDIT_TRAIL” en el archivo de configuración de la base de datos. Se recomienda que este parámetro sea inicializado con la entrada “DB” para habilitar la auditoría de la base de datos y direccionar los registros a la tabla “SYS.AUD$”. - Luego de editar el archivo de parámetros, se debe reiniciar la instancia de la base de datos para aplicar los cambios. - Definir la auditoría de manera global o distribuida por usuario. Esta se puede definir mediante el procedimiento “AUDIT”. Este procedimiento está constituído de la siguiente manera

<table>
<tr><th>Nro</th><th>Resumen de la situación identificada</th><th>Recomendación</th></tr>
<tr><td></td><td></td><td>

Police_name: Parámetro requerido. Especifica el nombre da la política definida para ser auditada.
Users: Parámetro opcional. Si no se definen usuarios, aplica para todos.
Options: Parámetro opcional. Las opciones definidas son las siguientes:

APPLY: Audita cambios de actualización sobre tablas y esquemas.
REMOVE: Audita cambios de eliminación sobre tablas y esquemas.
SET: Audita los cambios de autorizaciones de usuarios y privilegios de programas y usuarios.
PRIVILEGES: Audita el uso de todos los privilegios especificados.

Si no se especifica ninguna opción, se auditan todos los parámetros anteriores a excepción de “Privileges”.

Type: Parámetro opcional. Audita la información a grabar con las opciones “BY ACCESS” o “BY SESSION”. Si no se especifica, se audita por la opción “BY SESSION”.
Success: Parámetro opcional. Audita los eventos efectivos o no efectivos “SUCCESSFUL” o “NOT SUCCESSFUL”. Si no se especifica el parámetro se auditan ambos.

</td></tr>
<tr><td colspan="3">Administración de usuarios</td></tr>
<tr><td>28</td><td>Se identificaron cuentas genéricas</td><td>Evaluar la posibilidad de individualizar el uso de cuentas de usuarios para cada una de las personas que requieran obtener acceso a la base de datos. Asimismo, se recomienda que el personal de Banca Virtual investigue, documente y evalúe la necesidad de utilizar cuentas genéricas, para así mitigar los riesgos asociados con esta debilidad.</td></tr>
<tr><td>29</td><td>Existen parámetros en el perfil “Default” que pudieran ser optimizados</td><td>A continuación se presentan los parámetros de administración y valores que deberían definirse en el perfil predeterminado, según las mejores prácticas de seguridad y acorde a la funcionalidad del manejador de la base de datos:
<table>
<tr><th colspan="3">RESTRICCION DE RECURSOS A NIVEL DE SESION</th></tr>
<tr><th>Variables del sistema</th><th>Significado de la variable</th><th>Valores adecuados</th></tr>
<tr><td>SESSIONS_PER_USER <entero></td><td>Número máximo de sesiones concurrentes por cada usuario de la base de datos.</td><td>Acorde con las responsabilidades y requerimientos de los usuarios.</td></tr>
<tr><td>CONNECT_TIME</td><td>Tiempo de conexión por usuario a una</td><td>Acorde con las</td></tr>
</table>
</td></tr>
</table>

Nro	Resumen de la situación identificada	Recomendación

<entero>	instancia de base de datos.	responsabilidades y requerimientos de los usuarios.
IDLE_TIME <entero>	Tiempo máximo (minutos) permitido de inactividad en la conexión de un usuario a una instancia	Menor o igual a diez (10) minutos.

CONFIGURACION DE CONTRASEÑAS		
Variables del sistema	**Significado de la variable**	**Valores adecuados**
FAILED_LOGIN_ATTEMPTS <entero>	Cantidad de intentos fallidos de conexión antes de que la cuenta de usuario sea bloqueada.	Asignar tres (3) como valor.
PASSWORD_LOCK_TIME <entero>	Tiempo (días) en que una cuenta permanecerá bloqueada después de haber alcanzado el máximo número de intentos fallidos de sesión.	Asignar siete (7) como valor.
PASSWORD_LIFE_TIME <entero>	Tiempo (días) de vida de la contraseña.	Asignar noventa (90) como valor.
PASSWORD_REUSE_TIME <entero>	Tiempo (días) luego del cual puede reutilizarse una contraseña	Debe asignársele el valor “UNLIMITED” si en el parámetro “PASSWORD_REUSE_MAX” se ha especificado un valor entero.
PASSWORD_REUSE_MAX <entero>	Cantidad de contraseñas distintas antes de volver a reutilizar alguna de ellas.	Asignar diez (10) como valor.
PASSWORD_GRACE_TIME <entero>	Tiempo de gracia (días) para cambiar la contraseña.	Asignar tres (3) como valor.

Nro	Resumen de la situación identificada	Recomendación
Privilegios de acceso		
30	Se evidenció que el rol “PUBLIC” tiene privilegios sobre algunas tablas críticas de la base de datos	Restringir los privilegios asignados la cuenta “PUBLIC”, en particular los accesos a las vista de tipo “ALL_SOURCE”, asignando dichos privilegios de manera explicita a los usuarios, grupos o roles que así lo requieran.

CONCLUSIONES

Para las organizaciones invertir en seguridad de redes está muy lejos de ser un gasto. Es una decisión que les permitirá prevenir posibles pérdidas cuantiosas, reducir costos operativos, aumentar la productividad y en especial, potenciar el uso de las tecnologías de información para obtener aún más beneficios económicos.

Apegado a esta realidad la Entidad Financiera ABC ha iniciado esfuerzos en la definición de su esquema de seguridad global, para lo cual el desarrollo de este trabajo precedería las primeras bases del proceso. Cada vez son más las noticias de violaciones a las redes empresariales. Hackers que entran a los sitios web públicos de las empresas y colocan desafiantes graffitis en sus páginas; robos de información confidencial de bases de datos de compañías, incluyendo información interna privilegiada y direcciones de miles de clientes, que después circulan libremente por Internet; acceso a información de cuentas bancarias; y esto por citar sólo los casos más sonados.

Estas fallas en la seguridad de redes tienen un impacto económico valorado en millones de dólares, no sólo por las pérdidas originadas debido al uso ilegal de la información sino también por los efectos negativos en la reputación de las empresas atacadas.

En este sentido, el plan de recomendaciones sugeridas a la Entidad Financiera ABC, definitivamente dependerá de su disponibilidad y necesidades para la aplicación de las mismas. No obstante, el esquema planteado no busca la incorporación de nuevos componentes dentro del servicio de BANCA On-Line, sino aprovechar las facilidades de seguridad de los sistemas existentes, lo cual minimizaría los costos asociados al proyecto. El desarrollo de este tipo de trabajos en términos generales mejora rápida y efectivamente los niveles de calidad en la prestación de los servicios de tecnología ofrecidos por la Entidad a los clientes

internos y externos, no solamente desde el punto de vista de mejora del rendimiento, sino también asegurando la información, su integridad, y confiabilidad.

RECOMENDACIONES

Intrínsecamente este tipo de trabajos incrementa la cultura organizacional respecto a la seguridad de la información, aunado a ventajas especificas disponibles desde el inicio del mismo; entre estas tenemos mejoras en la integridad, disponibilidad, prestación de servicios de la información, disminución de problemas operacionales, transferencia de conocimiento entre el personal técnico informático y expertos especialistas de la seguridad informática, drástica reducción de costos asociados a pérdidas de información por incidentes de seguridad, reducción de la manipulación de información confidencial por personas no autorizadas (internas o externas), aumento de destrezas técnicas asociadas a detección, prevención y corrección de incidentes que amenacen la información de la organización, reducción de los tiempos de evaluación e implantación de soluciones de seguridad, reducción en los costos asociados a adiestramiento y formación del personal técnico especializado, reducción de tiempos de dedicación del recurso humano en la ejecución de actividades especializadas, entre otras.

Indudablemente y dados los beneficios asociados, se hace necesario iniciar la planificación de una estrategia de seguridad en la Entidad Financiera ABC, la cual iniciaría con la aplicación del conjunto de recomendaciones descritas anteriormente, y cuyo seguimiento y supervisión debería asignarse a una estructura organizacional creada para la atención y control de la seguridad. Adicionalmente, recomendamos definir un plan para la revisión del resto de servicios críticos de la Organización que no formaron parte de este alcance y que en definitiva permitiría minimizar otras brechas de seguridad.

GLOSARIO DE TÉRMINOS

A

Acceso. Con respecto a la privacidad, es la habilidad de un individuo para ver, modificar y refutar lo completa y precisa que pueda ser la información personal identificable reunida sobre él o ella.

Acceso Remoto: Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

Actualización (update). Es el término que se utiliza para identificar todos los diferentes tipos de paquetes que pueden hacer que un sistema esté al día, incluyendo hotfixes, acumulados, Service Packs, y otros paquetes que incluyan características. Las actualizaciones se caracterizan por la severidad del tema que tratan. Algunas actualizaciones son críticas mientras que otras son recomendadas.

Administración con privilegios mínimos. Es una práctica de seguridad recomendada en la cual a cada usuario se le proporciona solamente los privilegios mínimos necesarios para llevar a cabo las tareas que están autorizados a realizar.

Amenaza: Situación o evento con que puede provocar daños en un sistema.

Antivirus. Es el software diseñado específicamente para la detección y prevención de virus conocidos.

Ataque de negación de servicio (DoS, por sus siglas en inglés). Ataque a una red diseñada para deshabilitarla mediante congestionamientos inútiles de tráfico.

Muchos de estos ataques, como los ataques Ping of Death y Teardrop, aprovechan las limitaciones de los protocolos TCP/IP.

Ataque remoto. Es un ataque que tiene como objetivo una PC diferente en la que el atacante ha iniciado una sesión interactiva. Por ejemplo, un atacante puede iniciar una sesión en una estación de trabajo y atacar a un servidor en la misma red o en una diferente.

Auditoría. Proceso de examinar y revisar un informe cronológico de los eventos de sistema para determinar su significado y valor.

Autenticación. Es el proceso de verificar que alguien o algo es quien o lo que dice ser. En redes de equipos públicos y privados (incluyendo Internet), la autenticación se lleva a cabo comúnmente a través de contraseñas de inicio de sesión.

Autorización. Con referencia a la computación, especialmente en los equipos remotos en una red, es el derecho otorgado a un individuo o proceso para utilizar el sistema y la información almacenada en éste. Típicamente la autorización es definida por un administrador de sistemas y verificado por el equipo basado en alguna identificación del usuario, como son un código o una contraseña.

B

Bomba de correo. Es una cantidad excesiva de información en correo electrónico enviada a la dirección de un usuario en un intento por hacer que el programa de correo electrónico del usuario colapse o para evitar que el usuario reciba mensajes legítimos.

C

Caballo de Troya. Es un programa computacional que aparentemente es útil pero que en realidad causa daño.

Calidad en el servicio – QoS. Es un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de información.

Capa de Sockets Seguros – SSL. Es un protocolo para establecer un canal de comunicaciones cifrado que ayuda a prevenir la interceptación de información crítica, como números de tarjeta de crédito en World Wide Web y en otros servicios de Internet.

Cifrado. Traducción de datos a un código secreto. El cifrado es la manera más eficaz de proteger datos, ya que para leer los archivos cifrados es necesario tener acceso a una clave secreta o contraseña que te permita descifrar la información. Los datos no cifrados se denominan texto sin formato, mientras que los cifrados se conocen como texto cifrado. Existen dos tipos principales de cifrado: cifrado asimétrico (también llamado cifrado por clave pública) y cifrado simétrico.

Cookie. Mensaje que un servidor de Web entrega a un explorador de Internet. Las cookies tienen como objetivo beneficiar al usuario recordando sus preferencias cada vez que visita un sitio.

Cracker. Es aquella persona que se dedica a romper las protecciones de software (o a veces hardware) de los programas comerciales, pero también es aquel que entra en un sistema sólo para destrozar y tirar todo.

D

Datos encriptados. Es la información que ha sido convertida de texto simple a texto cifrado.

Delito Informático. Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

DMZ. Zona desmilitarizada es usada por una compañía que requiere tener sus propios servicios de Internet sin sacrificar el acceso restringido a su red privada.

Dominio. Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre.

E

Extranet. La red usada por una empresa para conectarse con sus clientes y socios de negocios.

F

Firma digital. Código digital que se puede adjuntar a un mensaje transmitido por medios electrónicos y que identifica de manera exclusiva al remitente.

FTP (File Transfer Protocol). Protocolo de transferencia de archivos. Es el método normal de enviar archivos entre computadoras en el Internet.

G

Gusano. Programa o algoritmo que se reproduce en una red informática y suele realizar actividades maliciosas, como consumir los recursos de la computadora y hasta cerrar el equipo.

H

Hacker. Alude a una persona hábil con las computadoras y respetuosa con ellas, que ha logrado adquirir conocimientos avanzados sobre todo tipo de sistemas con la finalidad de introducirse a ellos solo para curiosear sin propósitos destructivos.

El Hacker quiere mantener el flujo de la información libre, sin atacar para nada empresas o intereses comerciales. Incluso ayuda a mantener un cierto orden dentro de Internet.

HTTP. Abreviación de la designación estadounidense para Protocolo de transferencia de hipertexto. Se trata del protocolo más utilizado para transferir datos entre un servidor y otra máquina.

I

Internet. (De inter, internacional y net, en inglés, red). Todas las computadoras del mundo conectadas entre si. como si se tratara de una enredadera o red. En su primera etapa la conexión de las computadoras es a través de la red telefónica existente. En su última etapa la conexión será por medio de fibra óptica, si es que no aparecen tecnologías que le permitan hacerlo vía inalámbrica.

Intranet. (De intra, interno y net, en inglés, red). Red interna de una empresa, que parcialmente puede exponer información al exterior vía Internet. Es el concepto moderno con el que se manejan los sistemas internos de una empresa, tales como inventarios, requisiciones, liberaciones; ordenes de entrada y salida de almacén; ordenes de trabajo, de venta y de compra; facturación, requisiciones; documentación MRP I y II, SPC; documentación técnica y de producto, etc. permitiendo que los empleados accedan al sistema a través de un sistema de accesos controlados.

IP o dirección IP (IP Address). Dirección en el protocolo del Internet que identifica a una máquina conectada.

IPsec - IP Security. Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben

compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

J, K , L

LAN. Red de Área Local Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topología en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

Log (Log File). Archivo creado por un servidor que contiene toda la información relativa al acceso a un sitio.

M, N

No repudio ("nonrepudiation"). Es la habilidad de identificar quien ha llevado a cabo varias acciones en una PC, para que los usuarios no puedan negar las responsabilidades de las acciones que ellos llevan a cabo. Generalmente utilizado en el sentido de crear una huella de auditoría indiscutible para identificar la fuente de una transacción comercial o acciones maliciosas.

O, P

Perfil de usuario. Configuraciones que definen las preferencias de personalización de un usuario en particular, tales como las configuraciones de

escritorio, conexiones de red persistentes, información personal identificable, utilización de un sitio Web y otros comportamientos y datos demográficos.
Permisos. Regla asociada con un objeto, como un archivo, para regular qué usuarios pueden obtener acceso al objeto y de qué manera. El dueño del objeto otorga o niega los permisos.

Plataforma (Platform). El sistema operativo de la máquina, tal como Windows 95, Windows NT, UNIX, LINUX, etc.)

Política de seguridad. 1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.
Privilegios. Es el permiso otorgado a un usuario para llevar a cabo una tarea específica, usualmente una que afecta a todo un sistema computacional en lugar de a un objeto en particular. Los privilegios son asignados por un administrador, a usuarios individuales o a grupos de usuarios, como parte de las configuraciones de seguridad de una PC.

Protección. Término que se refiere a las técnicas usadas para evitar la lectura y el daño intencional de los datos guardados en un computador. La mayoría de las medidas de protección exigen el cifrado de los datos y el uso de contraseñas.
Protocolo (Protocol). El conjunto de reglas que permite intercambiar datos entre dos máquinas.

Protocolo de Internet (IP). Parte de una serie de protocolos que rastrean la dirección de Internet de los nodos, encaminan los mensajes enviados y reconocen los mensajes recibidos.

Q

QoS (s). Calidad de Servicio.

R

Rechazo (“repudiation”). La habilidad de un usuario para negar haber llevado a cabo una acción que otras partes no puedan refutar. Por ejemplo, un usuario que borre un archivo puede con éxito negar haberlo hecho si no existe ningún mecanismo (como archivos de auditoría) que pueda contradecir su declaración.

Red Privada Virtual – VPN. Red de información privada que hace uso de una red pública, como Internet, al cifrar información en un nodo y utilizar procedimientos de seguridad que proporcionan un túnel a través del cual la información puede pasar a otro nodo.

S

Seguridad. Es la disciplina, técnicas y herramientas diseñadas para ayudar a proteger la confidencialidad, integridad y disponibilidad de información y sistemas

Service Pack – SP. Es un conjunto acumulado de todos los hotfixes creados y las correcciones para errores encontrados internamente desde la publicación del producto. Los Service Packs pueden contener también un numero limitado de peticiones del cliente para cambios de diseño o características. Éstos son ampliamente distribuidos y por tanto probados arduamente.

SMTP. (Simple Mail Transfer Protocol o Protocolo Sencillo de transferencia de correo). El protocolo con el que se transmite un mensaje de correo electrónico de una máquina a otra.

Sniffer. Programa o dispositivo capaz de leer los datos transmitidos por una red. Los programas de espionaje informático se pueden usar con fines legítimos de gestión de la red y para robar información de la red. En las redes TCP/IP en las que espían la información de los paquetes, suelen recibir el nombre de programas de espionaje informático de paquetes o packet sniffers.

SPAM. También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

SSL. Protocolo para permitir comunicaciones cifradas y autentificadas a través de la red Internet. La aplicación del protocolo se inicia generalmente con la llamada a una página con el protocolo "https". El protocolo proporciona privacidad, autentificación e integridad en el mensaje. En una conexión segura o SSL cada una de las partes envía información a la otra del Certificado de seguridad propio, que se utiliza para codificar la información. Para decodificar esta información se requiere por lo tanto dos claves, una del emisor y otra del receptor, garantizando la seguridad de los mensajes.

T

TCP/IP. Tomado de la expresión en inglés Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisiones y protocolo de la Internet). Es el conjunto de Protocolos que definen la comunicación Internet.

Troyano. Programa destructivo que se encubre bajo la forma de una aplicación inofensiva. A diferencia de los virus, los troyanos no son capaces de reproducirse por sí mismos, pero pueden ser igualmente destructivos.

U

URL (Uniform Resource Locator o Localizador uniforme del recurso). Es el mecanismo para identificar una ubicación exacta en el Internet. Por ejemplo, http://www.hermosillovirtual.com/servicios/glosario.htm define la ubicación de la página glosario.htm en el directorio servicios en la máquina hermosillovirtual.com con un protocolo específico (http, ftp, etc..).

V

Virus. Programa o parte de un código que se carga secretamente en tu computadora, por lo general a través de un documento adjunto a un mensaje de correo electrónico, y se ejecuta sin tu conocimiento.

Vulnerabilidades. Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

W

WAN - Red de Área Amplia. Tipo de red compuesta por dos o más redes de área local (LANs) conectas entre si vía teléfono (generalmente digital).

X, Y, Z

BIBLIOGRAFÍA

BOBROWSKI, Steve. Oracle 8i para Windows NT Edición de Aprendizaje. Oracle Press McGRAW-HILL, España 2000.

Espiñeira, Sheldon y Asociados, Firma Miembro de PriceWaterHouseCoopers. Encuesta Nacional 2004, Prácticas de seguridad de activos de información en las empresas en Venezuela, Diciembre 2004.

Information Systems audit. And Control Association. Manual de Información Técnica para la preparación al Examen CISA 2001. Octubre 2000.

PITTOL, Victor. Evaluación de seguridad de una institución financiera mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica. Trabajo de Grado presentado a la Universidad Central de Venezuela para optar al título de Especialista en Comunicaciones y Redes de Comunicación de Datos. Junio 2004.

MICROSOFT CORPORATION. Seguridad en Microsoft Windows 2000, Referencia Técnica. Primera Edición. McGraw-Hill. España, 2001.

FUENTES ELECTRÓNICAS

Tipos de Investigación

- Criterios Metodológicos de la investigación. http://medusa.unimet.edu.ve/faces/fpag40/criterios.htm#TIPOS%20DE%20INVESTIGACIÓN.

- Marco Metodológico.
  http://www.monografias.com/trabajos15/docencia/docencia2.shtml

- DiseñomMetodológico.
  http://docencia.udea.edu.co/investigacioninternet/contenido/metodologia.pdf

Programas de Auditoría

- Internal Audit Resources for Internal Auditors.
  http://www.auditnet.org

- Windows 2000 Security Checklist
  http://www.labmice.net/articles/securingwin2000.htm

Estándares de Seguridad de Información

- ISO/IEC 17799:2005
  http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

- Gestión de la Seguridad de Información: UNE 71502, ISO 17799
  http://www.criptored.upm.es/guiateoria/gt_m209b.htm

- Políticas de Seguridad Informática
  http://www.dnp.gov.co/archivos/documentos/Coinfo_politicas/seguridad.pdf

Centros especialistas en Seguridad Informática

- CERT® Coordination Center (CERT/CC)
  http://www.cert.org

- System Administration, Networking, and Security
  http://www.sans.org

- Center for Internet Security
  http://www.cisecurity.org/

Glosarios de Seguridad Informática

- http://espanol.sbc.com/help/internet_safety/utility/glossary.html
- http://www.microsoft.com/spain/technet/seguridad/recursos/glosario/default.mspxht
- http://www.virusprot.com/Glosarioc.html#Delito%20Informático
- http://www.rediris.es/cert/doc/unixsec/node36.html
- http://www.dgonzalez.net/es/glosario/es/