TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE SEGURIDAD DE UNA INSTITUCIÓN FINANCIERA MEDIANTE LA EJECUCIÓN DE UN ESTUDIO DE PENETRACIÓN INTERNO Y EXTERNO A SU INFRAESTRUCTURA TECNOLÓGICA

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. Víctor E. Pittol Mendoza

Caracas, Octubre de 2004

TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE SEGURIDAD DE UNA INSTITUCIÓN FINANCIERA MEDIANTE LA EJECUCIÓN DE UN ESTUDIO DE PENETRACIÓN INTERNO Y EXTERNO A SU INFRAESTRUCTURA TECNOLÓGICA

TUTOR ACADEMICO: Prof. Carlos Moreno

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. Víctor E. Pittol Mendoza

Caracas, Octubre de 2004

UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE INGENIERÍA

COMISIÓN DE ESTUDIOS DE POSTGRADO

VEREDICTO

Quienes suscriben, miembros del Jurado designado por el Consejo de la Facultad de Ingeniería para examinar el Trabajo Especial presentado por el Ing. **VICTOR E.PITTOL M.**, Cédula de Identidad número V-12.828.829, y titulado "*EVALUACIÓN DE SEGURIDAD DE UNA INSTITUCIÓN FINANCIERA MEDIANTE LA EJECUCIÓN DE UN ESTUDIO DE PENETRACÓN INTERNO Y EXTERNO A SU INFRAESTRUCTURA TECNOLÓGICA*", a los fines de cumplir con el requisito legal para optar al título de **ESPECIALISTA EN COMUNICACIONES Y REDES DE COMUNICACIÓN DE DATOS**, dan fe de lo siguiente:

1. Una vez leído, como fue, dicho trabajo por cada uno de los miembros del jurado, el coordinador del jurado convocó para efectuar la defensa en forma pública el día jueves 7 de octubre de 2004, a las 2:00 p.m., en la Auleta de Postgrado de la Facultad de Ingeniería de la U.C.V.

2. La defensa comenzó a las 2:15 p.m. en el sitio y en la fecha antes señalados. El aspirante hizo un resumen oral de su Trabajo Especial, luego de lo cual respondió satisfactoriamente las preguntas que le fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en el artículo 44 del Reglamento de Estudios de Postgrado de la Universidad Central de Venezuela.

3. Finalizada la defensa pública, el jurado deliberó en privado y por unanimidad decidió **APROBAR** el Trabajo por considerar, sin hacerse solidario de las ideas expuestas por el autor, que se ajusta a lo dispuesto y exigido en el Reglamento antes citado. Para dar este veredicto, el Jurado estimó que el Trabajo en cuestión ofrece un aporte desde el punto de vista técnico, para la implantación de los controles de seguridad necesarios para mitigar los riesgos de una organización, protegiendo así de una forma más segura sus activos.

En fe de lo cual se levanta la presente acta, en original y tres copias, en Caracas, a los siete días del mes de octubre del año dos mil cuatro, dejándose constancia que conforme a la normativa jurídica vigente, actuó como coordinador del jurado, el Prof. Carlos Moreno, tutor del trabajo.

Ing. Vincenzo Mendillo (M. Sc.)

Dra. Rina Suroz

Ing. Carlos Moreno (Esp.)

DEDICATORIA

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

AGRADECIMIENTO

A Dios y a mi Madre por no dejarme decaer ante los momentos difíciles.

A mi Hermano por servirme de motivación y permitirme ser su modelo como profesional.

A mi Abuela y Abuelo por contar siempre con su apoyo y preocupación.

A mi Padre por brindarme confianza en el desenvolvimiento de mis actividades.

A mi Novia por estar siempre apoyándome de manera incondicional y estar presente cuando la he necesitado.

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

A todas aquellas personas que de una u otra forma contribuyeron al logro de este objetivo y se sienten satisfechas de verme en el estatus que hoy represento profesionalmente.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE TABLAS

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES
Y REDES DE COMUNICACIÓN DE DATOS

EVALUACIÓN DE SEGURIDAD DE UNA INSTITUCIÓN FINANCIERA MEDIANTE LA EJECUCIÓN DE UN ESTUDIO DE PENETRACIÓN INTERNO Y EXTERNO A SU INFRAESTRUCTURA TECNOLÓGICA

AUTOR : Ing. Víctor E. Pittol M.
TUTOR : Prof. Carlos Moreno.
AÑO: 2004.

RESUMEN

El presente trabajo muestra los resultados obtenidos de una evaluación de seguridad de una institución financiera mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica. Por motivos de confidencialidad no se revelará el nombre real de la empresa financiera en cuestión. De aquí en adelante se hará referencia a la misma como Institución “XXX”. El objetivo principal del servicio fue dar a conocer las amenazas que representa un intruso o “hacker” a los activos de información de la Institución “XXX”, a través de un ataque desde cualquier punto interno y externo a su plataforma tecnológica, con el fin de concientizar a todos los niveles de la Institución en el tema de seguridad informática, para que de esta manera se implanten los controles de seguridad necesarios para mitigar los riesgos existentes y se efectúen seguimientos periódicos a los mismos, protegiendo así de una manera más efectiva sus activos de información.

Para el desarrollo del servicio, se tomó como base cuatro etapas generales ("Obtención de información e identificación de amenazas", "Evaluación de los riesgos o amenazas identificadas", "Intento de acceso "Intrusión" a la plataforma tecnológica" y "Análisis de resultados y emisión de recomendaciones") que constituyen la metodología aplicada. Basado en los resultados de la evaluación de seguridad mediante la ejecución de un estudio de penetración interno y externo a la Institución “XXX”, la misma en conocimiento de las vulnerabilidades y riesgos que posee su plataforma tecnológica, ha tomado conciencia en relación a la necesidad de implantar controles de seguridad que mitiguen los riesgos de acceso no autorizado e interrupción de su continuidad operativa producto de posibles intrusos que busquen de obtener acceso a sus activos de información, afectar su imagen e incursionar en problemas de índole legal, tomando una actitud proactiva en relación al tema.

INTRODUCCION

El mundo presenta constantes cambios, y en esta ocasión los mismos están enfocados hacia la utilización de la tecnología como reemplazo a los medios tradicionales de comunicación e interacción de las personas. No en vano, Internet es denominada en los medios publicitarios como “el cuarto medio”. Es normal suponer entonces, que si reemplazamos el cómo hacer las cosas, quienes deseen alterar el medio u obtener un beneficio ilícito deben también reemplazar su manera de actuar.

La delincuencia evoluciona en paralelo con la tecnología. A medida que se han desarrollado nuevas formas de protegerse de la delincuencia, ésta ha respondido ingeniando nuevas formas de violentar los controles. Si comparamos los sistemas de seguridad física y computarizada utilizadas hace 10 años, nos sorprendemos de su enorme evolución, pero esta evolución sólo se produce como consecuencia de la evolución equivalente de los tipos de ataques efectuados.

Hoy día, cualquier persona cuya vida profesional dependa total o parcialmente de las computadoras, conoce o ha escuchado la palabra “hacker” y con ella se identifica a aquellas personas que han atacado los sistemas informáticos de alguna organización o han demostrado debilidades en los mismos. La existencia de estos individuos, lejos de ser un mito, es un fenómeno del que puede sorprendernos su frecuencia.

El ser “hacker” o “cracker” (denominación dada a aquellas personas que utilizan las debilidades detectadas por los “hackers” para obtener un beneficio), no es un título adquirido sino una actividad efectuada por cualquier persona cuyo interés en la informática sea superior al promedio, y con una motivación para hacerlo.

El presente servicio (Estudio de Penetración), propone una solución viable a tal situación; éste muestra todos los aspectos que se tomaron en cuenta para evaluar los controles de seguridad existentes en la plataforma tecnológica de la institución financiera en cuestión y concienciar a la alta gerencia de la necesidad de evaluar periódicamente dichos controles dados a los constantes cambios en su plataforma tecnológica y el origen de nuevas brechas de seguridad.

Por motivos de confidencialidad no se revelará el nombre real de la empresa financiera en cuestión. De aquí en adelante se hará referencia a la misma como Institución "XXX".

Este trabajo consta de seis capítulos. El primero se refiere al PLANTEAMIENTO DEL PROBLEMA, donde se establecen de una manera clara y precisa las incidencias del problema; además junto a éste se enuncian la justificación, los objetivos (general y específicos), el alcance, las limitaciones y un breve estudio de factibilidad de este servicio.

El capítulo II corresponde al MARCO TEORICO, en el que se presentan las bases teóricas.

En el capítulo III se muestra el MARCO METODOLOGICO, el área, el tipo de investigación y la metodología empleada para desarrollar este servicio.

El capítulo IV hace referencia a la SITUACIÓN ACTUAL, donde se obtiene información de la plataforma tecnológica del cliente, se identifican las vulnerabilidades, se evaluan los riesgos de las vulnerabilidades identificadas y se mencionan los ambientes tecnológicos que pueden ser accedidos de manera no autorizada por "Intrusos".

El capítulo V muestra la SITUACIÓN PROPUESTA, en el que se elabora las

recomendaciones para minimizar los riesgos de seguridad de la plataforma tecnológica evaluada.

Finalmente en el capítulo VI se establecen las estrategias de implantación de las recomendaciones en períodos corto, mediano y largo plazo con relación a niveles de riesgo bajo, mediano y alto.

CAPITULO I

EL PROBLEMA

1. Planteamiento del Problema

Hoy en día muchas organizaciones de cualquier sector, cuyos procesos críticos de negocio dependen de la tecnología de información, desconocen los riesgos a los que se exponen, producto de las posibles brechas de seguridad existentes en su plataforma tecnológica, y las acciones a seguir para adaptar los controles de seguridad de sus activos de información contra ataques de personas no autorizadas tanto internas como externas a la organización. En este sentido, la Institución "XXX" se encuentra entre estas organizaciones que desconocen en gran parte los riesgos de seguridad tecnológicos a los que exponen sus activos de información y la necesidad de realizar seguimientos periódicos a los controles que se vayan implantando para mitigar los mismos.

Por lo mencionado anteriormente, una de las maneras más efectivas de crear conciencia de seguridad en la Institución "XXX" dado los posibles riesgos a los que se exponen desde el punto de vista tecnológico, fue ofreciendo un servicio de consultoría conocido como pruebas de penetración ("Penetration Test"), donde el mismo consiste en simular un "hacker" mediante ataques internos y externos controlados, sin producir daño en los sistemas del cliente.

"XXX" es una institución, que busca posicionarse en el mercado financiero a través de las ventajas competitivas que la caracterizan. Este tipo de mercado posee ciertas características que exigen elementos de control y seguridad en mayor grado que en otro tipo de industria, que deben intensificarse, cuando la orientación de la

Institución está enfocada a la prestación de servicios financieros a través de Internet. Las estrategias fundamentales de diferenciación de "XXX", están basadas en la calidad del servicio y en la utilización de tecnología de punta en todos sus procesos operativos, y como consecuencia de esto, son mayores los riesgos y debilidades técnicas que pueden existir en la infraestructura de hardware y software.

Por tal motivo, el esfuerzo inicial estuvo centrado en concientizar a la Institución de fortalecer su ambiente de seguridad, razón por la cual la Vicepresidencia de Sistemas solicitó la evaluación de seguridad de su infraestructura tecnológica, con el fin de determinar posibles brechas en los componentes que conforman los activos de información de la Institución, aceptando la propuesta de ejecutar un estudio de penetración interno y externo a su plataforma tecnológica con el fin de conocer sus actuales brechas de seguridad que pudieran ser usadas por un intruso para tener acceso a su información crítica o confidencial, o bien tratar de interrumpir la continuidad de sus operaciones.

En este sentido, la Presidencia General y la Vicepresidencia de Sistemas de la Institución "XXX" al entender los riesgos a los cuales pueden estar expuestos, manifiestan una mayor preocupación por parte de la misma en proteger la información crítica contra accesos no autorizados, que puedan alterar el funcionamiento normal de las actividades del negocio. Es por ello que consideran importante contar con una adecuada configuración orientada a la seguridad de los activos de información, para la protección de los recursos de computación los cuales pueden ser víctimas de numerosos ataques de "*hackers*", favorecidos por la integración de servicios de comunicación, como por ejemplo redes LAN, Internet, entre otras.

En este orden de ideas, toda organización como agrupación social, adquiere posiciones determinadas ante ciertas situaciones. Aun cuando ninguna Institución se puede enmarcar dentro de una posición de forma exacta, en general existen tres etapas que caracterizan la conducta de las mismas ante los riesgos que rodean a los activos de información, a saber:

Etapa Inactiva: las empresas con actitud inactiva con respecto a la seguridad son aquellas que se encuentran satisfechas de la forma como están sus controles y en consecuencia suponen que cualquier intervención al curso de los eventos no lo mejorará.

Etapa Reactiva: las empresas con este tipo de actitud, comienzan a reaccionar luego de la ocurrencia de eventos que de una u otra manera han atentado contra la operatividad del negocio, estableciendo entonces planes de acción para la definición de un marco global de seguridad de sus activos de información.

Etapa Proactiva: las empresas con actitud proactiva no se conforman con la seguridad ofrecida por su situación actual. Tratan de predecir y prepararse para disminuir los riesgos. Su objetivo principal es lograr un ambiente más seguro y adelantarse en ingenio al agresor tanto como sea posible.

Por lo mencionado anteriormente, la Institución “XXX” para el momento de ofrecerle el servicio de consultoría antes mencionado, se encontraba enmarcada con una actitud inactiva, y luego de aceptar este servicio se encuentra en vía de adquirir

una actitud proactiva.

2. Justificación del servicio

Para que una Institución financiera pueda mantener su prestigio y ser más competitiva, tiene que tomar en cuenta el mejoramiento continuo de sus procesos y en especial prestar atención a la calidad de sus servicios que deben estar soportados sobre una infraestructura tecnológica altamente disponible y con controles de seguridad implantados para mitigar los riesgos a los que pudieran estar expuestos.

Dado el planteamiento del problema y de acuerdo al incremento de ataques y fraudes informáticos sufridos por muchas empresas en los últimos años, fue necesario que la Institución "XXX" evaluara los controles de seguridad implantados en su plataforma tecnológica 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.

Mediante este servicio la Institución "XXX" puede proteger sus recursos de red y de información, lo que mitigaría ataques informáticos que puedan ocasionar paradas en los sistemas y en consecuencia pérdidas monetarias para la Institución, ya que dejaría de percibir fondos y ocasionaría desatención en los clientes que en muchos de los casos se podrían cambiar a la competencia.

Por otra parte, este trabajo estimulará a la Institución en asumir una actitud proactiva ante los aspectos relacionados a la seguridad de la información, dado a los continuos cambios que sufre su plataforma tecnológica y las nuevas vulnerabilidades producto de la globalización, sobre todo por la falta de iniciativa de muchas

corporaciones en dar importancia a la seguridad informática.

3. Objetivos

3.1. Objetivo General

Dar a conocer las amenazas que representa un intruso o "hacker" a los activos de información de la Institución "XXX", a través de un ataque desde cualquier punto interno y externo a su plataforma tecnológica, con el fin de concientizar a todos los niveles de la Institución en el tema de seguridad informática, para que de esta manera implanten los controles de seguridad necesarios para mitigar los riesgos existentes y efectúen seguimientos periódicos a los mismos, protegiendo así de una manera más efectiva sus activos de información.

3.2. Objetivos Específicos

Este servicio fué realizado de manera que se aseguró al cliente la efectividad, confidencialidad e integridad de los datos a explorar, manteniendo presente los objetivos que se describen a continuación:

- Detectar las brechas de seguridad que posee la plataforma tecnológica de la Institución "XXX" por donde un intruso o "hacker" podría acceder de forma no autorizada a sus activos de información.

- Presentar los riesgos asociados a las debilidades detectadas durante el estudio de penetración, detallando las consecuencias que podrían ocasionar a los activos de información. Además, se hará especial énfasis en los niveles de riesgo (Alto,

Medio, Bajo).

- Sugerir las alternativas que contribuyan a solventar o minimizar las vulnerabilidades detectadas durante el estudio de penetración, detallando los pasos a seguir para su implantación. De igual forma, se hará especial énfasis en el período de implantación de las recomendaciones o sugerencias (corto, mediano o largo plazo).

- Concienciar al cliente sobre los riesgos de seguridad a los que están expuestos sus activos de información contra posibles ataques de intrusos internos y externos a la organización, y la necesidad de efectuar revisiones periódicas en cuanto a los controles de seguridad de su plataforma tecnológica.

- Enmarcar a la Institución "XXX" sobre una actitud proactiva, de manera que no se conforme con los controles de seguridad que posea en un momento determinado, sino que por el contrario, busque de predecir y prepararse para disminuir los riesgos, logrando un ambiente más seguro y adelantarse en ingenio al agresor tanto como sea posible.

4. Alcance del servicio

El servicio consiste en evaluar la seguridad de la institución financiera "XXX" mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica, con el fin de colocarla en vías de una actitud proactiva ante las continuas amenazas de seguridad que surgen por el crecimiento tecnológico e implante los controles de seguridad necesarios para mitigar sus brechas o debilidades actuales.

A continuación se presentan las etapas que abarcará este servicio y la descripción

de las mismas:

- Identificación, la cual consiste en obtener información de la topología de red, servidores y equipos (routers y switches) críticos, sistemas operativos, puertos activos, servicios y tipo de aplicaciones utilizando herramientas especializadas o ingeniería social.

- Diagnóstico, en donde se analizan las vulnerabilidades de seguridad identificadas en los componentes de red y aplicaciones críticas para los procesos del negocio, empleando herramientas especializadas y conocimientos profesionales.

- Recomendaciones, con las cuales se indican los lineamientos a seguir para implantar los controles de seguridad necesarios para mitigar los riesgos identificados que eventualmente pudieran comprometer los activos de información de la Institución "XXX".

- Estrategias, en donde se le proporciona a la Institución "XXX" los planes de implantación de las recomendaciones en corto, mediano y largo plazo, así como los niveles de riesgo bajo, mediano y alto.

Con este alcance, se pretende mitigar los riesgos de acceso no autorizado e interrupción de la continuidad operativa de los equipos que posee actualmente la Institución "XXX" evaluados bajo la modalidad del servicio de estudio de penetración interno y externo, en donde no necesariamente debe reportar todas las debilidades del ambiente de los sistemas de información computarizados que posea la Institución.

5. Análisis de Factibilidad

Para lograr desarrollar este trabajo, se consideraron tres estudios de factibilidad,

todos con el mismo nivel de importancia o prioridad, ya que se encuentran enfocados hacia la búsqueda de una solución óptima al problema planteado.

5.1. Factibilidad Técnica

La Institución financiera "XXX" 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.

5.2. Factibilidad Económica

La Institución "XXX" tomando en cuenta las posibles brechas de seguridad en su plataforma tecnológica que pudieran permitir accesos no autorizados a sus activos de información e interrupción de su continuidad operativa, consideran necesario y factible evaluar sus controles de seguridad para prevenir perdidas financieras a futuro e incluso degradación de su imagen y credibilidad por parte de sus clientes. Por esta razón, están dispuestos a invertir en este servicio con el fin de mantenerse en el competitivo mundo financiero apoyado sobre la tecnología y la globalización.

5.3. Factibilidad Operativa

La evaluación de los controles de seguridad de la Institución "XXX" brindará a la misma conciencia de implantar las recomendaciones sugeridas, en donde sus procesos de negocio, tanto internos como el de sus clientes, sean confiables y auténticos, mitigando la posibilidad que la información sea capturada, modificada o falsificada por personas no

autorizadas con propósitos fraudulentos que pongan en juego la credibilidad de la Institución e incluso incurrir en problemas de índole legal.

CAPITULO II

MARCO TEORICO

1. Bases Teóricas

Como bien su nombre lo dice, 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 con el trabajo presentado, y como incide en las recomendaciones para evaluar, diseñar e implantar controles de seguridad que mitiguen los riesgos de acceso no autorizado e interrupción de continuidad operativa, tanto desde Internet como en la red interna de la institución 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.

1.1. Sistemas

Según la **Universidad Nacional Abierta (1985)** el concepto de sistemas se refiere a cualquier conjunto de elementos organizados y relacionados para un propósito o una actividad. Esta definición señala que cualquier situación puede ser vista aplicando el enfoque de sistemas, por lo tanto la problemática planteada en esta investigación puede ser estudiada como tal.

1.2. Seguridad

La filosofía de la protección de la información se basa en el balancear la protección de los datos vs. la productividad de una manera efectiva en términos de costos.

1.2.1. Administración de Seguridad:

La administración de seguridad se ha convertido en una de las áreas más importantes en la administración de redes. Entre sus objetivos principales está diseñar y mantener un buen sistema de seguridad tanto físico como lógico para proteger los componentes y la información manejada en la red, así como las otras áreas de la administración de redes. La administración de seguridad consta de dos niveles:

Seguridad Física: involucra consideraciones como la protección de todos los recursos de la infraestructura de la red (estructuras de apoyo, enlaces de comunicación, hosts, servidores, etc.). Los equipos de red deben estar en un cuarto o en un lugar en el cual se pueda restringir la entrada a través de control de acceso, limitar el número de personas con acceso y hasta ofrecer un registro de identidad y la hora en que las personas entran a la sala.

Seguridad Lógica: incluye la protección de los datos y el software de la red de posibles incidentes, que van desde la infección de virus hasta el robo o modificación de estos, mediante el uso de medidas y controles como passwords, logins y grupos de usuarios. La seguridad lógica implica también el establecimiento de estrategias de respaldo y recuperación de datos que permitan minimizar el tiempo de restablecimiento de los servicios de la red.

1.2.2. Objetivos de la Seguridad de la Información

Se entiende por seguridad, la cualidad o estado de estar libre de daño o riesgo. La seguridad en las redes está relacionada con la seguridad de los sistemas, programas y datos que existen en ella. En la red la seguridad de la información

implica reforzar al menos cuatro aspectos básicos o componentes de la seguridad de información: confidencialidad, integridad, disponibilidad y autenticidad.

a) Confidencialidad:

La confidencialidad permite proteger la información del acceso por parte de personas no autorizadas. Este objetivo de la seguridad busca asegurar que únicamente las personas que requieren acceso a cierta información sean las que la posean. En algunas situaciones, cuando se maneja información secreta y confidencial, las personas deben tener acceso sólo a la información necesaria para realizar su trabajo, protegiendo de esta forma la confidencialidad de dicha información.

b) Integridad:

La 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 la integridad puede ser causada por errores humanos, actitudes intencionadas o simplemente por eventos catastróficos. En este sentido se deben realizar esfuerzos para asegurar la exactitud y propiedad de la información en todo momento.

c) Disponibilidad:

La disponibilidad de la información 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 calamidades.

d) Autenticidad:

La autenticidad también permite proteger la información del acceso por parte de personas no autorizadas. Con ésta se busca asegurar que la persona quien dice ser

el que está requiriendo el acceso sea la persona verdadera. Una amenaza muy importante en una red de computadoras viene dada por personas mal intencionadas que intentan hacerse pasar por las personas que tienen autorización de entrada a la red violando de esta forma la seguridad de la información. Es por ello que, otro objetivo imprescindible de un sistema de seguridad es impedir ese tipo de falsificación.

1.2.3. Políticas de Seguridad de Redes

Antes de instalar un sistema de protección, es importante entender con exactitud qué recursos de la red y servicios se desean proteger. Las políticas de seguridad se plasman en un documento que describe los asuntos de seguridad de red de una organización.

El diseño de las políticas de seguridad debe realizarse de tal manera que no disminuya la capacidad operativa de la organización. Unas políticas que eviten que los usuarios cumplan con sus tareas en forma efectiva, puede tener consecuencias indeseables ya que los usuarios podrán encontrar formas de ignorarla y convertirla en algo inútil. Para que las políticas de seguridad de red sean efectiva, los usuarios y administradores de red deben poder aceptarlas y estar dispuestos a reforzarlas.

Para desarrollar las políticas se analizan con detenimiento varios aspectos, los cuales se resumen en la realización de un análisis de riesgos, que contempla identificar los recursos que se desean proteger, establecer de qué se requieren proteger, analizar la factibilidad de las amenazas, identificar la importancia del recurso y, al final, estudiar las medidas que se pueden implantar para proteger los bienes de una manera económica y oportuna.

Normalmente, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad.

Las políticas de seguridad deben examinarse con frecuencia para verificar si sus objetivos y circunstancias han cambiado. Un aspecto importante de las políticas de seguridad de red es asegurarse de que todas las personas involucradas conozcan sus responsabilidades para mantener la seguridad.

Entre los aspectos que incluyen las políticas de seguridad están: el control de acceso a los recursos, los procedimientos utilizados para la creación de cuentas de usuario, asignación de permisos, procedimientos utilizados para la creación de contraseñas, entre otros. En general, en éstas se definen los derechos y responsabilidades de los usuarios al utilizar los recursos y servicios de la red, así como el límite hasta dónde los administradores del sistema deben examinar los datos y archivos privados de los usuarios para el diagnóstico de problemas del sistema y para investigar violaciones de seguridad. A su vez, es necesario establecer lineamientos sobre la protección a la privacidad de los empleados, la cual no se debe limitar al correo electrónico y debe abarcar otros medios tales como discos duros, cintas y documentos en papel.

1.3. Análisis y Gestión de Riesgos

El objetivo de la Seguridad de los Sistemas de Información (SSI) es mantener la confidencialidad, integridad y disponibilidad de la información. Una violación de la seguridad es cualquier suceso que compromete estos objetivos. El análisis y gestión de riesgos es un método formal para investigar los riesgos de un Sistema de Información (SI) y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

En toda evaluación de riesgos deben tenerse en cuenta tres costos o valores fundamentales:

- Cr: Valor de nuestro sistema informático, esto es, de los recursos y la información a proteger.
- Ca: Costo de los medios necesarios para romper las medidas de seguridad establecidas en nuestro sistema.
- Cs. Costo de las medidas de seguridad.

Para que la política de seguridad de nuestro sistema sea lógica debe cumplirse la siguiente relación:

Ca > Cr > Cs

El que Ca sea mayor que Cr significa que el ataque a nuestro sistema debe ser más costoso que su valor. Así, los beneficios obtenidos de romper nuestras medidas de seguridad no deben compensar el costo de desarrollar el ataque.

El que Cr sea mayor que Cs significa que no debe costar más proteger la información que la información protegida. Si esto ocurriese, nos resultaría más conveniente no proteger nuestro sistema y volver a obtener la información en caso de perdida.

1.3.1. Evaluación del valor del sistema informático (Cr).

Al evaluar nuestro sistema informático, su valor puede desglosarse en dos partes fundamentales:

- El valor intrínseco del producto a proteger.
- Los costos derivados de su pérdida.

En resumen, aunque en principio pueda parecer fácil la valoración de los bienes protegidos, pueden existir numerosos costos ocultos inherentes a su pérdida o compromiso que sólo un análisis detallado puede revelar y que a menudo requieren una valoración por alguien con experiencia en seguridad en conjunción con expertos especializados en el tratamiento de los bienes protegidos.

1.3.2. Vulnerabilidad, amenazas y contramedidas

Hay tres conceptos que entran en discusión cuando se habla de la seguridad de un sistema informático: vulnerabilidad o inseguridad (*vulnerability*), amenazas (*threat*) y contramedidas (*countermesures*).

Vulnerabilidad.

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

Amenaza.

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, ...), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Contramedida.

Técnicas de protección del sistema contra las amenazas. La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que:

"No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

1.3.3. Tipos de vulnerabilidad

La seguridad es la facultad de estar a cubierto de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de lograr, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido el sistema. Lo que se manifiesta en los sistemas no es la seguridad, sino más bien la inseguridad o vulnerabilidad. No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos. Algunos tipos de vulnerabilidad de un sistema son los siguientes:

Vulnerabilidad física.

Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.

Vulnerabilidad natural.

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallas eléctricas o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tomar en cuenta.

Vulnerabilidad del hardware y del software.

Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Ciertas fallas o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos confiable. En este apartado se incluyen todos las vulnerabilidades publicadas en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.

Vulnerabilidad de los medios o dispositivos.

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

Vulnerabilidad por emanación.

Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios para interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las comunicaciones.

La conexión de los computadores a redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones como son:

- Penetrar al sistema a través de la red.

- Interceptar información que es transmitida desde o hacia el sistema.

Vulnerabilidad humana.

La gente que administra y utiliza el sistema representa la mayor vulnerabilidad del sistema. La seguridad del sistema descansa sobre el administrador del mismo que tiene acceso al máximo nivel y sin restricciones al mismo.

Los usuarios del sistema también suponen un gran riesgo al mismo. Ellos son los que pueden acceder al mismo, tanto físicamente como mediante conexión. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados son debidos a los usuarios de los mismos.

Por todo ello hay una clara diferenciación en los niveles de los distintos tipos de vulnerabilidad y en las medidas a adoptar para protegerse de ellos.

1.3.4. Tipos de amenazas

Las amenazas al sistema informático pueden también clasificarse desde varios puntos de vista. En una primera clasificación según el efecto causado en el sistema, las amenazas pueden englobarse en cuatro grandes tipos: intercepción, modificación, interrupción y generación. Vamos a verlas con más detalle.

Intercepción.

Cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Ejemplos:

- Escucha de una línea de datos.

- Copias de programas o archivos de datos no autorizados.

Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

Modificación.

Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en todo o en parte su contenido o modo de funcionamiento. Ejemplos:

- Cambiar el contenido de una base de datos.
- Cambiar líneas de código en un programa.
- Cambiar datos en una transferencia bancaria.

Interrupción.

Interrumpir mediante algún método el funcionamiento del sistema. Pudiendo ser intencionada o accidental. Ejemplos:

- Saturar la memoria o el máximo de procesos en el sistema operativo.
- Destruir algún dispositivo hardware.

Generación.

Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema. Ejemplos:

- Añadir campos y registros en una base de datos.
- Añadir código en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.

La vulnerabilidad de los sistemas informáticos es muy grande, debido a la variedad de los medios de ataque o amenazas. Fundamentalmente hay tres aspectos que se ven amenazados: el hardware (el sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.) y los datos.

Desde el punto de vista del origen de las amenazas, estas pueden clasificarse en: naturales, involuntarias e intencionadas.

Amenazas naturales o físicas.

Son las que ponen en peligro los componentes físicos del sistema. En ellas podemos distinguir por un lado los desastres naturales, como las inundaciones, rayos o terremotos, y las condiciones medioambientales, tales como la temperatura, humedad, presencia de polvo.

Entre este tipo de amenazas, una de las más comunes es la presencia de un usuario sentado delante del computador con su lata de bebida refrescante y su bocadillo cerca del teclado o la unidad central.

Amenazas involuntarias.

Son aquellas relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad. Entre las más comunes podemos citar:

- Borrar sin querer parte de la información,
- Dejar sin protección determinados archivos básicos del sistema
- Dejar pegado a la pantalla un post-it con el password u olvidar salir del sistema.

Amenazas intencionadas.

Son aquellas procedentes de personas que pretenden acceder al sistema para borrar, modificar o robar la información; para bloquearlo o por simple diversión.

Los causantes del daño pueden ser de dos tipos: internos y externos. Los externos pueden penetrar al sistema de múltiples formas:

- Entrando al edificio o accediendo físicamente al computador.
- Entrando al sistema a través de la red explotando las vulnerabilidades software del mismo.
- Consiguiendo acceder a través de personas que tienen acceso de modo autorizado.

Los internos pueden ser de tres tipos: empleados despedidos o descontentos, empleados coaccionados, y empleados que obtienen beneficios personales.

1.3.5. Tipos de medidas de seguridad o contramedidas

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, etc., porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variadas. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los

riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación o través de una serie de medidas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. A continuación se describen cada una de estas:

Medidas físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas
- Los daños físicos por parte de agentes nocivos o contingencias
- Las medidas de recuperación en caso de fallas

Concretando los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc....)
- Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)
- Vigilancia (cámaras, guardias jurados, etc.)

- Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.)
- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- Control de la entrada y salida de material (elementos desechables, consumibles, material anticuado, etc.)

Medidas lógicas

Incluye las medidas de acceso a los recursos, a la información y al uso correcto de los mismos, así como la distribución de las responsabilidades entre los usuarios. Se refiere mas a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la criptografía para proteger los datos.
- Uso de cortafuegos para proteger una red local de intrusos desde Internet.
- Definición de una política de copias de seguridad.

- Definición de una política de monitorización (logging) y auditoria (auditing) del sistema.

Medidas administrativas

Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
- Establecimiento de un plan de formación del personal.
- Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento son fundamentales para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.
- Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.
- Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

- Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas legales

Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.

Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales. Un ejemplo de este tipo de medidas es la Ley de Mensajes de Datos y Firmas Electrónicas. Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medidas de seguridad para su protección y las penalizaciones a imponer en caso de su incumplimiento.

1.3.6. Planes de contingencia

Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. La mayor parte de las medidas se refieren a la prevención ante posibles amenazas. Sin embargo, ningún sistema es completamente seguro, y por tanto hay que definir una estrategia a seguir en caso de fallas o desastre.

La clave de una buena recuperación en caso de fallas es una preparación adecuada. Por recuperación se entiende tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo habiendo reemplazado o recuperado la mayor cantidad de recursos e información.

La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada, mientras la recuperación del funcionamiento del sistema se basa en la preparación de unos recursos alternativos.

Dependiendo del tipo de compañía puede ser necesario recuperar el funcionamiento en un plazo más o menos breve. Todo depende del uso que se haga del sistema y de las perdidas que suponga no tenerlo en funcionamiento.

Las compañías pueden mantener o contratar dos tipos de instalaciones alternativas: frías (cold site) o calientes (hot site). Una instalación fría consiste en un lugar con las medidas de seguridad física disponibles, donde poder instalar el hardware y el software y funcionar en menos de una semana. Una instalación caliente incluye además computadores, periféricos, líneas de comunicaciones y otros medios e incluso personal para volver a funcionar en unas pocas horas.

1.4. Principios fundamentales de la Seguridad Informática

En el ámbito de la seguridad informática existen una serie de principios básicos que es necesario tener en cuenta al diseñar cualquier política de seguridad. A continuación se presentan algunos de los casos fundamentales:

Principio de menor privilegio

Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más. Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

La seguridad no se obtiene a través de la oscuridad

Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corrijamos estableciendo las medidas de seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evita que se corrija.

Principio del eslabón más débil

En todo sistema de seguridad, el mayor grado de seguridad es aquel que tiene su eslabón más débil. Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Defensa en profundidad

La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que este sea, sino que es necesario establecer varios mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Punto de control centralizado

Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.

Seguridad en caso de fallo

Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario que dejen pasar a cualquiera aunque no esté autorizado.

Participación universal

Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.

Simplicidad

La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallas. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

2. El perfil de un Hacker

Un Hacker es a todas luces, alguien con profundos conocimientos sobre una tecnología. Esta puede ser la informática, electrónica o comunicaciones. El Hacker normalmente conoce todos los terrenos en los que reposa la actual tecnología. Así pues, el verdadero Hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta más difícil de descifrar como sistemas de

cifrado o sistemas de codificación. En la actualidad los sistemas de cifrado y codificación están al orden del día, tomemos como ejemplo los canales de televisión de pago o cualquier soporte de grabación de datos como el CD o DVD.

Cada uno de estos dispositivos se basa en un estándar de codificación de datos, al igual que sucede con el protocolo de comunicaciones de Internet TCP/IP. En la actualidad y más en el futuro, la tecnología se basa en protocolos y datos correlacionados en cadena. El entendimiento de estas cadenas de datos nos dará una superioridad de control sobre cualquier tecnología. Este entendimiento nos permitirá entre otras cosas, modificar la información, un reto para todo Hacker. Así un Hacker busca, primero el entendimiento del sistema tanto de hardware como de software y sobre todo descubrir el modo de codificación de las órdenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema.

El perfil del Hacker no es el típico hombre que vive solo y para los computadores, aunque si es cierto que pasa largas horas delante de él. Los conocimientos que adquiere el Hacker los difunde, para que otros sepan como funciona realmente la tecnología.

Otros datos erróneos sobre la descripción del Hacker, es aquella que los presenta como adolescentes de gafas negras de montura de hueso y extendido acné sobre su cara, en la mayoría estudiantes de informática de cuerpos endebles que siempre consumen refrescos y pizzas. Esto es totalmente incierto, el Hacker puede ser adolescente o adulto, lo único que los caracteriza a todos por igual, son las ansias de conocimientos.

Tampoco es cierto que el Hacker surge a raíz de la nueva era de la informática, ya que Hacker es aquel que trata de averiguar cosas y esto se puede aplicar en las

comunicaciones que existieron mucho antes que los computadores. De modo que se desmiente que los Hackers tengan una edad temprana. Ya en la segunda guerra mundial se trataba de descifrar los mensajes del enemigo. Sin embargo, también es cierto que es ahora, cuando más proliferación de Hackers existe, dado la importancia que cobra la informática y la red de Internet hoy en día. Por otro lado en la actualidad existe más información al respecto a través de la prensa y WEB en la red.

Los verdaderos Hackers aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes.

2.1. La nueva cybersociedad

A raíz de la introducción de la informática en los hogares y los avances tecnológicos que esta aporta, ha surgido toda una generación de personajes más o menos peligrosos que difunden el miedo en la Internet y la prensa.

Catalogados todos ellos como ***"piratas informáticos"*** la nueva generación de ***"rebeldes"*** de la tecnología aportan unos, sabiduría y enseñanza, y otros difunden destrucción y desolación. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

Hasta la fecha esta nueva cybersociedad, ha sido dividida en una decena de grandes áreas fundamentales en las que reposan con fuerza, la filosofía de cada uno de ellos.

Todos y cada uno de los grupos aporta en gran medida algo bueno en un mundo dominado por la tecnología, pero esto, no siempre sucede así. Algunos grupos rebeldes toman estas iniciativas como partida de sus actos rebeldes.

Los hackers son el principio y el nivel más alto de toda esta nueva sociedad. Estos poseen mayores conocimientos que el resto de grupos, pero emplean metodologías poco agresivas para mostrar sus conocimientos. Los Crackers son probablemente el siguiente escalón, ya que son capaces de Crackear sistemas y romper su seguridad, extendiendo el terror entre fabricantes y programadores de Software. Los Lamers, auténticos curiosos aprendices, poseen mayor influencia en la red a través de WEB, por eso se debe tratar cada grupo por separado. A continuación se describen conceptualmente los protagonistas de los delitos informáticos:

- ***Hackers:*** el primer eslabón de una sociedad "delictiva" según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos.

  Les encanta entrar en computadores remotos, con el fin de decir aquello de "he estado aquí" pero no modifican ni se llevan nada del computador atacado.

  Normalmente son quienes alertan de una falla en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

  Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de virus o crack de un software o sistema informático.

- ***Crackers:*** es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas.

  Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Internet para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

  En la actualidad es habitual ver como se muestran los cracks de la mayoría de software de forma gratuita a través de Internet. El motivo de que estos cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.

  Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de software y hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

- ***Lamers:*** este grupo es quizás el que mas número de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en la Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la

posibilidad de girar un gráfico en la pantalla de otro computador, le fascinan enormemente.

Este es quizás el grupo que más peligro representa en la red ya que ponen en práctica todo el software de hackeo que encuentran. Así es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se dice auto denominándose Hacker.

También emplean de forma habitual programas sniffers, interceptan tu contraseña y correo electrónico y después envían varios mensajes, con dirección falsa amenazando los sistemas, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el computador esta apagado. Toda una negligencia en un terreno tan delicado.

- ***Copyhackers:*** es una nueva raza solo conocida en el terreno del crackeo de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año más de 25.000 millones de pesetas sólo en Europa.

  En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los "bucaneros" personajes que serán detallados mas adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

- ***Bucaneros:*** son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "Crackeados" pasan a denominarse "piratas informáticos". En este sentido, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de cracking a un nivel masivo.

- ***Phreaker:*** este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

- ***Newbie:*** es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los Lamers,

los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

- ***Script Kiddie:*** denominados Skid kiddie o Script kiddie, son el último eslabón de los clanes de la red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack en su estado puro. En realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la red y después los ejecutan sin leer primero los archivos Readme de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propio computador. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los "pulsabotones" de la Internet. Los Kiddies en realidad no son útiles en el progreso del Hacking.

Se ha descrito brevemente cada grupo, quedado claro quienes son cada uno de ellos y que papel interpretan en la nueva cibersociedad. Son cada vez más los jóvenes que se autodenominan Hackers y lo único que hacen es soltar virus y probar programas de Hacking. Esto confunde a la sociedad y este tipo de personas si son algo violentas y adolecen lo material. Disfrutan "fastidiando" al vecino y muestra una cara de idiota brillando bajo la luz de la bombilla, cuando suelta uno de esos fatídicos virus o gusanos en la Internet. Los buenos Hackers, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema demasiado seguro.

2.2. Vulnerabilidades y Riesgos

2.2.1. Virus, Caballos de Troya y Bombas Lógicas

Además de los peligros que amenazan la seguridad física de las redes (es decir el hardware), existen en la actualidad los peligros que amenazan la integridad de los datos (es decir el software). Entre estos, los de mayor preocupación son los denominados *virus informáticos* y sus semejantes (caballos de Troya, bombas lógicas). En este capítulo se estudian algunas de sus características y los daños que pueden producir, mientras que en el siguiente capítulo se analizan en detalle las medidas de protección.

En general, tiende a asociarse el virus informático con la idea genérica que tenemos del virus biológico, pero se debe considerar que la palabra *virus* procede del latín y significa *veneno*. Así, en sentido amplio, se considera virus a cualquier programa que produzca efectos indeseables en la computadora. Atendiendo a esta definición, podríamos establecer dos categorías de virus: Los que son capaces de reproducirse, (que son los virus más puros en sentido estricto) y los que son incapaces de reproducirse.

Los primeros son muy variados y se transmiten por sus propios medios de una computadora a otra, bien a través de las redes o a través de diskettes, ya que un concepto inherente a los virus es su capacidad de contagio.

.La llegada de los virus ha traído consigo una auténtica terminología propia y definiciones como caballo de Troya, bomba de tiempo, polilla, gusano, etc., son actualmente términos genéricos usados en el sublenguaje informático. Esta terminología obedece a la forma de actuar de los virus:

- ***Caballos de Troya***: se refiere a aquellos virus que entran en la computadora "disfrazados de una aplicación inocente", pero que están esperando determinadas circunstancias para atacar. Estas circunstancias pueden ser de lo más variadas: podría ser un contador de las veces que el programa se ha ejecutado, la introducción de determinada cifra o dato, etc. Un caballo troyano puede, desde su aparente inocencia, destrozar archivos a los que teóricamente no debe tener acceso, mientras que la causa se busca en los programas que sí tienen acceso legítimo a esos archivos. También es frecuente el que aparezcan falsas versiones nuevas de programas conocidos que en realidad son caballos troyanos de acción fulminante. La forma más burda de caballo troyano es el programa cuya simple ejecución por primera vez, y sin ninguna condición, provoca el ataque.

- ***Bombas de tiempo***: son aquellas que explotan un día exacto. Las más conocidas son las que lo hacen los viernes y trece, los veinticinco o treinta y uno de diciembre, y el dos de marzo (en el caso de los Macintosh de Apple). En general, buscan que la fecha tenga algún significado, aunque en otras se trata simplemente de un plazo de meses o años.

- ***Gusanos:*** son programas que tienen como finalidad su propagación mediante la clonación de sí mismos, bien en la memoria del computador o a través de una red. Sus efectos suelen ser la saturación del sistema por la cantidad de recursos que consumen. Ejemplos recientes son Happy99 y Melissa.

2.2.2. Cookies y Spams

El HTTP (*Hypertext Transfer Protocol*) es el protocolo en que se basa la conexión y transferencia de información entre navegadores y servidores Web. Uno de sus principales inconvenientes es que es un protocolo sin estados, es decir no memoriza ni conserva información sobre anteriores conexiones del usuario. Se han desarrollado varias técnicas para evitar este inconveniente y posiblemente la más conocida y utilizada es la de los *Cookies*.

Un Cookie no es más que una cadena de información que el servidor nos envía acompañando a la página Web que hemos solicitado, y que el navegador se encargará de grabar en un archivo de texto de nuestro disco duro. De esta manera el servidor en próximas conexiones podrá acceder a esta información y por tanto recordar acciones que hemos realizado en anteriores conexiones. Si deseamos ver estos archivos, en el caso de utilizar el navegador Netscape, no tenemos más que buscar el archivo "cookies.txt" y visualizarlo. En el caso de utilizar el Explorer, en el directorio Windows tenemos que buscar la carpeta Cookies y en ella encontraremos un archivo *.txt* por cada Cookie que hayamos recibido.

La forma de utilizar e implementar estos Cookies, no es en absoluto complicada, y se puede realizar de varias maneras, por ejemplo con programas CGIs y Javascript.

Por lo que se refiere a los *Spam*, se trata de un mensaje de correo que se envía a muchos grupos de usuarios o listas de correo, o que se envía repetitivamente a un mismo usuario o lista. Por ejemplo, el mensaje que pedía enviar otro mensaje a la sociedad anticancerosa genera un spamming a la dirección de correo indicada.

2.2.3. Negación de Servicio DoS

Un ataque de negación de servicio es uno en el que una actividad o proceso

consume de tal manera los recursos compartidos (por ejemplo, CPU, memoria o ancho de banda), que no deja nada para otros usuarios o usos. Aunque las computadoras mainframe tenían algunas defensas contra los ataques de negación de servicio, los sistemas de cómputo modernos son notoriamente pobres para repeler tales ataques.

Combatir ataques de negación de servicio es difícil. Esto se debe a que sin importar cuántas formas se encuentren para resolver el problema, los atacantes inteligentes tal vez encontrarán algún otro modo de afectar el sistema. Sin embargo, la experiencia muestra que hay formas de reducir el impacto de los ataques de negación de servicio y la mayoría de las veces son el resultado de errores de programación, más que de atacantes.

2.2.4. Técnicas de ataques comunes

Actualmente los hackers disponen de una amplia variedad de herramientas para efectuar sus ataques contra las redes. Por lo que se refiere a los sistemas que operan bajo ambiente TCP/IP, existen algunas técnicas que son muy utilizadas y que se mencionan brevemente a continuación:

- **Ping sweep** (barrido de ping): como el mismo nombre sugiere, mediante esta técnica un intruso envía un *ping* a una serie de direcciones IP. Un ping es la solicitud de "eco" contenida en mensajes ICMP (Internet control message protocol). El objetivo es encontrar máquinas a las cuales se les puedan detectar vulnerabilidades para luego penetrarlas. Una variación de esta técnica utiliza una serie aleatoria de direcciones IP para hacer más difícil su descubierto.

- **Port scan** (escaneo de puerto): una vez que el hacker sabe que una máquina está viva, su próximo paso probablemente sea el determinar cuáles servicios

están disponibles. En las máquinas hay procesos que están "escuchando", es decir, monitoreando, los puertos TCP y UDP esperando solicitudes por parte de los usuarios. Si hay una respuesta en un determinado puerto, el intruso puede aprovecharse de ciertas vulnerabilidades conocidas para determinados servicios.

- **Dig** (excavar): una buena fuente de información sobre la red que se quiere atacar son los servidores DNS (domain name system). Dig es una herramienta común que se encuentra en la mayoría de los sistemas Unix y puede usarse para copiar un banco de datos entero desde cualquier servidor DNS.

- **SYN flood** (inundación de SYN): con esta técnica no se pretende penetrar en una máquina, sino más bien saturarla a fin de impedir que preste servicio a los usuarios legítimos. Se trata de una clase de ataque conocida como denial-of-service (negación de servicio). El bombardeo de SYN probablemente es el más conocido de estos ataques y consiste en enviar un flujo continuo de solicitudes de establecimiento de conexiones TCP mediante mensaje SYN de sincronismo. En efecto, cuando una máquina cliente establece una conexión TCP con un servidor, hay un intercambio de mensajes iniciales. El cliente envía un mensaje SYN, el servidor contesta con un mensaje SYN-ACK y por último el cliente manda un mensaje ACK estableciéndose así la conexión. Pero el intruso no completa la secuencia correcta del protocolo, ya que no envía el SYN-ACK luego que la máquina le contesta, por lo que la máquina queda con un gran número conexiones TCP semiabiertas, así que finalmente no puede abrir más de ellas. Este ataque produce una saturación de memoria por creación de conexiones incompletas TCP y afecta a todos los servicios de red del sistema.

- **ICMP flood** (inundación ICMP): este es el ataque de negación de servicio más directo, ya que una máquina recibe tantos pings que no puede manejar el resto de tráfico.

- **UDP flood** (inundación UDP): UDP es un protocolo de tipo connectionless (sin conexión) ya que el receptor no confirma la recepción de los paquetes. Además, debido a que no se establece ninguna conexión antes de enviar los paquetes, el bombardeo de una máquina con paquetes UDP hace que al emisor no lo puedan bloquear. Un hacker podría lanzar un ataque de negación de servicio enviando paquetes UDP a un puerto que no se use. La máquina responderá con un mensaje "ICMP port unreachable" (puerto ICMP no accesible) por cada paquete UDP enviado. Si se envían muchos paquetes UDP, la máquina se bloqueará (también pueden quedar bloqueadas las máquinas en el mismo segmento compartido debido a la cantidad de tráfico).

- **Ping of Death** (ping de la muerte): esta técnica consiste en enviar un paquete de ping ilegalmente grande que inunda los buffers de la máquina atacada, haciendo que se cuelgue. Muchos sistemas Unix, Windows NT y routers eran vulnerables a este ataque cuando fue descubierto hace un par de años, y si bien los fabricantes rápidamente elaboraron parches, todavía existen muchas máquinas indefensas en las organizaciones.

- **Land** (tierra): técnica que es usada para lograr que una máquina se cuelgue “land attack”, donde se envían paquetes con idénticos números de puerto e idénticas direcciones IP de origen y destino. Este ataque tiene variantes, por ejemplo fuentes idénticas pero ausencia del número del puerto.

- **Supernuke**: un ataque específico a Windows es supernuke (también conocido como winnuke), el cual causa que se bloqueen las máquinas que escuchan al puerto 139 UDP.

- **Teardrop** (lágrima): esta técnica de ataque consiste en activar la bandera "urgente" en el header (encabezamiento) del fragmento de un mensaje TCP. Algunas implementaciones del protocolo TCP/IP no logran ensamblar correctamente los fragmentos que se solapan, causando que el sistema se cuelgue. El sistema Windows NT 4.0 es particularmente afectado, incluso si se aplica del Service Pack 3. Un parche salió a la luz pública en enero de 1998.

- **Tojan horse** (caballo de Troya): es un programa que imita la ejecución de otro programa, pero realiza funciones completamente distintas a las esperadas, permitiendo al intruso tomar el control de la máquina remotamente, abriendo algún puerto en el sistema.

- **Spoofing** (falsificación): se trata de falsificar el origen de los mensajes para que aparenten venir de otra fuente. Existen dos ataques tipo spoofing: IP Spoofing y DNS Spoofing. El primero de ellos se hizo famoso al usarlo Kevin Mitnick en su ataque en Diciembre de 1995 a la red informática de Tsutomu Shimomura, un especialista en seguridad que trabajaba en el Centro de Supercomputación de San Diego.

  El ataque DNS Spoofing consiste en la manipulación de paquetes UDP para así comprometer el cache del servidor de nombres (DNS). Si se permite el método de recursión en la resolución de "nombre < - - > dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una

petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método típico de funcionamiento.

- **Spamming** (bombardeo de e-mail): es un ataque que utiliza el servicio de correo electrónico y consiste en mandar múltiples mensajes a una dirección particular. El spamming puede dañar aún más si los destinatarios contestan ese e-mail, causando que todas las direcciones originales reciban esa contestación. Esto puede ocurrir de forma inocente, resultado de mandar el mensaje a listas de correo y esas listas multiplican ese mensaje. El spamming puede combinarse con el spoofing para ocultar la procedencia del mensaje.

2.3. Medidas de Protección

2.3.1. Firewall, Muro de Seguridad o Cortafuegos:

Se puede definir de una forma simple un firewall, como aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre 2 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 de firewalls:

- Nivel de red (o packet filter).
- Nivel de aplicación (o application gateway).
- Inspección de paquetes (stateful inspection).

Los firewalls a nivel de red generalmente toman las decisiones basándose en la fuente, dirección de 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.

Los Firewalls a nivel de aplicación son generalmente hosts 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 firewall a nivel de aplicación se puede usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos firewalls a nivel de aplicación son bastante transparentes. Estos tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto es lo que los hace diferenciarse de los firewalls a nivel de red.

Los 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 sólo filtran los paquetes, sino también consideran el contenido y la dirección. Los firewalls de este tipos 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 efectivo en el rendimiento respecto a los firewalls de aplicación.

Adicional a lo anterior, también se toma en cuenta el estado ("*state")* de las conexiones que manejan. Por ejemplo, un paquete legítimo que entra puede ser correspondido con un requerimiento de salida por el paquete y permitir su establecimiento. Inversamente, un paquete de entrada como respuesta a un requerimiento de salida no existente puede ser bloqueado. Esto va más allá de un simple filtrado de paquete, y a esta tecnología se le conoce con el nombre de "*stateful inspection"* la cual se vale comunicaciones previamente establecidas para permitir otras que están en su intento de conexión. En consecuencia, generalmente puede manejar paquetes más rápidos que los de aplicación.

Otra facilidad de este tipo de firewall es que puede esconder direcciones internas y trasladar éstas a direcciones públicas (NAT & hiding), así como también otros servicios como detecteción de virus, tal y como en los firewalls de aplicación.

2.3.2. Redes Privadas Virtuales (Virtual Private Network VPN)

Una conexión entre redes basada en Redes Privadas Virtuales (Virtual Private Network, VPN), usa la infraestructura distribuida y abierta de Internet o una infraestructura IP, Frame Relay o ATM de un proveedor de servicio para transmitir datos entre sitios de la corporación de una forma segura.

Las VPN se comportan como *túneles encriptados* a través de medios compartidos para transmitir información privada entre sitios. Proporcionan un modo de construir una red de área extendida a escala global con un costo muy inferior a

hacerlo con redes privadas.

Básicamente, la tecnología VPN conforma un canal de comunicaciones encriptadas seguro a través del medio compartido para oficinas remotas, usuarios móviles y socios comerciales. La VPN necesita proveer cuatro funciones críticas para garantizar la seguridad de los datos:

- Autenticación, asegurando que el usuario que desea conectarse a la red es quien dice ser.
- Control de acceso ó autorización, restringiendo el acceso a la red y a los recursos de los usuarios no autorizados.
- Confidencialidad, previniendo que alguien copie los datos que viajan a través de la Internet.
- Integridad, asegurando que los datos no han sido alterados durante la transferencia.

2.3.3. Programas Antivirus

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

- ***Vacunas*****,** que 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.

- ***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, etc...).

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

- ***Chequeadotes,*** 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 alertar al usuario.

Algunas formas de protección no requieren programas especializados, sino que se pueden tomar con las facilidades que proporciona el 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 3½"), 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. No obstante, no abuse de las vacunas

protectoras; piense que una vacuna instalada al máximo nivel de protección le pedirá permiso al formatear un diskette de alta densidad.

2.3.4. Sistemas de Detección de Intrusos

La detección de intrusos se puede llevar a cabo a partir de la caracterización anómala del comportamiento y del uso que se hace de los recursos del sistema. Este tipo de detección pretende cuantificar el comportamiento normal de un usuario. Para una correcta distinción hay que tener en cuenta las tres distintas posibilidades que existen en un ataque, dependiendo de quién lo lleva a cabo:

- ***Penetración externa*.** Que se define como la intrusión que se realiza desde otra red.
- ***Penetraciones internas*.** Son aquellas que llevan a cabo por usuarios internos que no están autorizados.
- ***Abuso de recursos*.** Se define como el abuso que un usuario lleva a cabo sobre datos o recursos de un sistema al que está autorizado su acceso.

La idea central de este tipo de detección es el hecho de que la actividad de intruso es un subconjunto de las actividades anómalas. Esto puede parecer razonable por el hecho de que si alguien consigue entrar de forma ilegal en el sistema, no actuará como un usuario normal. Sin embargo en la mayoría de las ocasiones una actividad de un intruso resulta del agregado de otras actividades individuales que por sí solas no constituyen necesariamente un comportamiento de intruso. Idealmente el conjunto de actividades anómalas es el mismo del conjunto de actividades de intruso, de todas formas esto no siempre es así:

- ***Actividades de intruso pero no anómalas.*** Se les denomina falsos negativos y en este caso la actividad es de intruso, pero como no es anómala, entonces no se consigue detectarla. Se denominan falsos negativos porque el sistema erróneamente indica ausencia de intrusión.

- ***Actividades no de intruso pero anómalas.*** Se denominan falsos positivos y en este caso no hay intruso, pero como es anómala, el sistema decide que es de intruso. Se denominan falsos positivos, porque el sistema erróneamente indica la existencia de intrusión.

- ***Actividades no de intruso ni anómalas.*** Son negativos verdaderos, la actividad es no intruso y se indica como tal.

- ***Actividades de intruso y anómalas.*** Se denominan positivos verdaderos, ya que la actividad es de intruso y además es detectada.

Los falsos negativos no son deseables, porque dan una falsa sensación de seguridad del sistema y el intruso en este caso puede operar libremente en el sistema. Los falsos positivos se deben de minimizar, en caso contrario lo que puede pasar es que se ignoren los avisos del sistema de seguridad, incluso cuando sean acertados. Los detectores de intrusiones anómalas requieren mucho gasto computacional, porque se siguen normalmente varias métricas para determinar cuánto el usuario se aleja de lo que se considera comportamiento normal.

Características deseables de un IDS

- Debe ser ligero, es decir su ejecución no debe cargar al sistema de una manera tal que le impida ejecutar otras tareas con relativa normalidad

- No debe ser una caja negra, es decir, que se sepa cómo funciona.

- Debe ser confiable y difícil de engañar (es decir que no detecte intrusos).
- Debe ser capaz de tolerar fallas, en el sentido de que pueda sobrevivir a una caída del sistema.

Clasificación de los IDS

Los IDS pueden clasificarse en base a varios aspectos: método de detección, tipo de monitoreo y forma de recolección y análisis de la información. Según el método de detección, los hay de detección de mal uso y detección de anomalías.

El modelo de detección de mal uso consiste en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las diferentes acciones que integran el mencionado proceso, comúnmente se denominan *patrones o firmas del ataque.*

Según el tipo de monitoreo, hay IDS con detección orientada al host o detección orientada a la red.

El modelo orientado al host se basa en el monitoreo y análisis de información, que refleja el estado del host donde reside el IDS. La mayoría de la información que este tipo de sistema recopila es obtenida a través del sistema operativo del host. Esto último causa complicaciones debido a que la información que se procesa no contiene registros del comportamiento, de bajo nivel, de la red.

Los IDS que utilizan el modelo orientado a red, fundamentan su monitoreo en información recolectada de la red. Generalmente esta información es capturada mediante mecanismos de *"sniffing*". El "sniffing" consiste en habilitar la interfaz de red en modo promiscuo para que así capture todos los paquetes que reciba, incluso aquellos que no le han sido destinados. En base al mecanismo antes expuesto, se

pueden definir patrones o firmas de ataques, según la estructura, información y ocurrencia de los paquetes.

2.3.5. 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 de 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 Oficial de Seguridad (Chief Security Officer, CSO), quién 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 Oficial de Seguridad (Chief Information Officer) 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 criterio que debe prevalecer en una gerencia de esta naturaleza.

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 implementación 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.

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 información de la compañía. Cada área funcional debe tener objetivos definidos, los cuales deben ser consistentes con los objetivos de 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 la 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 de seguridad de la organización, 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 bases 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 esta razón, dentro e 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 computadoras, 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 va a llevar a la organización de seguridad a un alto grado de cooperación con las funciones de Auditoría Interna y/o el departamento de Seguridad Física.

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

Funciones de las unidades que conforman la FSAI

Políticas, Estándares y Procedimientos

Una vez establecido el alcance de la FSAI, la cual provee una guía y experticia en la implementación de políticas de seguridad y estándares. La retroalimentación de los grupos asesores, los cambios en los requerimientos del negocio y avances de los requerimientos de seguridad deben proveer una retroalimentación continua para ayudar definir y mejorar las políticas de seguridad de activos de información.

Administración de Seguridad y Monitoreo

Las métricas son críticas para la evaluación del ambiente de seguridad de una organización. La FSAI debe monitorear y evaluar los procesos de seguridad y el perímetro de implantación de los mismos y junto con grupos asesores de seguridad deben revisar que los resultados cumplen con las metas en cuanto a seguridad de activos de información de la organización. Este nivel de colaboración crea un ambiente continuo de mejoras y posiciona la seguridad de la información como responsabilidad primaria de la organización y no como una función.

Soporte Técnico y Staff de Asistencia

No todas las áreas de la organización tienen la experticia para seleccionar, configurar, instalar y mantener el perímetro de seguridad de tecnología de información y procesos relacionados. El Soporte Técnico y Staff de Asistencia debe proveer un rango de servicios, desde la asistencia telefónica o en sitio para responder

interrogantes de seguridad de tecnología.

Entrenamiento en Seguridad a Usuarios Finales

El establecimiento y refuerzo de las comunicaciones de seguridad de la organización es fundamental. Esta comunicación puede tomar muchas formas; desde conferencias de seguridad de frecuencia anuales, comunicados de vulnerabilidades detectadas, análisis de reportes de debilidades, hasta entrenamientos en aspectos de seguridad de activos de información. Esta área de entrenamiento es el catalizador para aumentar los conocimientos en materia de seguridad de activos de información de las áreas que conforman la organización, tanto personal ejecutivo, técnico como administrativo.

Reporte de Incidentes y Análisis de Vulnerabilidades

Otra función de seguridad importante es la revisión y administración de los incidentes de seguridad. Este grupo activa el proceso de investigación de incidentes de seguridad. El objetivo de esta área es proporcionar una visión a futuro de las posibles brechas de seguridad y comunicar información preventiva a la organización.

2.4. Estadísticas sobre delitos informáticos

A continuación se presentan estadísticas globales relacionadas con delitos informáticos, las cuales son fuente de “ISM Product Survey”, “CSI – Computer Security Institute”, “CERT”, “FBI” y “PwC Global”:

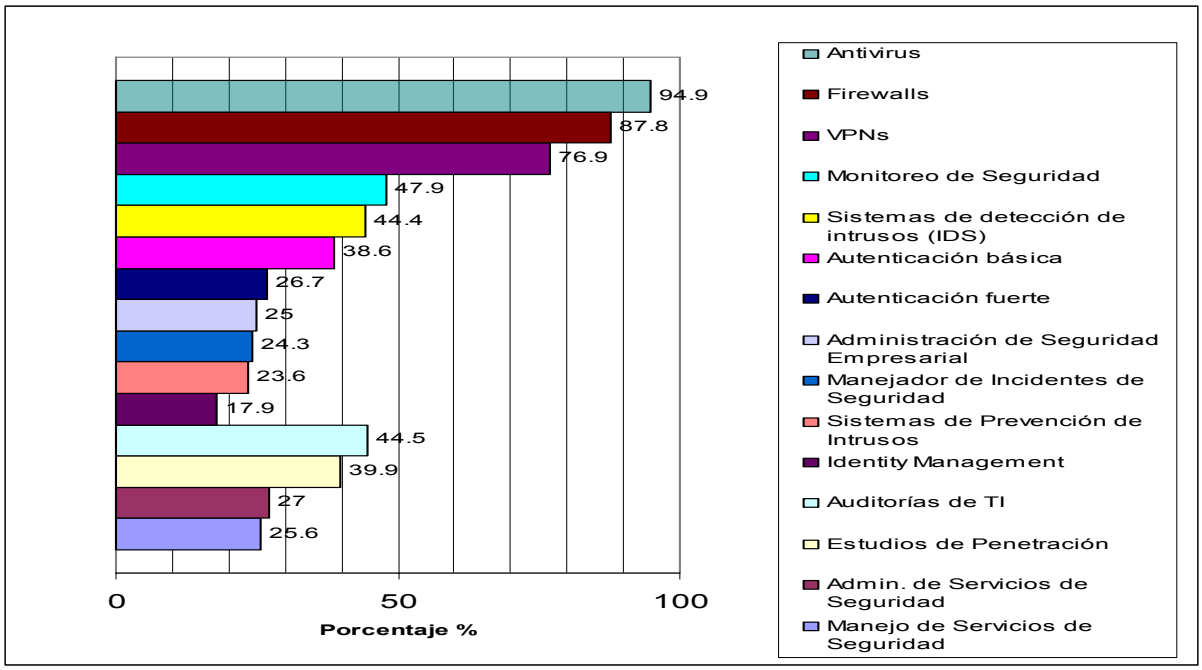

Figura N° 1. Porcentaje de utilización de mecanismos de seguridad – Fuente: 2003 ISM Product Survey

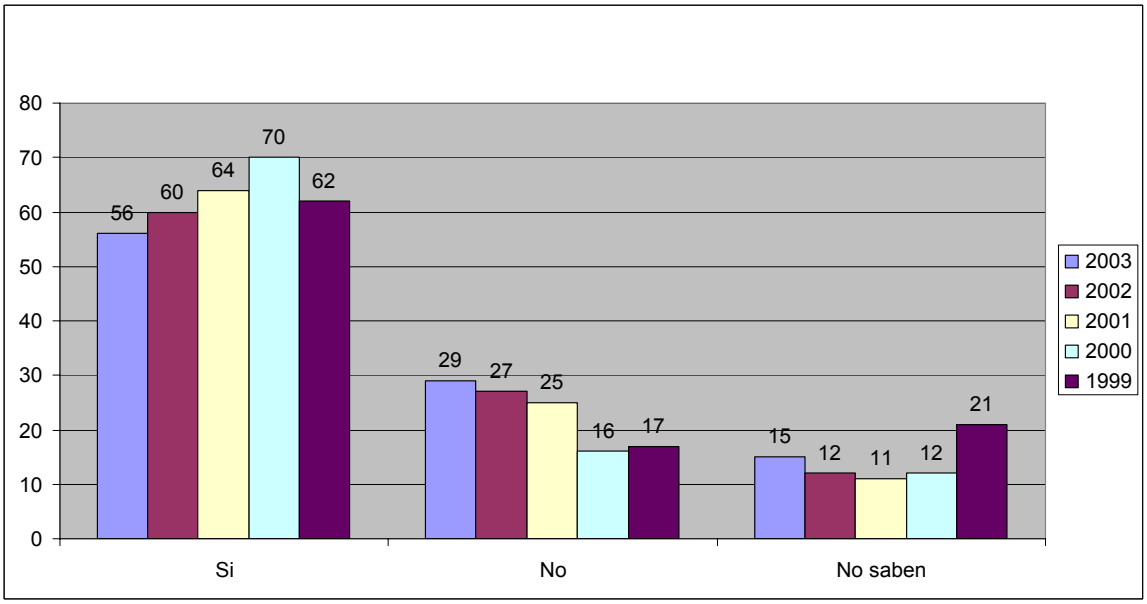

Figura N° 2. Uso no autorizado de sistemas en los últimos doce meses – Fuente: Computer Security Institute (CSI)

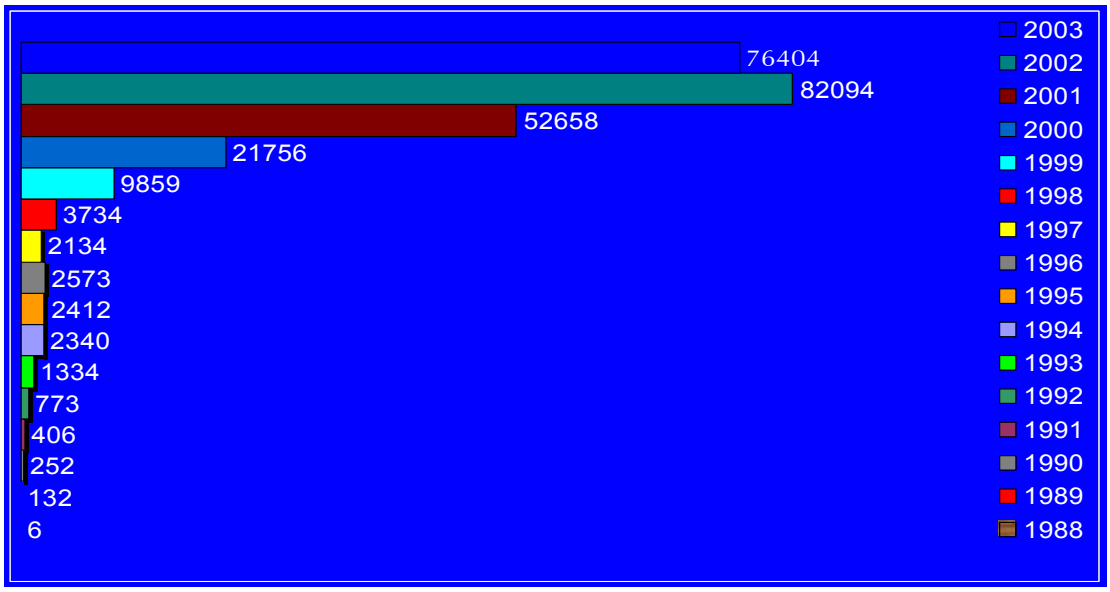

Figura N° 3. Incidentes reportados en el uso de la tecnología de información – Fuente: CERT Coordination Center (CERT/CC)

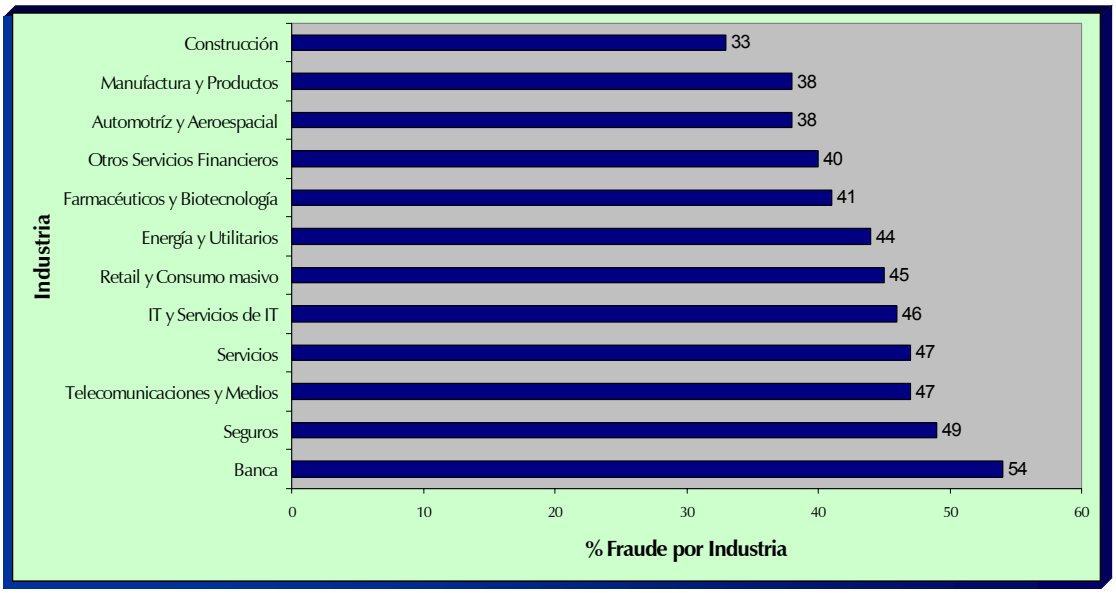

Figura N° 4. Porcentaje de víctimas de fraude por Industria – Fuente: PwC Global Economic Crime Report 2003

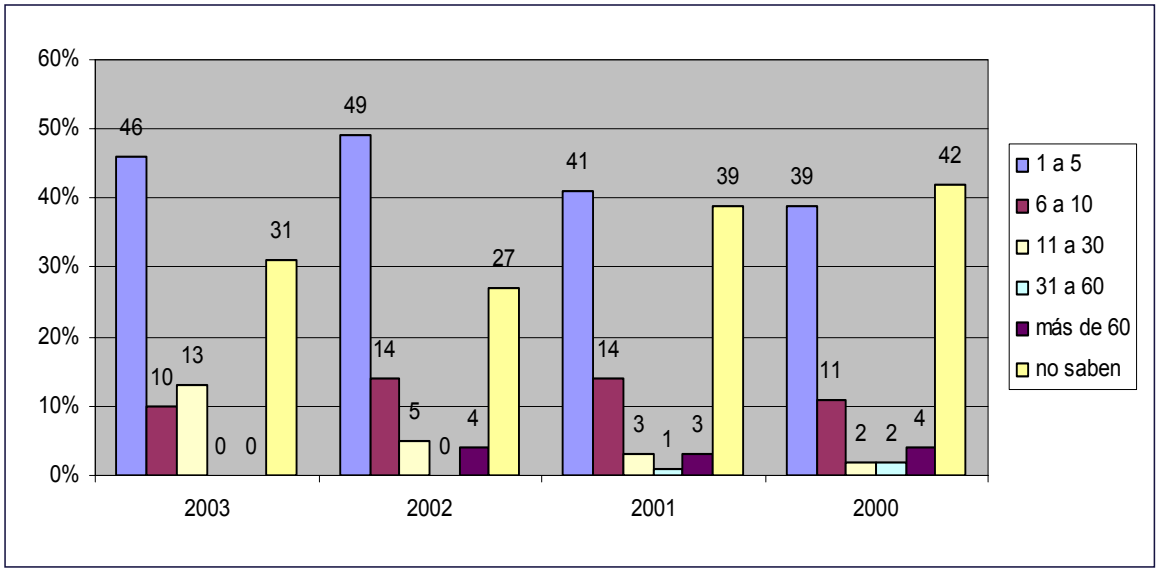

Figura N° 5. Número de incidentes desde fuera de la empresa – Fuente: Computer Security Institute (CSI)

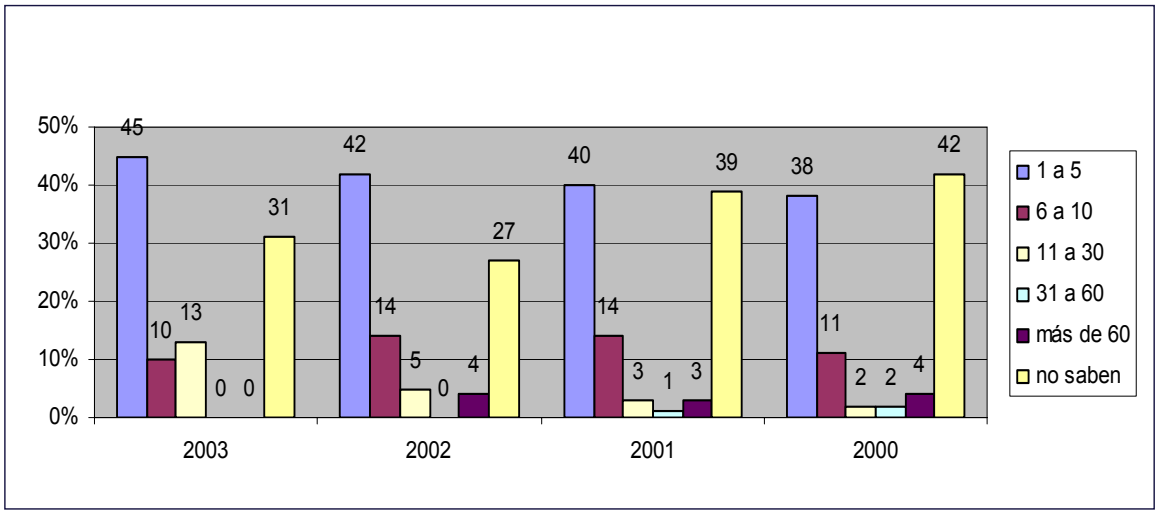

Figura N° 6. Número de incidentes desde dentro de la empresa – Fuente: Computer Security Institute (CSI)

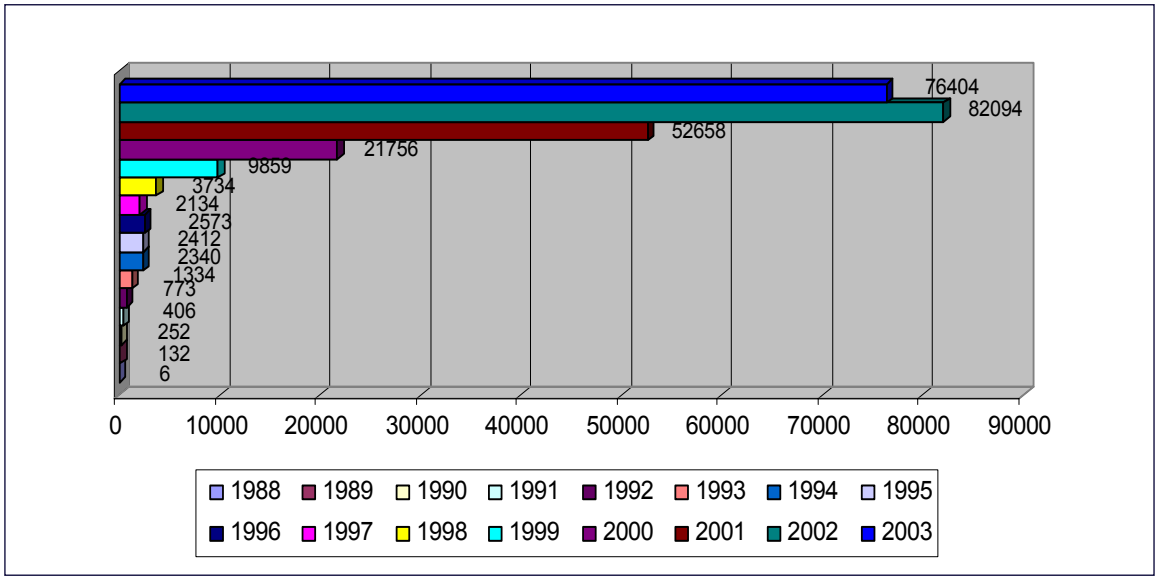

Figura N° 7. Incidentes reportados desde Internet – Fuente: CERT / Coordination Center (CERT/CC)

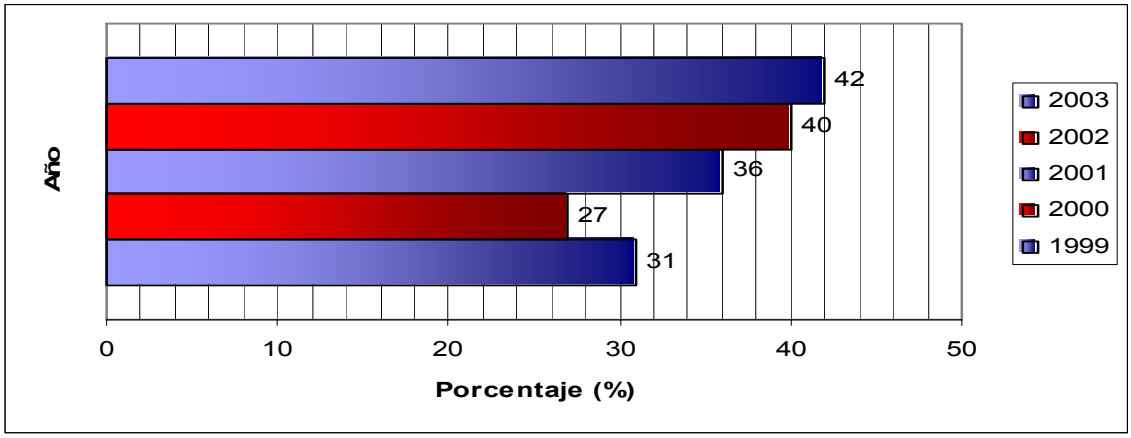

Figura N° 8. Porcentaje de Ataques de Negación de Servicio – Fuente: CSI/FBI, www.gocsi.com

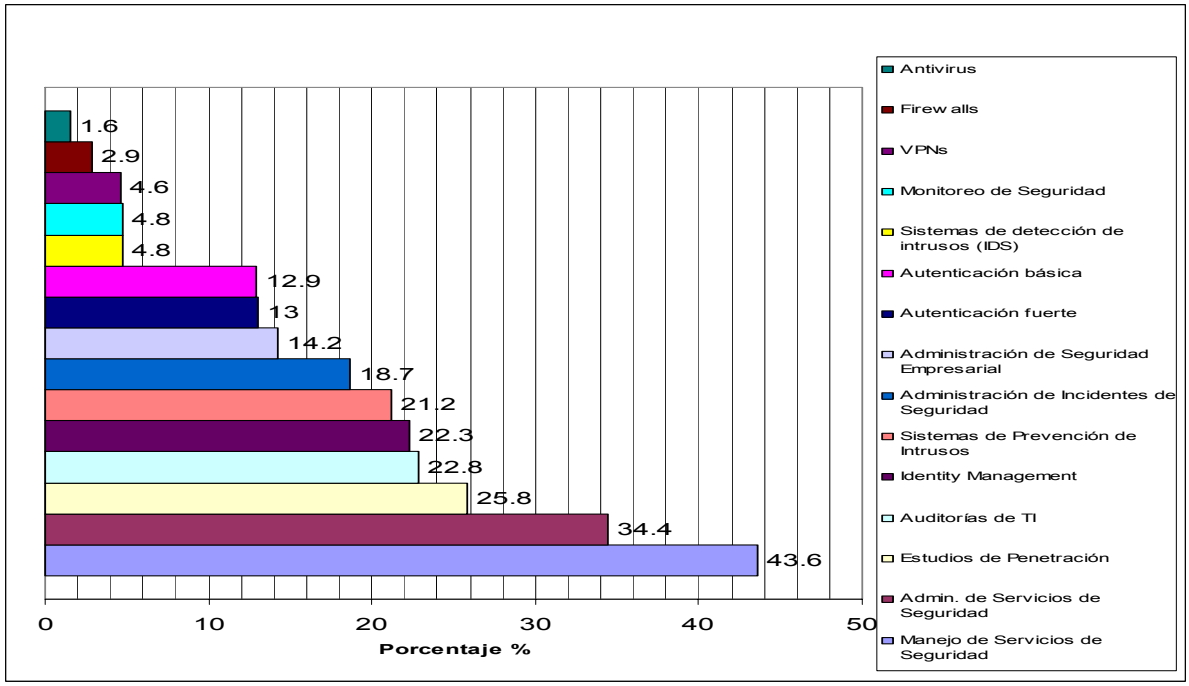

Figura N° 9. Empresas que no planean utilizar estas tecnologías para el 2005 –

Fuente: 2003 ISM Product Survey

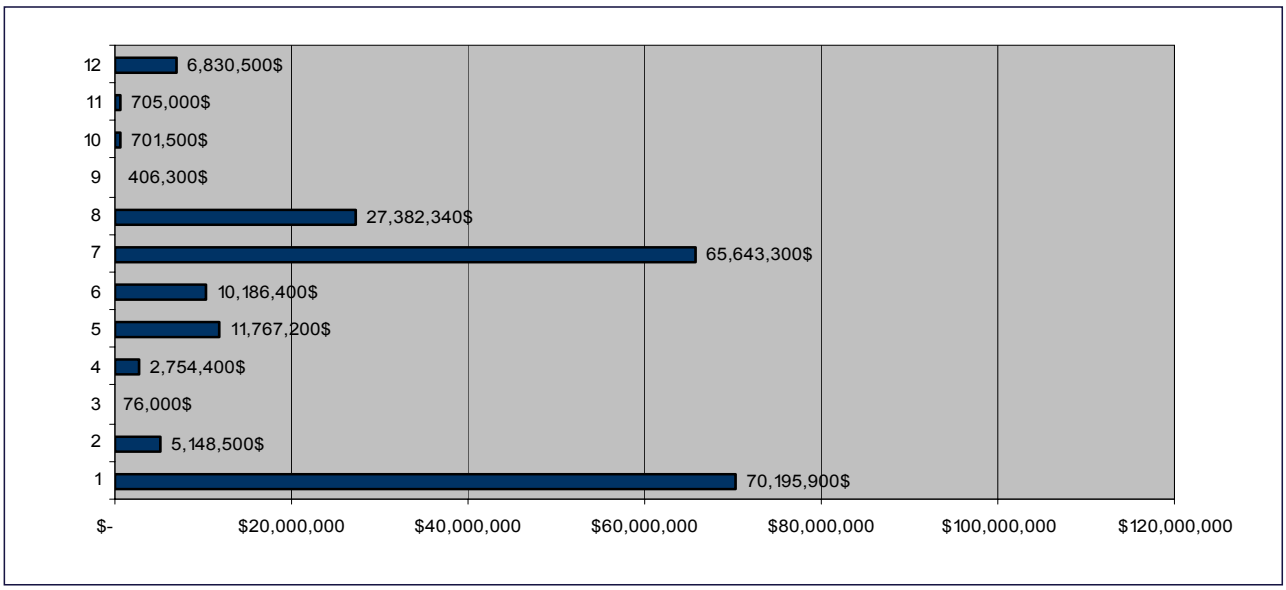

Figura N° 10. Pérdida de dólares por incidentes de seguridad –
Fuente: 2003 CSI - Computer Security Institute

CAPITULO III

MARCO METODOLOGICO

1. Tipo de Investigación

El estudio estuvo concebido dentro de la modalidad de Proyecto Factible. 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). Basado en lo anterior, el estudio consistirá en la ejecución de un estudio de penetración interno y externo a la plataforma tecnológica de la Institución Financiera "XXX", lo cual permitirá mitigar las deficiencias de seguridad en el acceso a los activos de información de manera no autorizada por el personal interno o desde la Internet, y de manera viable, satisfacer las necesidades de la misma.

2. Area de Investigación

El desarrollo de este servicio (Penetration Test), se divide en dos etapas que comprende el estudio de las vulnerabilidades de seguridad internas y externas de la Institución "XXX" con respecto a posibles accesos no autorizados a los activos de información. En este sentido, el estudio de penetración interno se llevó a cabo desde el piso de la Vicepresidencia de Sistemas, y el estudio de penetración externo desde Internet. La Institución "XXX" se encuentra ubicada en la ciudad de Caracas.

3. Técnicas e Instrumentos de Recolección de Datos

Básicamente se utilizó la observación de tipo simple o no participativa indirecta como técnica y la entrevista de tipo no estructurada como instrumento para obtener los requerimientos iniciales del servicio prestado.

Para la ejecución inicial de este servicio, se realizó una entrevista no estructurada del tipo focalizada. La misma fue aplicada a la Vicepresidencia de Sistemas de la Instutición "XXX" con la finalidad de obtener información general de la plataforma tecnológica actual, y así poder determinar el alcance del trabajo, realizar el análisis situacional y finalmente establecer los sistemas críticos a ser evaluados de manera prioritaria.

La *Observación del tipo simple o no participativa indirecta* consistió en emplear herramientas especializadas en obtener información de los distintos componentes y aplicaciones que conforman la plataforma tecnológica de la Institución "XXX" teniendo presente los recursos críticos definidos como parte del alcance en la entrevista no estructurada del tipo focalizada con la Vicepresidencia de Sistemas.

4. Metodología Utilizada

El desarrollo de este servicio a la Institución Financiera "XXX" fue basado en las etapas que se muestran en la Figura N° 11 y se describen posteriormente, las cuales constituyen la metodología utilizada:

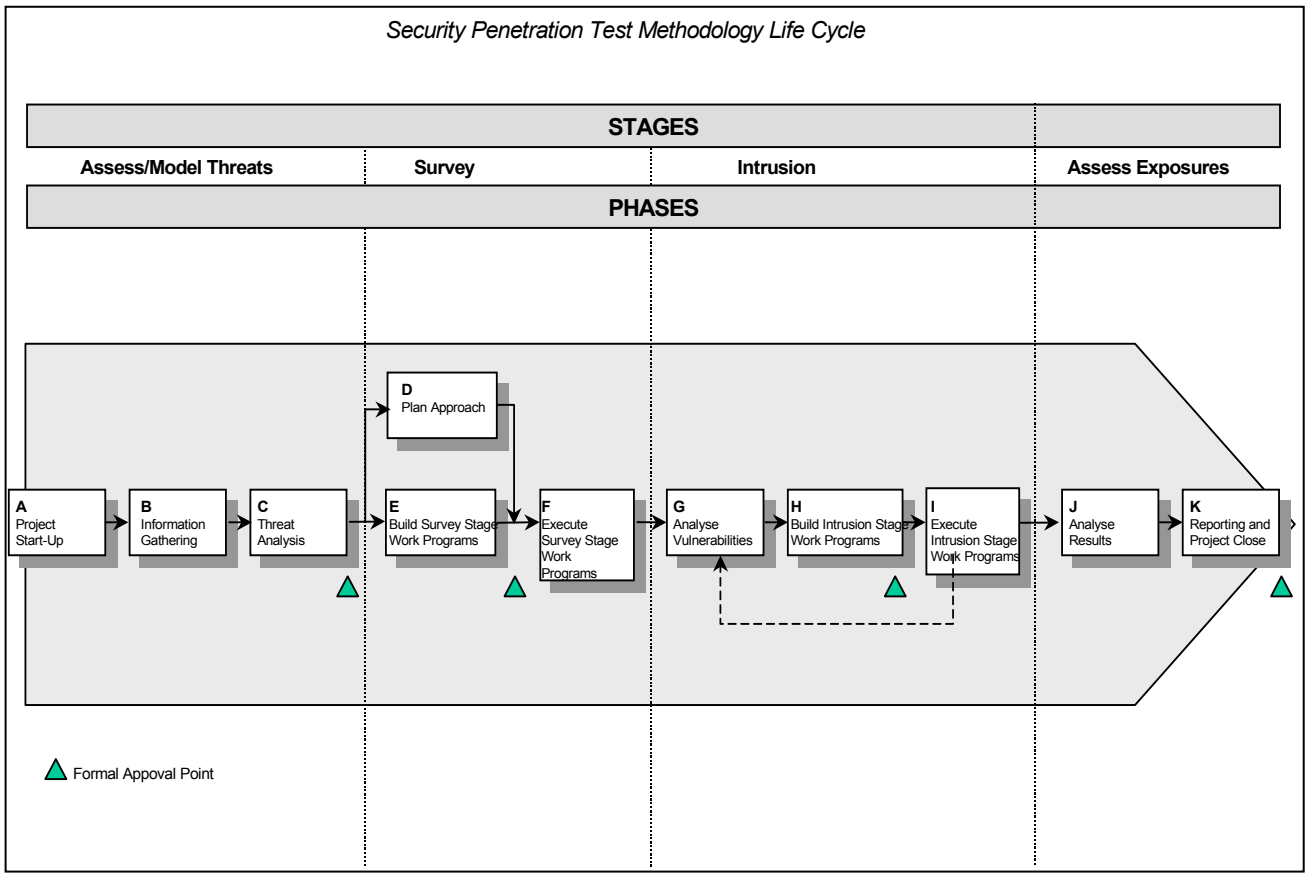

Figura N° 11. Metodología de un Estudio de Penetración

I. Obtención de información e identificación de amenazas

Se determina con el cliente el detalle del rol de intruso a ser adoptado. Se utilizan técnicas para el análisis de amenazas para determinar la causa, los medios y la oportunidad de los intrusos y vincularlos a escenarios específicos.

En este sentido, usando herramientas especializadas, al igual que la información proveída por el cliente, se identifican debilidades en la seguridad de la red, las cuales permitirían el acceso a los sistemas de la Institución.

II. Evaluación de los riesgos o amenazas identificadas

Se utilizan una serie de herramientas y métodos para ejecutar pruebas como las que se describen a continuación:

- Versiones configuradas de software de monitoreo de seguridad tal como Cybercop, ISS, etc., para monitorear la red externamente desde la Internet.
- Sniffers de redes, para intentar capturar información confidencial o sensitiva, tal como claves de acceso.
- Software de monitoreo de puertos IP, para detectar vulnerabilidades en las comunicaciones.

El servicio se lleva a cabo empleando las herramientas mencionadas para identificar vulnerabilidades que puedan ser explotadas en la siguiente etapa. Las pruebas de esta etapa estudian el alcance hasta el cual los equipos externamente visibles desde Internet son vulnerables a ataques que incluyen entre otras, las siguientes vulnerabilidades:

- Información general de importancia al intruso
- Vulnerabilidades del protocolo de transferencia de archivos (FTP). Incluyendo TFTP
- Vulnerabilidades de periféricos de hardware
- Puertas traseras y errores de configuración
- Vulnerabilidades de correo electrónico
- Vulnerabilidades de llamadas remotas a procedimientos (RPC)

- Vulnerabilidades en el sistema de archivos de la red (NFS)
- Vulnerabilidades de ataques de negación de servicio (DOS)
- Ataques de fuerza bruta para determinar claves de acceso
- Vulnerabilidades World Wide Web (WWW)
- Ataques tipo spoofing del protocolo de Internet (IP)
- Vulnerabilidades del Firewall
- Vulnerabilidades del sistema de información de la red (NIS)
- Vulnerabilidades de servicios remotos (Incluyendo X-11, trusted hosts, y rlogin)
- Vulnerabilidades Server Message Block (SMB): Netbios
- Vulnerabilidades Domain Name Server (DNS)
- Vulnerabilidades en Windows NT/2000 y Unix
- Vulnerabilidades del Simple Network Management Protocol (SNMP)

III. Intento de acceso "Intrusión" a la plataforma tecnológica

Teniendo identificadas las áreas de potencial vulnerabilidad, se pasará a explotar las vulnerabilidades para ganar acceso a los sistemas "objetivo". El objetivo general sería el de llevar a cabo una penetración mínima para adecuadamente demostrar la exposición de los sistemas, y alcanzar esto sin realizar algún daño.

Esta etapa se llevará a cabo usando pruebas manuales detalladas y la experiencia. Puede incluir intentos de explotar relaciones de confianza no apropiadas entre equipos (por ejemplo, servidores de producción con relaciones de altos niveles de confianza con servidores de desarrollo menos seguros) y las vulnerabilidades identificadas durante la etapa de supervisión.

IV. Análisis de resultados y emisión de recomendaciones

Una vez concluido el servicio de “Penetration Test” se analizan los resultados y se identifica el origen o las causas de las debilidades identificadas. Basados en los resultados de las pruebas se elabora un informe, cuyo contenido se basa en describir los hallazgos, riesgos y recomendaciones.

CAPITULO IV

SITUACION ACTUAL

1. Información identificada de la plataforma tecnológica de la Institución "XXX"

Empleando herramientas especializadas en la identificación de componentes de red como servidores, routers, switches, firewalls, etc., a continuación se presentan los ambientes que conforman la plataforma tecnológica de la Institución "XXX" identificados desde Internet como internamente desde las instalaciones del cliente:

1.1. Información identificada desde Internet

La siguiente tabla presenta la información obtenida sobre la plataforma tecnológica de la Institución "XXX" accesible desde Internet:

Tabla N° 1. Información obtenida desde Internet

Objetivo	Acción	Resultado
Identificar la existencia de una página WEB de la Institución "XXX" y sus características.	– Mediante buscadores en la Internet como www.google.com.ve, identificar la página Web asociada a la Institución "XXX". – En caso de existir la página WEB: • Verificar el tipo de página (estática y/o dinámica) • Mecanismo de control de acceso que utiliza (Certificados digitales, sólo contraseña, etc) • Verificar si la página maneja el protocolo "https"	Se identificó que la Institución "XXX" posee una página WEB en la Internet por donde ofrece servicios a sus clientes, la cual responde a la dirección "http://www.institucionxxx.com". El site de la Institución "XXX" es dinámico y estático. La página WEB tiene un link de autenticación para acceder a información confidencial, por lo que requiere el uso de una contraseña de acceso suministrada por la Institución "XXX" para cada uno de sus clientes. En el momento que se accede al link para autenticación, el site pasa a ser

Tabla N° 1. Información obtenida desde Internet		
Objetivo	**Acción**	**Resultado**
	para asegurar la información confidencial enviada por Internet.	seguro, utilizando el protocolo "https".
Identificar información en la Internet relacionada con el dominio de la Institución "XXX".	Consultar en sites que ofrecen información relacionada a dominios registrados en la Internet. En este sentido, partiendo de la dirección IP válida de la Institución "XXX", dos de los sites a ser consultados son: http://www.geektools.com/whois.php http://ws.arin.net/cgi-bin/whois.pl Por otra parte, ejecutar desde un ambiente Unix con salida a Internet, el comando "DIG" bajo la siguiente sintaxis <dig institucionxxx.com MX> con el cual se obtendrán las direcciones IP asociadas a servicios de correo e información relacionada a las direcciones IP que ha adquirido.	Se identificaron las direcciones IP válidas adquiridas por la Institución "XXX", observando las direcciones asociadas al servicio SMTP y servicios WEB del dominio registrado.
Identificar los saltos o las rutas por donde pasan las solicitudes de consulta al dominio de la Institución "XXX" desde Internet.	Ejecutar comandos del tipo "ICMP" como "ping" y "Tracert" hacia la dirección IP que responde al dominio registrado por la Institución www.institucionxxx.com	Se identificaron los saltos o las rutas por donde pasan las solicitudes de consultas desde Internet al dominio registrado por la Institución "XXX".
Identificar los equipos que tienen inherencia en los servicios ofrecidos a Internet.	Ejecutar herramientas especializadas en detectar puertos y servicios activos. Ejecutar herramientas especializadas en obtener los Banners de los servicios activos y el nombre de la comunidad SNMP en los equipos de la Institución "XXX" accesibles desde Internet.	Se detectaron los puertos y servicios activos en los componentes de red que tienen inherencia en los servicios prestados vía WEB por la Institución "XXX", detectando la existencia de un Router (Cisco), un Firewall (CheckPoint Firewall-1), un servidor WEB con IIS 5.0. y el nombre del dominio de la Institución "XXX" junto con el nombre del servidor de correo mediante el "Banner" que muestra por conexiones al puerto 25.

1.2. Información identificada desde la red interna

A continuación se presenta la información obtenida sobre la plataforma tecnológica de la Institución "XXX" en sus instalaciones (red interna) empleando un equipo portátil (Laptop):

Tabla N° 2. Información obtenida desde la red interna		
Objetivo	**Acción**	**Resultado**
Identificar las características del direccionamiento IP configurado en la red LAN de la Institución.	Conectar el equipo portátil "laptop" a un punto de red disponible. Emplear para ello un cable UTP Nivel 5 y verificar si hay respuesta a la conexión (LINK). Conectado el equipo a un punto de red, ejecutar el comando IPCONFIG /ALL desde la línea de comandos (CMD) para obtener la información requerida. En caso que la asignación de direcciones IP no sea dinámico (DHCP), aplicar ingeniería social para obtener la información requerida en una estación de trabajo de un usuario final.	Los puertos de red que están disponibles no se encuentran deshabilitados y no hay restricciones por direcciones físicas (Mac-Address), dado que hubo respuesta a la conexión. Se observó que la asignación de las direcciones IP se realiza de manera dinámica (DHCP), siendo clase "C" definida por la red "192.168.0.0/24". Asimismo, se obtuvo la dirección del servidor DHCP, WINS, la puerta de enlace y los DNS definidos.
Identificar si existen otras sub redes o segmentos en la plataforma tecnológica de la Institución.	Ejecutar desde el equipo portátil, el comando "TRACERT a la página WEB de la Institución para observar la ruta que siguen los paquetes desde la red interna (LAN).	Observando el resultado de los saltos, se pudo identificar que existe una red "DMZ" identificada con la red 10.0.0.0/24.
Identificar los componentes activos que conforman la red interna de la Institución "XXX" y las características que los definen.	Ejecutar herramientas especializadas en detectar equipos activos en la red de la Institución. Para ello, la misma debe ser configurada en un rango de direcciones desde la 192.168.0.1 hasta 192.168.0.254. y desde la dirección 10.0.0.1 hasta la 10.0.0.254. Configurar la herramienta empleada	Mediante la ejecución de herramientas especializadas en detectar equipos activos y descripción relacionada, se obtuvo el siguiente resultado: – Se detectaron ochenta y siete (87) estaciones de trabajo activas con sistema operativo Windows 2000. Red 192.168.0.0/24. – Se detectaron dos (2) servidores

Tabla N° 2. Información obtenida desde la red interna		
Objetivo	**Acción**	**Resultado**
	para detectar los componentes activos en la plataforma tecnológica de la Institución para que realice consultas SNMP bajo el nombre de la comunidad "Public" y consultas del tipo NetBios.	Unix SUN Solaris Versión 8. Red 192.168.0.0/24. – Se detectaron cinco (5) servidores con sistema operativo Windows 2000. Un mayor detalle de la información obtenida se menciona a continuación: • Un servidor de correo electrónico. En la red 10.0.0.0/24. • Un servidor Active Directory. Red 192.168.0.0/24. • Dos servidores de servicios WEB a Internet. (Producción y Desarrollo). En la red 10.0.0.0/24 el de producción. • Un servidor Proxy. Red 192.168.0.0/24. – Se identificaron cinco (5) switches marca CISCO. Uno de ellos en la red 10.0.0.0/24. – Se identificó un (1) router Cisco. En la red 192.168.0.0/24.
Identificar los puertos y servicios activos en los servidores, Switches y el Router identificado.	Ejecutar herramientas especializadas en detectar los puertos activos en los distintos componentes que conforman la plataforma tecnológica de la Institución "XXX" en su sede principal.	Se detectaron los puertos activos por cada uno de los servidores y equipos que conforman la plataforma tecnológica de la Institución "XXX". Del proceso de identificación de puertos y servicios activos, se identificó la presencia de los manejadores de base de datos SQL Server (Puerto 1433) en los servidores WEB, y ORACLE en los servidores Unix SUN Solaris.
Identificar la existencia de redes inalámbricas.	Activar "Wireless Network Connection" en el equipo portátil e identificar si hay alguna red Wireless cercana perteneciente a la Institución "XXX"	Al activar "Wireless Network Connection" en el equipo portátil, se identificó la existencia de una red inalámbrica, ya que la misma provee el nombre de la red "SSID" por Broadcast.

1.3. Plataforma tecnológica identificada

Producto de la información obtenida desde Internet y de la red interna, se presenta en la Figura N° 12 el diagrama de red que conforma la plataforma tecnológica de la Institución "XXX" destacando sus principales componentes:

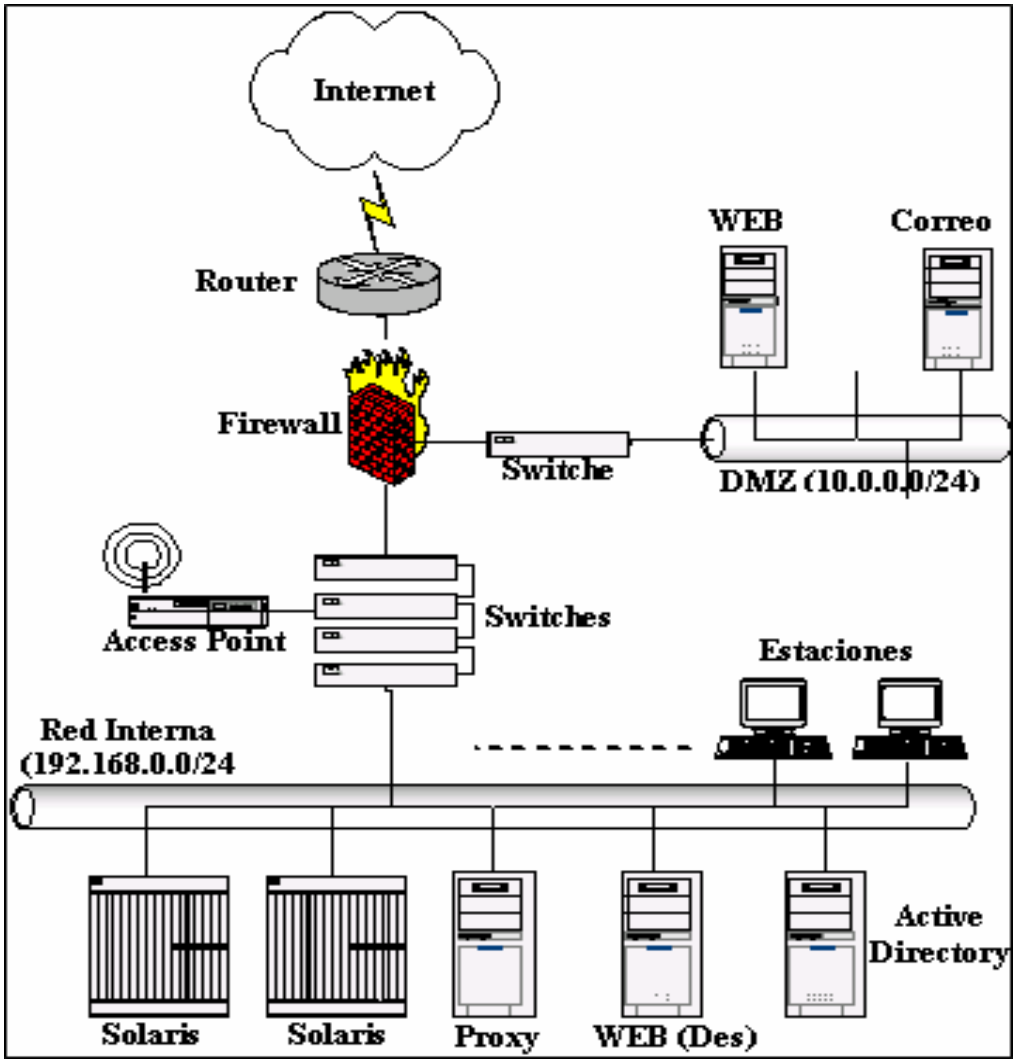

Figura N° 12. Estructura de red identificada en la Institución "XXX"

2. Vulnerabilidades y riesgos identificados en la plataforma tecnológica de la Institución "XXX"

En función a los componentes de red que conforman la plataforma tecnológica de la Institución "XXX" identificados anteriormente, se procedió a efectuar una serie de pruebas y la ejecución de herramientas especializadas en identificar brechas o vulnerabilidades en seguridad, las cuales representan niveles de riesgos para la confidencialidad e integridad de los activos de información. A continuación se presentan las vulnerabilidades y riesgos asociados a los activos de información de la Institución "XXX" identificados tanto de forma externa como interna:

2.1. Vulnerabilidades y riesgos identificados desde Internet

A continuación se presentan las vulnerabilidades o brechas de seguridad y riesgos identificados en los componentes tecnológicos de la Institución "XXX" desde Internet, empleando herramientas especializadas y la experticia técnica adquirida:

Tabla N° 3. Vulnerabilidades y riesgos identificados desde Internet

Vulnerabilidad	Hallazgo	Riesgo
El Router de Internet posee un nombre trivial de comunidad SNMP.	El protocolo SNMP ("Simple Network Management Protocol") es utilizado para realizar labores de monitoreo y control en los equipos que interactúan en la red. Con este protocolo, se puede administrar los diversos equipos en forma remota e identificar conflictos o fallas en los mismos. Usualmente los equipos (servidores y otros componentes de la red) vienen configurados para responder a las peticiones SNMP (puertos 162 y 163) cuando le son solicitados bajo el	La utilización de la comunidad genérica "public" y "cable-docsis" en los equipos de red es ampliamente conocida y el intruso lo puede utilizar para identificar el tipo de componentes instalados en la red y la topología de la misma.

Tabla N° 3. Vulnerabilidades y riesgos identificados desde Internet		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	nombre de una comunidad. En este sentido se pudo detectar que el Router evaluado responde a la comunidad SNMP "Public" identificando que es marca CISCO.	
Se detectaron puertos del Router evaluado abiertos a Internet que pudieran comprometer su operatividad.	El Router evaluado tiene abiertos hacia Internet los siguientes puertos: – Echo (port TCP 7): Mediante este servicio el Router reenvía toda información que recibe por el puerto 7 TCP. – Chargen (port TCP 19): Es un generador de caracteres que se utiliza sobre todo para comprobar el estado de las conexiones de red y cuando accede a este servicio, simplemente ve en su terminal una secuencia de caracteres ASCII que se repite indefinidamente. – Finger (port TCP 79) y Rwhod (port UDP 513): Este servicio permite obtener una lista de nombres de usuarios válidos y conexiones, lo cual podría ser utilizado por personas no autorizadas para intentar obtener accesos desautorizadamente a los activos de información de la Compañía. – Daytime (port TCP 13): Este	Esta situación pudiera ser utilizada por personas no autorizadas o intrusos desde Internet para obtener información confidencial y ejecutar ataques de negación de servicios "DoS" contra el Router, ocasionando continuas interrupciones en su operatividad y de los servicios que dependen del mismo.

Tabla N° 3. Vulnerabilidades y riesgos identificados desde Internet		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	servicio permite obtener información de la fecha, hora de la localidad donde se encuentra el Router. – Discard (port TCP 9): La función de este servicio es desechar toda información que le es transmitida sin respuesta alguna. – Telnet (port TCP 23): Servicio utilizado para establecer conexiones remotas.	
El Router de Internet acepta conexiones externas vía "Telnet" desde cualquier dirección IP.	El Router que interviene en el acceso a Internet desde las instalaciones de la Institución "XXX", acepta conexiones vía "Telnet" desde cualquier dirección de la red pública (Internet) a su interfaz externa.	Posibilidad de que una persona no autorizada logre autenticarse efectivamente contra el Router, pudiendo posteriormente interrumpir los servicios que dependen de este. Además, un intruso teniendo control del Router, se le facilita la ejecución de otros ataques contra la plataforma tecnológica de la Institución "XXX", dado a que ha superado uno de los mecanismos de seguridad de la Institución.
El Firewall permite el flujo de paquetes "ICMP" ("Internet Control Message Protocol") desde Internet hacia los equipos ubicados en la "DMZ".	El Firewall permite la transmisión de paquetes ICMP desde y hacia cualquier dirección interna, lo cual permite la ejecución de comandos como el "tracert [IP Address]", con el cual es posible crear mapas asociados a la topología de la red de la Institución.	Esta situación, puede ocasionar que personas no autorizadas logren tener conocimiento sobre la plataforma tecnológica, permitiéndoles identificar la topología de red, pudiendo los equipos ser objeto de ataque DoS (Denied of Service) con el fin de atentar contra la operatividad de la Institución.
El Firewall responde a	Ejecutando herramientas	Esta situación permite que

Tabla N° 3. Vulnerabilidades y riesgos identificados desde Internet		
Vulnerabilidad	**Hallazgo**	**Riesgo**
conexiones externas por varios puertos abiertos desde Internet por donde se obtiene información confidencial.	especializadas desde Internet hacia la interfaz externa del Firewall, se detectaron puertos abiertos que pueden ser accedidos por cualquier intruso o persona no autorizada desde Internet, destacando que dos (2) de los puertos identificados "259" y "900" son empleados para conectarse respectivamente vía "Telnet" y "http" hacia el Firewall, usando como mecanismo de autenticación "SecureID" y el resto de los puertos son empleados para propósitos de administración de las políticas del Firewall en forma remota.	cualquier intruso o persona no autorizada desde Internet, obtenga información confidencial para la Compañía, como el tipo de Firewall que se está usando, el mecanismo de autenticación empleado e incluso el nombre de red que tienen los servidores donde están instalados. De esta manera, se le facilita al intruso sus ataques con intenciones de interrumpir los servicios que dependen del Firewall o ingresar a los activos de información de la Compañía. Los ataques de negación de servicios y fuerza bruta, son los ataques más comunes que pudieran ser ejecutados hacia el Firewall por parte de intrusos o personas no autorizadas.
El servidor de correo electrónico y WEB muestra hacia Internet información confidencial para la Compañía	El servidor de correo electrónico entrante muestra información relacionada al software de correo, versión, dominio y nombre físico del servidor en la red de la Compañía, al responder a peticiones por el puerto "25 - smtp" con la sintaxis "telnet <IP>". Por otra parte el servidor WEB permite mediante consultas por el puerto 80, conocer la versión de Internet Information Server "IIS".	Esta situación le permite a un intruso obtener información confidencial para la Compañía, centrando su atención en obtener vulnerabilidades características del servidor de correo y WEB, las cuales podrían ser usadas para ejecutar ataques contra el mismo, interrumpiendo su operatividad y disminuyendo la calidad del servicio.
El servidor de correo no restringe los ataques de tipo "spam"	Se entiende por "spam" el envío masivo de mensajes no solicitados, así como todas las	La carencia de controles de seguridad adecuados, que contribuyan a evitar ataques de

Tabla N° 3. Vulnerabilidades y riesgos identificados desde Internet		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	formas de abuso ligadas al servicio de correo electrónico (ACE). En este sentido, actualmente la Compañía no cuenta con mecanismos suficientes que contribuyan a frenar la proliferación de correos no deseados "spam". Evidencia de lo mencionado, fue las pruebas de "spam" a una cuenta de correo de un contacto interno desde una dirección falsa anonymous@falso.com, recibiendo un promedio de mil (1000) correos electrónicos. Los métodos utilizados por los "spamers" se sustentan principalmente en las deficiencias del protocolo "SMTP".	correos no deseados "spam", puede traer como consecuencia continuas interrupciones del servicio de correo electrónico, dado a que la capacidad de los buzones de correo electrónico llegarán rápidamente a su limite. Asimismo, la posibilidad de recibir correos falsos, puede traer como consecuencia, la ejecución de actividades no autorizadas a favor de los intrusos.

2.2. Vulnerabilidades y riesgos identificados desde la red interna

A continuación se presentan las vulnerabilidades o brechas de seguridad y riesgos identificados en los componentes tecnológicos de la Institución "XXX" desde la red interna o privada, empleando herramientas especializadas y la experticia técnica adquirida:

Tabla N° 4. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente de Red)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
No se encuentran deshabilitados los puntos de red que no están siendo utilizados y no se han configurado los que se requieren con la dirección física de la estación de trabajo conectada.	Las instalaciones de la Institución "XXX" poseen puntos de conexión a la red en cada una de sus diferentes localidades, los cuales se encuentran habilitados aun cuando no están siendo utilizados. Adicionalmente,	Esta situación le permite a una persona no autorizada, conectar una estación de trabajo de escritorio o portátil a cualquier punto de red y obtener una dirección IP de forma dinámica, pudiendo posteriormente ejecutar

Tabla N° 4. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente de Red)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	aquellos puntos que efectivamente están siendo utilizados, no se encuentran restringidos a las estaciones de trabajo que tienen conectadas (filtro por "Mac-Address").	herramientas de monitoreo, sniffing y de negación de servicio hacia los equipos más críticos de la Institución.
El Firewall no restringe el flujo de paquetes ICMP desde la red Interna hacia la Zona Desmilitarizada "DMZ" y viceversa.	El Firewall permite el flujo de paquetes "ICMP" desde y hacia cualquier dirección interna, lo cual permite la ejecución de comandos como el "tracert [IP Adress]", con el cual es posible crear mapas asociados a la topología de la red de la Institución. Asimismo, es importante destacar que estos comandos son requeridos sólo por los administradores de los servidores.	Esta situación, puede ocasionar que personas no autorizadas logren tener conocimiento sobre la plataforma tecnológica, pudiendo tomar ventaja de esta situación y atentar contra la operatividad de los servicios de red de la Institución.
No existen mecanismos o sistemas de detección de intrusos en red (NIDS).	La Institución "XXX", carece de sistemas para la detección de intrusos y actividades sospechosas (NIDS), destacando que durante dos días consecutivos se realizó un "scanning" de la red sin levantar ningún tipo de alarmas o acciones por parte de la Institución.	Esta situación permite identificar y obtener información confidencial de los componentes que conforman la red de la institución, en cuanto a servidores, estaciones de trabajo, switches, etc., pudiendo observar tipos y versiones de sistemas operativos, puertos habilitados e información en general, lo cual pudiera ser utilizado para conseguir una vía de acceso a los activos de información.
No se cuenta con mecanismos de seguridad para restringir el redireccionamiento de "Mac Address" en los equipos críticos de la Institución	El Protocolo de Resolución de Direcciones (Address Resolution Protocol o ARP) - RFC 826, permite identificar los equipos que conforman una red mediante una dirección física	En este sentido, aún cuando el esquema de red la Institución "XXX" es conmutado, no escapa de la posibilidad de recibir un ataque de este tipo, ya que no cuenta con ningún

Tabla N° 4. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente de Red)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	única, la cual es asignada permanentemente a las tarjetas de red desde su fabricación. En este sentido, cuando un sistema o aplicación necesite comunicarse por primera vez con otro dentro de la misma red enviará un broadcast ARP buscando la dirección del hardware del sistema destino. El sistema apropiado responderá a la petición ARP enviando su dirección de hardware y la comunicación podrá comenzar. Sin embargo, los mensajes ARP pueden ser utilizados para forzar el paso del tráfico desde el sistema que lo ha originado al sistema del atacante, incluso dentro de un ambiente de red conmutado.	mecanismo de seguridad implantado para solventar o identificar esta situación, en donde una persona no autorizada podría observar el tráfico que haya redireccionado hacia su equipo utilizando un analizador de paquetes o sniffer y posteriormente volver enviarlo al destino real. Este escenario recibe el nombre de ataque "Man in the middle".
Los Routers y Switches responden al nombre de comunidad "Public" del protocolo SNMP.	Los Routers y Switches que conforman parte de la red de la Institución "XXX", emplean el protocolo SNMP para ser gestionados de manera centralizada. Sin embargo, el nombre definido en la comunidad de dicho protocolo, no ha sido cambiado "Public".	El uso de nombres conocidos o por defecto an la comunidad del protocolo SNMP, trae como consecuencia que un intruso pueda obtener información relacionada a los equipos que conforman parte de la red como los Routers y Switches. Dicha información como por ejemplo la marca del equipo y so versión de software operativo, permite canalizar de manera más certera ataques de acceso no autorizados o negación de servicio.
Las contraseñas de acceso a los Routers y Switches de la Institución son de conocimiento público.	Los componentes activos que conforman parte de la red de la Institución "XXX" como los Routers y Switches, partiendo	Esta situación, puede traer como consecuencia, accesos no autorizados al entorno de los Routers y Switches, pudiendo

Tabla N° 4. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente de Red)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	del hecho que fueron identificados como equipos CISCO, presentan contraseñas por defecto para su administración, las cuales no fueron cambiadas al momento de su instalación y configuración.	alterar su configuración con intenciones de eliminar las restricciones o controles de seguridad previamente implantados para proteger en lo posible los activos de información.

Tabla N° 5. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Wireless)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
La configuración de los componentes activos de la red inalámbrica (”Access Points”) puede ser accedida en forma anónima desde la red fija o cableada.	El “Access Point” (“AP-AM0001”) es el encargado de proveer acceso inalámbrico a un grupo de personas a la red de la Institución. En este sentido, la configuración del mismo puede ser accedida de manera anónima vía “HTTP” desde la red fija o cableada, permitiendo visualizar parámetros confidenciales como el “ESSID” y las direcciones “MAC Address” de los equipos válidos a conectarse sin autenticación.	Esta situación le permite a cualquier personal interno a la Institución, obtener la configuración del “Access Point” y suministrarla a terceros, para que puedan acceder a los activos de información de la Institución desde la red inalámbrica, tomando en cuenta que su alcance trasciende sus instalaciones.
No existen mecanismos para controlar el flujo de información desde la red inalámbrica hacia la red fija o cableada.	El direccionamiento de la red inalámbrica es el mismo de la red interna (“192.168.0.0/24”). Destacando, que no existe ningún tipo de restricción de servicios o acceso de las estaciones de trabajo conectadas desde esta red hacia la red fija o cableada.	Partiendo del hecho que la ubicación física del “Access Point” permite que la señal de la red inalámbrica trascienda las instalaciones de la Institución “XXX”, esta situación genera un riesgo de seguridad, dado que no existen mecanismos para controlar el tráfico proveniente de la red inalámbrica, pudiendo un intruso que logre conectarse, trabajar sin restricciones hacia la red fija o cableada, facilitándole el acceso a los

Tabla N° 5. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Wireless)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
		servidores críticos y posibilitando el obtener información confidencial o poner en peligro la continuidad de las operaciones.
El "Access Point" no tiene configurado la opción de cifrado de información.	El "Access Point" no tiene configurado la opción de cifrado de paquetes utilizando el protocolo "WEP" ("Wired Equivalent Privacy") y no cuentan con mecanismos robustos para la verificación de las listas de acceso por direcciones físicas "MAC-Address".	Esta situación facilita el acceso no autorizado a los activos de información de la Institución mediante el uso de la red inalámbrica, pudiendo generar interrupciones de la continuidad operativa de aplicaciones y servidores, así como la obtención de información confidencial tal como credenciales de acceso a los distintos ambientes.

Tabla N° 6. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
No han sido restringidas las consultas anónimas hacia las estaciones de trabajo.	El servicio "Lan Manager" está configurado de tal modo que permite que usuarios no autenticados en la red de la Institución, puedan solicitar información sobre las estaciones de trabajo, permitiendo que personas no válidas dentro de la comunidad de usuarios, puedan obtener información de los recursos publicados en los equipos y cuentas con privilegios administrativos.	Esta situación puede representar un riesgo de acceso no autorizado, debido a la obtención de información importante y confidencial, que puede ser empleada para planificar actividades de ataque hacia los servidores principales o críticos conectados a la red.
La contraseña de la cuenta de administración local es común en varias estaciones de trabajo, siendo ésta de fácil deducción.	Se identificó que las estaciones de trabajo tienen en común la cuenta de administración local "Administrator", las cuales poseen la misma contraseña que	La situación descrita, permite extraer el archivo de contraseñas local ("SAM") y descifrar mediante herramientas especializadas la clave de la

Tabla N° 6. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	se considera de fácil deducción, debido a que fue descifrada en menos de una hora (1 hora) por mecanismos sencillos como "Brute Force".	cuenta de administración local de las estaciones de trabajo. De esta manera, se puede tener acceso a los equipos que presentan esta situación, pudiendo comprometer la información confidencial que contienen y su operatividad.
El orden de inicio de las estaciones de trabajo permite utilizar discos de arranque para omitir el proceso de carga del sistema operativo y la contraseña de configuración del "BIOS" no está definida.	El orden de inicio de las estaciones de trabajo permite utilizar discos de arranque para omitir el proceso de carga del sistema operativo (Windows NT). Asimismo, se detectó que la contraseña de configuración del "BIOS" no está definida, la cual es solicitada cuando se requiere el acceso a las opciones de configuración que son definidas por los fabricantes de los equipos.	La situación descrita permite que las estaciones de trabajo puedan ser accedidas por una vía distinta a la autenticación provista por el sistema operativo Windows NT, facilitando la obtención de información confidencial para los usuarios y extraer el archivo de contraseñas, para ser descifrado posteriormente e intentar acceder de forma remota al resto de las estaciones de trabajo.
No ha sido removida la compartición administrativa en las estaciones de trabajo.	Las estaciones de trabajo no le ha sido removida la compartición administrativa por defecto, lo cual es un estándar de Windows NT que permite la conexión a los equipos mediante el uso de los recursos administrativos.	Esta situación incrementa la posibilidad de que usuarios no autorizados puedan efectuar posibles accesos sobre información sensitiva de la Compañía, partiendo de lo que puedan conseguir en los equipos que presentan la debilidad mencionada.
No se detectaron mecanismos para el control de aplicaciones instaladas de manera no autorizada en las estaciones de trabajo.	Fue posible instalar en las estaciones de trabajo una herramienta para el monitoreo de las actividades de los usuarios ("Spy Software"), de forma remota sin que fuese detectado por lo usuarios ni por los custodios de la red. La instalación se realizó dado a que las estaciones de trabajo tienen	La situación descrita aunado al hecho de no contar con mecanismos de control de aplicaciones instaladas en las estaciones de trabajo, permiten la captura tanto del texto escrito por los usuarios, como del contenido de las pantallas, facilitando la obtención de credenciales válidas para acceder a los sistemas de la

Tabla N° 6. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	compartición administrativa y está habilitada la conexión remota al registro (Registry).	Institución.
El protocolo "Netbios" se encuentra activo en las estaciones de trabajo.	El protocolo "Netbios", fue desarrollado para ser utilizado en los servicios de grupos de trabajo "Workgroup" en la plataforma Windows 3.x y Windows 95/98, para el soporte de esquemas de redes distribuidas en instalaciones sencillas. Este protocolo permite identificar la tabla de enrutamiento y la tabla de resolución de nombres "WINS" ("Windows Internet Naming Service"), lo cual puede ser utilizado por el intruso para identificar componentes claves en la red y planificar de esta forma su ataque, debido a que se podría obtener información tal como el nombre de los dominios definidos, las cuentas de los usuarios que se encuentran conectados, entre otros. Asimismo, este protocolo permite obtener perfiles de usuario válidos, mediante el uso de identificación numérica cuya asignación para el caso de los perfiles básicos es de conocimiento público, lo que permitió identificar usuarios con altos privilegios y canalizar el ataque sobre estos.	Debido al tipo de utilización para el cual se diseñó, "Netbios" no ofrece un esquema de seguridad consistente y puede ser causa de accesos no autorizado a los activos de información que residen en la red de la Institución.
Las estaciones de trabajo responden al nombre "Public" de la comunidad del protocolo	El protocolo "SNMP" ("Simple Network Management Protocol") es utilizado para realizar labores	La utilización de la comunidad genérica "public" del protocolo "SNMP" en los equipos de red

Tabla N° 6. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
SNMP.	de monitoreo y control en los equipos que interactúan en la red. Con este protocolo, se puede administrar los diversos equipos en forma remota e identificar conflictos o fallas en los mismos. Usualmente los equipos (servidores y otros componentes de la red) vienen configurados para responder a las peticiones "SNMP" cuando le son solicitados bajo el nombre de comunidad "public", el cual está configurado bajo este esquema en las estaciones de trabajo.	es ampliamente conocida y un intruso puede utilizar este hecho para identificar el tipo de componentes instalados en la red y la topología de la misma.
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en las estaciones de trabajo.	La configuración actual de las estaciones de trabajo permite a usuarios con privilegios administrativos locales, acceder el registro del sistema ("registry") de otras estaciones de trabajo conectadas a la red de la Compañía. Este tipo de configuración es inadecuada, considerando que en el registro se encuentra todas las configuraciones del sistema, además de los perfiles de usuarios definidos y sus contraseñas (cifrada).	Esta situación puede comprometer la operatividad de los equipos, así como la confidencialidad que deben poseer las contraseñas de los usuarios, para evitar accesos no autorizados a los activos de información de la Compañía.
No ha sido desactivado el cifrado "LanMan" en las estaciones de trabajo.	Windows cuenta con algoritmos distintos para el cifrado de las contraseñas de los usuarios, tales como los varios algoritmos "LanMan", "NTLM" y "NTLMV2". El algoritmo "LanMan" permanece para mantener la compatibilidad con las plataformas distintas a Windows NT (Windows 95 ó	Esta situación, le permite a un usuario no autorizado descifrar los "hashes" (patrones) obtenidos de las contraseñas en poco tiempo, dado a que el algoritmo "LanMan" divide la contraseña en dos (2) partes de siete (7) caracteres, así como también convierte todos los caracteres a mayúsculas. Esto

Tabla N° 6. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	98), el cual presenta debilidades en su cifrado. En este sentido, se pudo detectar que este algoritmo no ha sido desactivado en las estaciones de trabajo.	reduce el espacio de búsqueda notablemente, permitiendo calcular todas las posibles contraseñas alfanuméricas en un tiempo máximo de doce (12) horas en un procesador Pentium III 800mhz.

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
La solicitud de consulta de usuarios anónimos mediante el uso del servicio "Lan Manager" en los servidores no ha sido restringida.	El servicio "Lan Manager" está configurado de tal modo que permite que usuarios no autenticados en la red de la Institución, puedan solicitar información sobre los servidores evaluados, permitiendo que personas no válidas dentro de la comunidad de usuarios remotos puedan conocer acerca de los recursos publicados en el mismo y el nombre del administrador de la red u otros usuarios.	Esta situación representa un riesgo de acceso no autorizado, motivado por la obtención de información confidencial, que puede ser empleada para planificar actividades de ataque a los sistemas.
Las políticas de contraseñas de usuarios definidas en el servidor de "Active Directory" no cumple con las mejores prácticas de seguridad.	En relación a las políticas de cuentas definidas en los servidores evaluados, se detectaron las siguientes situaciones: – En los servidores Web, Correo y Proxy, no se encuentra activo el bloqueo de cuentas por intentos fallidos de conexión. Asimismo, en el servidor de "Active Directory" este control presenta deficiencias, dado que tienen configurado diez (10) intentos fallidos	Esta situación le facilita a un intruso o persona no autorizada el acceso a los recursos de la Institución, dado que las contraseñas pudieran permanecer invariables por tiempo indeterminado. Asimismo, la configuración implantada para el bloqueo de cuentas por intentos fallidos de conexión, permite que sus contraseñas puedan ser deducidas en menor tiempo, ya que se pueden configurar aplicaciones que manejen mecanismos de "Brute Force" de forma continua hacia las cuentas

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	antes de bloquear una cuenta en vez de tres (3); y el tiempo para el reinicio del contador de intentos fallidos de acceso está configurado para 30 min y el tiempo de bloqueo en 1 hora. – El control de historial de contraseñas se encuentra desactivado en los servidores evaluados. – La longitud mínima de las contraseñas de usuarios está configurada en seis (6) caracteres en los servidores evaluados. – En el servidor de "Active Directory", el tiempo mínimo para cambiar las contraseñas está definido en cero (0) y el tiempo máximo en noventa (90) días. Asimismo, en relación al resto de los servidores no está configurada estas opciones.	definidas en los servidores y en especial al servidor de "Active Directory".
Las bondades de auditoría no se encuentran configuradas en el servidor de "Active Directory" acorde a las mejores prácticas y se encuentra inactiva en los servidores de correo, Web y Proxy.	En el servidor de "Active Directory" sólo se encuentra activa la opción de auditoría que registra los intentos de acceso efectivos. Asimismo, en el resto de los servidores no se encuentran activas las opciones de auditoría.	Al existir eventos que no están siendo auditados, puede traer como consecuencia que no se registren ciertas actividades inusuales en los servidores evaluados, dificultando la toma oportuna de acciones preventivas y correctivas ante una actividad no autorizada.
Se detectaron usuarios con contraseñas de fácil deducción en los servidores evaluados.	De un total de 107 cuentas definidas en el servidor de "Active Directory", se detectaron 71 cuentas con contraseñas de fácil deducción, las cuales mantienen patrones como los que	Esta situación incrementa el riesgo de que las claves de acceso de los usuarios puedan ser identificadas por personas no autorizadas que deseen obtener acceso a la red, mediante

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	se mencionan a continuación: – Contraseñas relacionadas con el identificador de usuario (User Name) – Contraseñas relacionadas con el entorno de trabajo. – Contraseñas relacionadas con palabras comunes y sin uso de caracteres especiales. En el caso de los servidores Web, Correo y Proxy, la cuenta local "Administrator", tiene contraseña de fácil deducción. Adicionalmente, por ser servidores miembros del dominio principal, hay cuentas definidas en el servidor de "Active Directory" con acceso a los servidores mencionados, las cuales han sido identificadas con contraseñas triviales.	paquetes de software o utilizando técnicas de "sniffing", logrando acceso a los servidores evaluados, y pudiendo alterar la configuración del sistema operativo u obtener acceso a opciones que se tienen restringidas.
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en los servidores evaluados	La configuración actual de los servidores evaluados permite a usuarios con privilegios administrativos locales, acceder el registro del sistema ("registry") de otras estaciones de trabajo conectadas a la red de la Institución. Este tipo de configuración es inadecuada, considerando que en el registro se encuentra todas las configuraciones del sistema, además de los perfiles de usuarios definidos y sus contraseñas (cifrada).	Esta situación puede comprometer la operatividad de los equipos, así como la confidencialidad que deben poseer las contraseñas de los usuarios, para evitar accesos no autorizados a los activos de información de la Institución.
Existen deficiencias en la administración de los controles	De un total de 107 cuentas definidas en el servidor de	Se le puede facilitar en gran medida a un intruso o persona no

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
de acceso asignados a las cuentas de usuarios definidas en el servidor de "Active Directory".	"Active Directory", se detectaron las siguientes situaciones: – Sesenta y cinco (65) cuentas no le caduca la contraseña de acceso a la red, las cuales nunca han sido cambiadas. – Treinta y cuatro (34) cuentas no pueden cambiar su contraseña de acceso. – Veinticinco (25) cuentas se encuentran inactivas por más de tres meses.	autorizada, el acceso a los activos de información de la Institución, valiéndose de una de las cuentas de usuarios que presenta estas situaciones.
El protocolo "Netbios" se encuentra activo en los servidores Windows 2000 evaluados.	El protocolo "Netbios", fue desarrollado para ser utilizado en los servicios de grupos de trabajo "Workgroup" en la plataforma Windows 3.x y Windows 95/98, para el soporte de esquemas de redes distribuidas en instalaciones sencillas. Este protocolo permite identificar la tabla de enrutamiento y la tabla de resolución de nombres "WINS" ("Windows Internet Naming Service"), lo cual puede ser utilizado por el intruso para identificar componentes claves en la red y planificar de esta forma su ataque, debido a que se podría obtener información tal como el nombre de los dominios definidos y las cuentas de los usuarios que se encuentran conectados, entre otros. Asimismo, este protocolo permite obtener perfiles de usuario válidos, mediante el uso de identificación numérica cuya	Debido al tipo de utilización para el cual se diseñó, "Netbios" no ofrece un esquema de seguridad consistente y puede ser causa de accesos no autorizados a los activos de información que residen en la red de la Institución.

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	asignación para el caso de los perfiles básicos es de conocimiento público, lo que permitió identificar usuarios con altos privilegios y canalizar el ataque sobre estos.	
Los servidores evaluados responden al nombre "Public" de la comunidad del protocolo SNMP.	El protocolo "SNMP" ("Simple Network Management Protocol") es utilizado para realizar labores de monitoreo y control en los equipos que interactúan en la red. Con este protocolo, se puede administrar los diversos equipos en forma remota e identificar conflictos o fallas en los mismos. Usualmente los equipos (servidores y otros componentes de la red) vienen configurados para responder a las peticiones "SNMP" cuando le son solicitados bajo el nombre de comunidad "public", el cual está configurado bajo este esquema en los servidores evaluados.	La utilización de la comunidad genérica "public" del protocolo "SNMP" en los equipos de red es ampliamente conocida y un intruso puede utilizar este hecho para identificar el tipo de componentes instalados en la red y la topología de la misma.
Los recursos compartidos administrativamente al instalar el sistema operativo no han sido removidos.	Windows NT Server cuando es instalado, crea automáticamente recursos compartidos para labores de administración, además de crear un directorio compartido en la raíz de cada volumen. En este sentido, se observó que no han sido removidos los recursos administrativos por defecto en los servidores evaluados.	Aun cuando estos recursos poseen privilegios apropiados al tipo de usuario que hace uso de éstos, dado un eventual acceso por parte de personas no autorizadas con un perfil privilegiado, es importante acotar que esta configuración expone la totalidad de recursos contenidos en los discos duros o en directorios, que no requieren estar publicados para el uso normal de los servidores.
No ha sido desactivado el cifrado "LANMAN" de contraseñas en	La plataforma Windows cuenta con algoritmos distintos para el	Esta situación, le permite a un usuario no autorizado descifrar

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
los servidores evaluados.	cifrado de las contraseñas de los usuarios, tales como "LanMan", "NTLM" y "NTLMV2". El algoritmo "LanMan" permanece para mantener la compatibilidad con plataformas distintas a Windows NT (Windows 95 ó 98), el cual presenta debilidades en su cifrado. En este sentido, se pudo detectar que este algoritmo no ha sido desactivado en los servidores evaluados.	los "hashes" (patrones cifrados de las contraseñas) en poco tiempo, debido a que el algoritmo "LanMan" divide la contraseña en dos (2) partes de siete (7) caracteres, así como también convierte todos los caracteres a mayúsculas. Esto reduce el tiempo de búsqueda notablemente, permitiendo calcular todas las posibles contraseñas alfanuméricas en un tiempo máximo de doce (12) horas en un procesador Pentium III 800mhz.
Existen servicios activos que no son requeridos por los servidores evaluados.	Los servidores evaluados tienen varios servicios activos que no son requeridos para su operatividad. En este sentido, a continuación se muestran los servicios más empleados por intrusos y virus que pudieran ser desactivados: – Remote Procedure Call (RPC): es un utilitario del sistema operativo que permite la ejecución remota de aplicaciones en los servidores. Este crea una brecha de seguridad en el sentido que supedita el control que ofrece la seguridad de acceso físico, ya que no es necesario ingresar por la consola para efectuar la administración y ejecutar aplicaciones de forma remota en los servidores de la red. – Alerter y Messenger: son	Esta situación, pudiera ser utilizada por personas no autorizadas para obtener información relacionada a usuarios, recursos, hardware y sistema operativo. Asimismo, en relación al servicio VNC, dado que el cifrado de su contraseña en el registro de Windows 2000 es poco robusto y adicionalmente no se ha restringido el acceso remoto al Registro, es posible mediante herramientas gratuitas y públicas en la Internet, descifrar la contraseña del mismo y gestionar de forma remota la consola de los servidores.

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	servicios utilizados para mensajería y alertas. Estos servicios proporcionan cierta información relacionada a la red. – Schedule: Servicio empleado para ejecutar tareas programadas. – WinVNC: Servicio empleado para administración remota vía consola, cuya contraseña se encuentra cifrada con un mecanismo poco robusto en el registro de Windows 2000.	
No han sido renombradas las cuentas "Administrator" y "Guest" en los servidores evaluados.	En los servidores evaluados, las cuentas "Administrator" y "Guest" no han sido renombradas. Windows NT al momento de su instalación crea las referidas cuentas y aquellas personas que desean tener acceso no autorizado al sistema, usualmente intentan adivinar la contraseña de los usuarios creados en tiempo de instalación.	Este estándar es conocido públicamente y aquellas personas tales como los "Hackers", que desean hacer accesos no autorizados al sistema, frecuentemente intentan descifrar la clave de los usuarios creados por instalación, incrementando la posibilidad que el uso de esta cuenta se vea comprometido. Windows 2000 ofrece la posibilidad de cambiar el nombre a cualquier usuario sin tener que eliminarlo y volverlo a definir.
No han sido habilitados los esquemas de seguridad para puertos en los servidores Windows 2000	La Institución no tiene implantado un esquema de seguridad a nivel del protocolo de telecomunicaciones TCP/IP en los servidores evaluados, lo cual significa que todos los puertos del referido protocolo se encuentran activos. En el	TCP/IP es un protocolo ampliamente estudiado, por lo que ha sido utilizado y manipulado para obtener acceso a información sensible. Por este motivo, los sistemas operativos han incorporado controles sobre el entorno de TCP/IP, los cuales

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	entorno de redes Windows NT, se emplea intensivamente el protocolo de comunicaciones TCP/IP.	no están habilitados en los servidores mencionados.
Existen vulnerabilidades del servicio IIS que permiten la ejecución de código en los servidores Web.	En los servidores Web tanto de producción como el de desarrollo, se detectaron tres vulnerabilidades relacionadas al uso del "Internet Information Server", las cuales no han sido corregidas con las actualizaciones liberadas por el proveedor.	El 10 de Agosto de 2000, en el boletín de seguridad de Microsoft MS00-057 (http://www.microsoft.com/ technet/ treeview/?url=/ technet/security/ bulletin/ MS00-057.asp), se reportó una vulnerabilidad relacionada con la forma en que IIS maneja un URL que contenga ".." y representaciones de los caracteres "\" o "/", esta vulnerabilidad permite a un atacante ejecutar código no autorizado de manera remota. En fecha 14 de mayo de 2001 en el boletín de seguridad de Microsoft MS01-026 (http://www.microsoft.com/ technet/treeview/ default.asp?url=/ technet/security/ bulletin/ ms01-026.asp), se reportó ua vulnerabilidad relacionada al manejo de seguridad de los URL que realiza IIS. Esta vulnerabilidad permite a un atacante obviar las restricciones de directorios virtuales, permitiéndole ejecutar comandos de manera remota. El 17 de Marzo del 2003, en el boletín de seguridad de Microsoft MS03-007 (http://www.microsoft.com/

Tabla N° 7. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
		technet/treeview/ ?url=/technet/ security/bulletin/ MS03-007.asp), se reportó una vulnerabilidad de desbordamiento de buffer en el componente WebDav de IIS, que permite a un atacante ejecutar código de manera remota.

Tabla N° 8. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Unix)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
Las contraseñas de las cuentas definidas en el servidor Unix del ambiente de desarrollo son de fácil deducción.	Las cuentas creadas en el ambiente Unix de desarrollo poseen contraseñas de fácil deducción, dado que están definidas con palabras relacionadas con el nombre de la Institución y otras son iguales al nombre del usuario.	Esta situación le permite a un intruso deducir las contraseñas de las cuentas definidas en el ambiente de desarrollo como la cuenta "root"; lo cual permitirá mediante herramientas especializadas descifrar el resto de las cuentas definidas. Por otra parte, dado que ambos servidores tienen relación de confianza con el usuario "root", un intruso podría acceder al ambiente de producción y descifrar todas las cuentas definidas en el mismo.
Existen relaciones de confianza entre los servidores Unix evaluados.	Actualmente entre los servidores Unix evaluados existe relación de confianza con el super usuario "root", en donde al acceder a cualquiera de los servidores con este usuario, se puede acceder al otro servidor sin necesidad de	Esta situación genera un riesgo de seguridad para los activos de información de la Institución, destacando que la contraseña del super usuario "root" del servidor de desarrollo es de fácil deducción, por lo que un intruso puede acceder sin

Tabla N° 8. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Unix)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	autenticación.	mayores inconvenientes el servidor de producción, interrumpiendo la continuidad operativa de la base de datos ORACLE o manipular la información confidencialidad que contiene.
El Banner de los protocolos "FTP", "Telnet" y "SMTP" presentan información para identificar características de los servidores evaluados.	Los servicios TCP/IP se inician solicitando una conexión al puerto asignado a cada uno de éstos, de esta manera se puede identificar el nombre de red asignado a los servidores, el tipo de sistema operativo, proveedor y la versión del servicio que se encuentra instalado.	Los servicios mencionados presentan mensajes de conexión, los cuales permiten identificar la plataforma que opera sobre el equipo facilitando las labores de planificación de ataques por parte de intrusos.
No se están empleando mecanismos seguros de conexión y transferencia de información mediante los servicios "Telnet" y "FTP".	Actualmente no se está empleando ningún mecanismo de conexión segura ("Secure Shell - SSH") hacia los equipos, en donde se empleen los servicios "Telnet" y "FTP" para la transmisión de información, lo cual incluye las contraseñas de los usuarios que establecen conexión con estos servicios, pudiendo evitar que se transmita la información y contraseñas en texto claro (leíble).	Esta situación representa una brecha de seguridad, debido a que una persona no autorizada puede capturar, mediante herramientas especializadas, usuarios y contraseñas que son transmitidos en texto claro por la red, pudiendo ingresar posteriormente en los servidores, obtener información confidencial e interrumpir la continuidad operativa de los mismos.
La totalidad de los usuarios del ambiente Unix pueden utilizar el protocolo "FTP".	Los servidores evaluados permiten la utilización del protocolo FTP (File Transfer Protocol) a la totalidad de usuarios.	Este tipo de configuración incrementa el riesgo que personas con intereses en contra de la Institución, pudiesen reemplazar u obtener información contenida en dichos servidores, que no se encuentre restringida de forma adecuada. Adicionalmente, en

Tabla N° 8. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Unix)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
		caso que alguna de las cuentas definidas sea deducida su contraseña por un intruso, podría ser usada para extraer o copiar información sensitiva.
El servicio "SendMail" se encuentra activo en los servidores evaluados.	En los servidores Unix evaluados se encuentra activo el servicio de correo SMTP ("Simple Mail Transfer Protocol") identificado como "Sendmail", destacando que dicho servicio no es requerido por las funciones que desempeñan los servidores.	La configuración de este servicio presenta las siguientes debilidades: – Los servidores soportan los comandos ESMTP ("Extended SMTP") lo cual permite la utilización de los comandos "VFRY" y "EXPN" desde cualquier servidor o estación de trabajo de la red de la Institución. Estos comandos proveen al intruso o usuario que intenta acceder de forma no autorizada, identificar cuales son los perfiles válidos definidos en el ambiente. – Posibilidad de falsificar el servidor emisor del correo, lo cual puede ocasionar la llegada de correos cuyo servidor origen no existe. – Esta situación puede ser utilizada para degradar el rendimiento de los servidores.
Se detectaron servicios activos sin ser requeridos por los servidores acorde a sus funcionalidades.	Los servidores evaluados tienen activos una serie de servicios los cuales no ser requeridos. En este sentido, de los servicios activos en los servidores evaluados, los	A continuación se describe cada uno de los servicios activos que pudieran comprometer los servidores evaluados:

Tabla N° 8. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Unix)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	mostrados a continuación tienden a ser usados frecuentemente por intrusos: – Rstatd – Rusersd – Daytime – Exec – Chargen – echo	– "rstatd": Muestra estadísticas sobre la "ETHERNET" y el "Kernel" del equipo donde se esté ejecutando. – "rusersd": Proporciona información sobre quién está conectado a la red desde un equipo remoto. – "daytime": Proporciona información del día y hora en un formato similar al resultado de la orden "date". Esta información se muestra al recibir una petición de conexión al puerto 13 TCP/UDP. – "exec": Consiste en la recepción de solicitudes para la ejecución de comandos en el servidor. – "chargen": Es un generador de caracteres que se utiliza sobre todo para comprobar el estado de las conexiones de red y cuando se accede a este servicio, se ve en el terminal una secuencia de caracteres ASCII que se repite indefinidamente. – "echo": Este servicio en conjunto con el "chargen" pueden producir gran cantidad de tráfico entre varios equipos, lo cual puede ser utilizado por

Tabla N° 8. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Unix)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
		intrusos para ejecutar ataques de negación de servicio. Esta situación pudiera ocasionar una brecha de seguridad, ya que un intruso puede valerse de ciertos servicios e información que suministran para lograr obtener acceso a los activos de información e interrumpir la continuidad operativa de los servidores.
La cuenta del super usuario "root" en los dos servidores Unix evaluados, no están restringidos para conexiones remotas.	Actualmente, desde cualquier equipo activo conectado a la red de la Institución, podría ejecutar intentos de conexión remota empleando por ejemplo el comando "Telnet" hacia los servidores Unix evaluados.	Esta situación, le facilita a un intruso o persona no autorizada conectarse con la cuenta "root" sin ser detectado oportunamente mediante los registros de auditoría.
No se encuentra limitado la ejecución del comando "su" en los servidores evaluados.	No se encuentra restringido el uso del comando "su" para las cuentas de usuarios que no lo requieren en los servidores evaluados.	Esta situación, le facilita a un intruso la posibilidad de elevar sus privilegios de acceso sobre el sistema operativo.

Tabla N° 9. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
La contraseña de la cuenta "sa" (System Administrator) del manejador de base de datos SQL Server en los servidores Web es trivial.	Empleando un cliente de SQL Server instalado en el equipo portátil empleado, se procedió a intentar establecer sesiones con la cuenta "sa". En este sentido, en el ambiente de desarrollo la misma no tenía contraseña y en el ambiente de producción la contraseña era el nombre de la Institución "XXX".	Esta situación trae como consecuencia que un intruso puede acceder con privilegios administrativos a las bases de datos creadas en el manejador de base de datos SQL Server en los servidores WEB evaluados; pudiendo de esta manera afectar el servicio WEB que presta la Institución "XXX" a sus clientes.

Tabla N° 9. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
El manejador de bases de datos "SQL Server" presenta vulnerabilidades que permiten accesos no autorizados.	El manejador de base de datos SQL Server instalado en los servidores Web, presenta dos vulnerabilidades que podrían facilitar el acceso no autorizado con privilegios administrativos a información confidencial.	El 24 de julio del 2002 se reportó una vulnerabilidad en el manejo de la pila del servicio de resolución de SQL Server 2000, en el boletín de seguridad de Microsoft MS02-039 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security /bulletin/ms02-039.asp) la cual puede ser aprovechada por un atacante para ganar privilegios administrativos en el servidor. Adicionalmente, se detectó otra vulnerabilidad en el manejo del buffer en el proceso de autenticación de SQL Server 2000 reportada el 31 de octubre de 2002 en el boletín de seguridad de Microsoft MS02-056 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-056.asp), esta vulnerabilidad puede ser aprovechada por atacantes para obtener privilegios administrativos en los servidores afectados.
Las claves por defecto de los usuarios preestablecidos en el manejador de base de datos ORACLE no han sido cambiadas.	Cuando se instala una base de datos ORACLE, se crean varios usuarios preestablecidos los cuales tienen contraseñas por defecto. Durante la revisión se identificaron ocho (8) usuarios en el manejador de base de datos en los servidores Unix que presentan estas contraseñas por defecto. En este sentido, a continuación se	La existencia de usuarios con contraseñas definidas por defecto, representa un riesgo para los activos de información de la Institución, considerando que dichas contraseñas se encuentran públicas en la Internet, libros, etc; y una vez conocidas, se pudiera tener acceso a información del

Tabla N° 9. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
	presenta los usuarios detectados: – System, Sys e Internal: Son cuentas iniciales desde la que se hace la mayor parte de la creación de objetos. Estas cuentas son creadas durante la instalación y uno de sus roles asignados es el DBA. – Scott: Sirve como herramienta útil para aprender SQL (Structured Query Languaje) y probar la conexión con la red de la base de datos y del sistema. – DBSNMP: Se utiliza para apoyar al ORACLE Enterprise Manager (OEM) Intelligent Agent en la administración de la base de datos remota. – Clark: Es una cuenta asociada de Scott con privilegios mínimos. – Ordsys: Se utiliza para apoyar la opción Time Series Option de Oracle, que sirve para activar el trabajo con calendarios y datos de series de tiempo. – Mtssys: Se utiliza para sustentar al servidor Microsoft Transaction Server y al software Microsoft Application Demo.	manejador de base de datos ORACLE mediante la aplicación "SQLPlus". Adicionalmente, hay que destacar que en ORACLE se encuentra todas las transacciones financieras de la Institución "XXX".

Tabla N° 9. Vulnerabilidades y riesgos identificados desde la red interna (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Hallazgo**	**Riesgo**
Se detectaron cuentas de usuarios definidas en el grupo "DBA" sin ser requeridas.	En el grupo "ORADB" de los servidores Unix que soportan el ambiente ORACLE de desarrollo y producción, se encuentran definidas cuentas de usuarios que no requerida acorde a sus funcionalidades.	A partir de las versiones de ORACLE superiores a la 7, toda cuenta de usuario definida a nivel del sistema operativo en los grupos "ORA_DBA" para Windows y "ORADB" para Unix, pueden acceder de forma anónima con privilegios "SYSDBA" al manejador.
Los permisos de acceso a nivel de sistema operativo sobre los directorios, archivos y utilitarios no han sido adecuadamente configurados.	Tanto en el servidor Unix de desarrollo como en el de producción, no han sido configurados adecuadamente los accesos sobre los recursos pertenecientes al manejador de base de datos ORACLE. Entre los recursos relacionados se encuentran los siguientes con permiso de acceso World Writable: – Ufl – Oracle_home – Oracle_home\dbs – Oracle_home\rdbms – Oracle_home\rdbms\log – Oracle_home\rdbms\audit – Oracle_home\rdbms\public – Oracle_home\root.sh – Oracle_home\network – Oracle_home\bin – Oracle_home\bin\oracle – Oracle_home\bin\dbsnmp – Oracle_home\bin\sqlplus	Esta situación puede traer como consecuencia posibles accesos no autorizados a la información confidencial de la Institución, mediante la ejecución de utilitarios como "sqlplus" por parte de intrusos que logren obtener una cuenta válida en los servidores Unix, prestando especial atención sobre el ambiente de producción.

3. Ambientes tecnológicos que pueden ser accedidos de manera no autorizada por "Intrusos"

Identificada la plataforma tecnológica de la Institución "XXX" de manera anónima y detectando las vulnerabilidades y riesgos a los que se encuentra expuesta, se procedió a efectuar accesos no autorizados a los recursos sensitivos o activos de información por las vías identificadas. En este sentido, a continuación se presentan los resultados obtenidos:

3.1. Ambientes tecnológicos que pueden ser accedidos de manera no autorizada desde Internet

Los componentes tecnológicos que pueden o pudieran ser accedidos de manera no autorizada son los siguientes:

Tabla N° 10. Ambientes que pueden ser accedidos desde Internet

Componente	Causas principales
Router	– Responde a solicitudes de "SNMP" bajo el nombre de la comunidad "Public", lo que permitió identificar el modelo. – Acepta solicitudes de conexión "Telnet" desde cualquier dirección de Internet. – La contraseña de acceso al Router Cisco en modo usuario y en modo administrador, está relacionada directamente con el nombre da la Institución "XXX". Comentario: Acceso efectivo en corto tiempo.
Firewall	– Los puertos activos revelan el modelo del Firewall utilizado. – Responde a solicitudes "Telnet" por el puerto "259" y "http" por el puerto "900" desde cualquier dirección de Internet. Comentario: Acceso no efectivo, dado que se requiere de herramientas especializadas ejecutando continuos intentos de acceso por largo período.
Servidor Web	– Provee por el puerto "80" la versión del IIS "Internet Information Server"

Tabla N° 10. Ambientes que pueden ser accedidos desde Internet	
Componente	**Causas principales**
	– El IIS presenta tres vulnerabilidades las cuales no han sido corregidas con las actualizaciones liberadas por el proveedor. Comentario: Acceso efectivo en corto tiempo.

3.2. Ambientes tecnológicos que pueden ser accedidos de manera no autorizada desde la red interna

Los componentes tecnológicos que pueden o pudieran ser accedidos de manera no autorizada son los siguientes:

Tabla N° 11. Ambientes que pueden ser accedidos desde la red interna (Ambiente de Red)	
Componente	**Causas principales**
Router y Switches	– Responden a solicitudes de "SNMP" bajo el nombre de la comunidad "Public", lo que permitió identificar los modelos, los cuales son "CISCO". – Aceptan solicitudes de conexión "Telnet" desde cualquier dirección interna. – La contraseña de acceso en modo usuario y en modo administrador, están relacionadas directamente con el nombre da la Institución "XXX". Comentario: Acceso efectivo en corto tiempo.

Tabla N° 12. Ambientes que pueden ser accedidos desde la red interna (Ambiente Wireless)	
Componente	**Causas principales**
Access Points	– Su alcance trasciende las instalaciones de la Institución. – Puede ser accedido en forma anónima vía "http". Comentario: Acceso efectivo en corto tiempo.

Tabla N° 13. Ambientes que pueden ser accedidos desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Componente	**Causas principales**
Estaciones de Trabajo	– Ineficientes mecanismos de monitoreo. – Permiten consultas anónimas. – El orden de inicio de las estaciones de trabajo es inadecuado. – No tienen contraseñas del BIOS.

Tabla N° 13. Ambientes que pueden ser accedidos desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Componente	**Causas principales**
	– Poseen recursos compartidos administrativamente. – El mecanismo de cifrado de las contraseñas locales es "LANMAN" y no "NTLM". – La cuenta local de administración y su contraseña es la misma en todas las estaciones de trabajo. Comentario: Acceso efectivo en corto tiempo.

Tabla N° 14. Ambientes que pueden ser accedidos desde la red interna (Ambiente Windows 2000 – Servidores)	
Componente	**Causas principales**
Servidores	– Registros de auditoría configurados inadecuadamente en el servidor de "Active Directory" y no activada en el resto de los servidores. – Ineficiente monitoreo de actividades inusuales. – Responden a solicitudes de consultas "SNMP" con comunidad "Public" y a "NetBios". – Permiten consultas anónimas. – El bloqueo de las cuentas de usuarios es inadecuado servidor de "Active Directory" y no activado en el resto de los servidores. – El acceso remoto al registro no se encuentra restringido. – Poseen recursos compartidos administrativamente. – El mecanismo de cifrado de las contraseñas locales es "LANMAN" y no "NTLM". – Cuentas de usuarios en desuso y que no han cambiado su contraseña por largo tiempo. – Cuentas de usuarios de fácil deducción con privilegios administrativos. – En el caso de los servidores WEB, presentan vulnerabilidades por el servicio IIS. Comentario: Acceso efectivo en corto tiempo.

Tabla N° 15. Ambientes que pueden ser accedidos desde la red interna (Ambiente Unix)	
Componente	**Causas principales**
Servidores	– Mensajes que revelan el sistema operativo empleado mediante los "Banners" de conexión "Telnet", "Ftp" y "smtp".

	– El tráfico de información que se maneja hacia los servidores Unix, no está siendo cifrada. – Existe relación de confianza del servidor de desarrollo al servidor de producción con el usuario "root". – Es posible captura usuarios y contraseñas válidas mediante la ejecución de ataques "Man in the Middle" – La contraseña de la cuenta "root" del servidor de desarrollo es de fácil deducción. Comentario: Acceso efectivo en corto tiempo.

Tabla N° 16. Ambientes que pueden ser accedidos desde la red interna (Ambiente Oracle y SQL Server)

Componente	Causas principales
Oracle	– Contraseñas definidas por defecto para las cuentas "System", "Sys", "Internal", "Scott", "dbsnmp", "Clark", "Ordsys" y "Mtssys". – Cuentas de usuarios definidas en el grupo "DBA" del ambiente Unix, lo que permitió acceder con privilegios "SYSDBA" al manejador de forma anónima. Comentario: Acceso efectivo en corto tiempo.
SQL Server	– La contraseña de la cuenta de administración "sa" posee una contraseña de fácil deducción. – El manejador de base de datos presenta dos vulnerabilidades que podrían facilitar el acceso no autorizado con privilegios administrativos a información confidencial. Comentario: Acceso efectivo en corto tiempo.

CAPITULO V

SITUACION PROPUESTA

1. Recomendaciones emitidas para mitigar los riesgos de seguridad identificados en la plataforma tecnológica de la Institución "XXX"

A continuación se describen las recomendaciones necesarias a implantar en cada uno de los componentes que constituyen la plataforma tecnológica de la Institución "XXX", para mitigar los riesgos identificados con posibles intentos de acceso no autorizado a los activos de información de la Compañía, desde Internet (Externamente) y desde la Red privada (Internamente).

1.1. Recomendaciones para mitigar los riesgos de acceso externos (Desde Internet) a los activos de información de la Compañía

Tabla N° 17. Recomendaciones para mitigar riesgos de acceso desde Internet

Vulnerabilidad	Recomendación
El Router de Internet posee un nombre trivial de comunidad SNMP	El protocolo "Simple Network Management Protocol" (SNMP) permite el monitoreo de algunas labores de administración remota de los componentes de red y opera bajo esquemas de solicitud de información, utilizando un nombre de comunidad específico. Este parámetro debe ser modificado de su valor conocido ("public", "admin" o "cable-docsis") por una denominación no trivial, que dificulte su deducción por parte del intruso.
Se detectaron puertos del Router evaluado abiertos a Internet que pudieran comprometer su operatividad.	Restringir el acceso desde redes no confiables al Router evaluado. Asimismo, se recomienda deshabilitar los puertos bajos (menores del 1024) mediante las instrucciones "no service tcp-small-servers" y "no service udp-small-servers".
El Router de Internet acepta conexiones externas vía "Telnet" desde cualquier dirección IP.	Restringir la posibilidad de establecer conexiones desde redes no confiables vía "Telnet" a ninguna de las interfaces del Router, particularmente la que responde a la dirección pública.

Tabla N° 17. Recomendaciones para mitigar riesgos de acceso desde Internet	
Vulnerabilidad	**Recomendación**
El Firewall permite el flujo de paquetes "ICMP" ("Internet Control Message Protocol") desde Internet hacia los equipos ubicados en la "DMZ".	Restringir mediante las políticas del Firewall el flujo de solicitudes "ICMP" desde Internet hacia la red interna o privada de la Compañía.
El Firewall responde a conexiones externas por varios puertos abiertos desde Internet por donde se obtiene información confidencial.	Restringir todo acceso desde redes no confiables e Internet, a establecer cualquier tipo de conexión por los puertos activos actualmente en el Firewall. Asimismo, se recomienda evaluar la posibilidad de deshabilitar los puertos que no sean requeridos actualmente.
El servidor de correo electrónico y WEB muestra hacia Internet información confidencial para la Compañía.	Eliminar o modificar el mensaje "Banner" que se muestra al establecer conexión directa al puerto "25 - smtp" del servidor de correo y al puerto "80 – http" del servidor Web . Evitando de esta manera, que un intruso pueda obtener información confidencial para la Compañía.
El servidor de correo no restringe los ataques de tipo "spam"	Evaluar las medidas técnicas descritas en el documento "RFC 2505 (Anti-Spam Recomendations for SMTP MTAs, febrero de 1999)", con el objetivo de implantar mecanismos de seguridad que disminuyan una posible proliferación de correos no deseados en la Compañía. Entre los aspectos que se tratan en el documento mencionado, como medidas de protección se encuentran: ✓ Recopilación y validación de datos. ✓ Organización centralizada del servicio de correo. ✓ Control sobre la procedencia y destino de los mensajes. ✓ Control de flujo. A continuación se presenta el link para obtener el archivo ".pdf" del documento "RFC 2505": http://www.faqs.org/rfcs/rfc2505.html.pdf

1.2. Recomendaciones para mitigar los riesgos de acceso internos (Desde la red privada) a los activos de información de la Compañía

Tabla N° 18. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente de Red)	
Vulnerabilidad	**Recomendación**
No se encuentran deshabilitados los puntos de red que no están siendo utilizados y no se han configurado los que se requieren con la dirección física de la estación de trabajo conectada.	Para mitigar los riesgos asociados a esta situación, se recomienda deshabilitar los puntos de red que no estén siendo requeridos e identificarlos apropiadamente. Adicionalmente, se recomienda que los puntos de red que estén siendo utilizados, sean configurados para que sólo acepten peticiones de la estación de trabajo que tengan conectados, es decir, que reconozcan la dirección física de la máquina ("Mac-Address").
El Firewall no restringe el flujo de paquetes ICMP desde la red Interna hacia la Zona Desmilitarizada "DMZ" y viceversa.	Definir en el Firewall de la Institución el filtrado de paquetes ICMP (Internet Control Message Protocol) a excepción de los administradores, de manera que los servidores y equipos críticos no respondan a dichas solicitudes.
No existen mecanismos o sistemas de detección de intrusos en red (NIDS).	Implantar sistemas de detección de intrusos (NIDS) con la finalidad de identificar y tomar acciones oportunas ante intentos de acceso no autorizado o actividades sospechosas contra los componentes que conforman la red de la Institución "XXX".
No se cuenta con mecanismos de seguridad para restringir el redireccionamiento de "Mac Address" en los equipos críticos de la Institución.	En vista que un ataque "Man in the Middle" resultaría relativamente sencillo de realizar por un intruso, falsificando mediante herramientas especializadas las respuestas "ARP" y engañar la mayoría de los equipos que se encuentren conectados a la red, una de las soluciones más efectivas para minimizar los riesgos asociados con esta brecha de seguridad es configurar las entradas "ARP" estáticas en los equipos críticos e implantar procedimientos de monitoreo constante sobre los mismos. Para llevar a cabo esta recomendación, se sugiere implantar los mecanismos de seguridad que se detallan a continuación: – Configurar las direcciones "ARP" de los servidores de forma estática en cada uno de los equipos o estaciones de trabajo de la Institución, evitando de esta manera, que el tráfico de información de las estaciones de trabajo hacia los servidores sea redireccionado hacia el equipo del atacante. El comando para configurar las direcciones "ARP" estáticas en cada una de las estaciones de

Tabla N° 18. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente de Red)	
Vulnerabilidad	**Recomendación**
	trabajo es el siguiente: "**arp –s <ip address><MAC-Address>"** – Definir procedimientos de monitoreo constante de las "MAC-Address" registradas en los servidores con el fin de detectar cualquier duplicidad en un momento dado. A tales efectos y para simplificar el proceso de monitoreo, se recomienda desarrollar e implantar una herramienta que permanezca activa en los servidores verificando cada cierto tiempo el comportamiento de las "MAC-Address" registradas.
Los Routers y Switches responden al nombre de comunidad "Public" del protocolo SNMP.	El protocolo "Simple Network Management Protocol" ("SNMP") permite el monitoreo y administración remota de los componentes de red y opera bajo esquemas de solicitud de información, utilizando un nombre de "comunidad" específico. Este parámetro debe ser modificado de su valor original ("public") por una denominación no trivial, que dificulte su deducción por parte del intruso. En caso de que no sea necesario este protocolo en los servidores, se recomienda desactivarlo.
Las contraseñas de acceso a los Routers y Switches de la Institución son de conocimiento público.	Cambiar las contraseñas de conocimiento público o definidas por defecto por los proveedores de los Routers y Switches por una denominación no trivial, la cual sea de difícil deducción por parte de intrusos.

Tabla N° 19. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Wireless)	
Vulnerabilidad	**Recomendación**
La configuración de los componentes activos de la red inalámbrica ("Access Points") puede ser accedida en forma anónima desde la red fija o cableada.	Debido a que las páginas web para configurar el "Access Point" presenta información suficiente para facilitarle a un usuario no autorizado obtener acceso a la red fija o cableada mediante la red inalámbrica, se recomiendan las siguientes alternativas: – Deshabilitar la administración Web del "Access Point". – Definir controles de accesos para todos los elementos de la administración Web del "Access Point" en caso de ser requerida. – Restringir el acceso a la administración Web del "Access Point" mediante el uso de un Firewall.
No existen mecanismos para	Para minimizar los riesgos de acceso por parte de usuarios no

Tabla N° 19. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Wireless)	
Vulnerabilidad	**Recomendación**
controlar el flujo de información desde la red inalámbrica hacia la red fija o cableada.	autorizados que se encuentren fuera de las instalaciones de la Institución, se recomienda tomar en consideración la creación de un esquema de DMZ (Zona desmilitarizada) similar al siguiente: – Crear una subred distinta para los equipos pertenecientes a la red inalámbrica, utilizando preferiblemente direcciones IP inválidas por ejemplo: 10.*.*.* – Colocar un Firewall entre la red fija y la red inalámbrica que controle el tráfico de información. Es importante destacar, que existen "Access Point" que incluyen las funciones de Firewall.
El "Access Point" no tiene configurado la opción de cifrado de información.	Debido a que las redes inalámbricas son más susceptibles a ataques externos, se recomienda reforzar los controles que esta posee, de la siguiente manera: – Activar los parámetros de cifrado, preferiblemente utilizando el protocolo "WEP", con claves de 128 bits. – Establecer una "VPN" para los equipos pertenecientes a la red inalámbrica. – Crear mecanismos para el cambio periódico del "ESSID". – Establecer un mecanismo más robusto para el control de las listas de acceso por dirección "MAC", utilizando posibles combinaciones de valores tales como: • Dirección MAC • Nombre del Equipo • Número IP • Fecha/Hora de la Conexión

Tabla N° 20. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Vulnerabilidad	**Recomendación**
No han sido restringidas las consultas anónimas hacia las estaciones de trabajo.	Para restringir la solicitud de consulta de usuarios anónimos mediante el uso del servicio "Lan Manager", se recomienda modificar la siguiente clave del registro: **Clave:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa **Tipo:** REG_DWORD **Valor:** RestrictAnonymous = 1

Tabla N° 20. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Vulnerabilidad	**Recomendación**
La contraseña de la cuenta de administración local es común en varias estaciones de trabajo, siendo ésta de fácil deducción.	Con el propósito de minimizar los riesgos de acceso no autorizado a las estaciones de trabajo, se recomienda implantar los siguientes controles de seguridad: – Definir una contraseña robusta para la cuenta de administración local de las estaciones de trabajo, constituida por caracteres numéricos, especiales y alfanuméricos en mayúsculas y minúsculas. – Configurar la longitud mínima de la contraseña a ocho (8) caracteres. – Evaluar la posibilidad de generar contraseñas aleatorias individuales para cada equipo basándose en semillas únicas como por ejemplo el nombre del equipo.
El orden de inicio de las estaciones de trabajo permite utilizar discos de arranque para omitir el proceso de carga del sistema operativo y la contraseña de configuración del "BIOS" no está definida.	Definir un plan de acción para implantar las recomendaciones, tomando como prioridad las estaciones de trabajo de usuarios que manejan información crítica para la Institución. En este sentido a continuación se presentan las actividades que se sugieren implantar: – Para evitar que el proceso de carga del sistema operativo Windows 2000 de las estaciones de trabajo sea omitido empleando "diskettes" o "CDs" de inicio, se sugiere configurar en el "BIOS", que el disco duro sea la primera opción de lectura que realiza la secuencia de arranque en busca de los archivos de inicio. – Definir una contraseña de acceso a la configuración del "BIOS" de las estaciones de trabajo. Los pasos para definir la contraseña del "BIOS" son los siguientes: • Presionar la tecla F2 al momento de arranque. • Seleccionar la opción "System Security": ➢ Dentro de este menú seleccionar la opción"Setup Password". ➢ Definir una contraseña robusta y mantenerla almacenada en un lugar seguro. – Configurar los protectores de pantalla con contraseñas en las estaciones de trabajo definiendo como intervalo de tiempo para su

Tabla N° 20. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Vulnerabilidad	**Recomendación**
	activación de 10-15 minutos aproximadamente, a fin de optimizar la seguridad de las mismas y la plataforma tecnológica.
No ha sido removida la compartición administrativa en las estaciones de trabajo.	Con el fin de mitigar los riesgos asociados con esta debilidad, se recomienda eliminar la compartición administrativa en la totalidad de las estaciones de trabajo Windows 2000, mediante la modificación desde el editor del registro "regedt32", de la siguiente clave: **Clave:** HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\ LanmanWorkstation\Parameters **Tipo:** REG_DWORD **Valor:** AutoshareWks = 0
No se detectaron mecanismos para el control de aplicaciones instaladas de manera no autorizada en las estaciones de trabajo.	Dado que es posible instalar aplicaciones sin autorización en las estaciones de trabajo, producto de la inexistencia de mecanismos para su detección, se recomienda instalar herramientas para el monitoreo y detección de posibles aplicaciones que puedan comprometer la seguridad de la Institución. Es importante destacar, que deben evaluarse aplicaciones cuyas bondades permitan emitir mensajes de alerta tanto para el propietario de la estación de trabajo en cuestión, como al administrador de la red.
El protocolo "Netbios" se encuentra activo en las estaciones de trabajo.	Dado que el protocolo "Netbios" se encuentra habilitado en las estaciones de trabajo Windows 2000, se incrementa el riesgo de obtención de información relevante sobre los componentes que integran la red de la Compañía. En este sentido, parte de la información que puede obtener un intruso mediante "Netbios" proviene de la enumeración de equipos, por lo que se recomienda deshabilitar el servicio "Server Message Block" ("SMB") para mitigar los riesgos asociados a esta debilidad. Para deshabilitar el servicio "SMB", se deben evaluar las siguientes alternativas: – Deshabilitar el servicio de sesión "NetBIOS" (Puerto TCP 139), marcando la opción "Deshabilitar NetBIOS sobre TCP/IP" en la pestaña "Wins" de la ventana "Configuración avanzada de TCP/IP" en aquellos servidores que no requieran de este servicio. Esta recomendación aplica sólo si los servicios "SMB" no son necesarios. – Deshabilitar la opción de compartir impresoras y archivos para redes Microsoft (Puerto TCP 445). Esta configuración debe

Tabla N° 20. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Estaciones de Trabajo)	
Vulnerabilidad	**Recomendación**
	realizarse mediante la pestaña "Adaptadores y enlaces", de la ventana "Configuración avanzada" para conexiones de red y acceso telefónico. Con esta opción deshabilitada no se podrán compartir archivos ni directorios. Esta recomendación aplica sólo si los servicios "SMB" no son necesarios.
Las estaciones de trabajo responden al nombre "Public" de la comunidad del protocolo SNMP.	Para cambiar el nombre de la comunidad en ambientes Windows 2000, se deben seguir los siguientes pasos: – Editar el Registro de las estaciones de trabajo mediante la ejecución del archivo "\Winnt\System32\regedit.exe", modificar la siguiente entrada: **Ruta:** HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services\ SNMP\Parameters\ **Clave:** ValidCommunities **Tipo:** REG_SZ **Valor:** Nombre distinto a "public", "admin" o "private" – Adicionalmente, en la opción del menú "Security | Permissions" del editor de registro, se pueden establecer permisos para el acceso a usuarios autorizados. – Otra opción, es modificar el nombre de la comunidad mediante la interfaz gráfica que ofrece el servicio.
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en las estaciones de trabajo.	Para disminuir la posibilidad de acceder en forma remota al registro del sistema ("registry") se recomienda deshabilitar el servicio "Remote Registry" mediante el acceso a la ventana de servicios de Windows 2000.
No ha sido desactivado el cifrado "LanMan" en las estaciones de trabajo.	Para mitigar el riesgo que esta situación representa, se recomienda modificar la siguiente clave del registro: **Clave:** HKEY_LOCAL_MACHINE\System \CurrentControlSet \control\LSA **Tipo:** REG_DWORD **Valor:** LMCompatibilityLevel = 2 Es importante denotar que el nivel más restrictivo lo representa el valor cinco (5), sin embargo, este pudiera afectar la operatividad y entorpecer la utilización de aplicaciones por parte de los usuarios.

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
La solicitud de consulta de usuarios anónimos mediante el uso del servicio "Lan Manager" en los servidores no ha sido restringida.	Para restringir la solicitud de consulta de usuarios anónimos mediante el uso del servicio "Lan Manager", se recomienda modificar la siguiente clave del registro: **Clave:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Lsa **Tipo:** REG_DWORD **Valor:** RestrictAnonymous = 1
Las políticas de contraseñas de usuarios definidas en el servidor de "Active Directory" no cumple las mejores prácticas de seguridad.	En función de mitigar los riesgos asociados a esta situación, se recomienda: – Activar el bloqueo de cuentas de usuarios en los servidores Web, Correo y Proxy. Para ello se recomienda definir en tres (3) los intentos fallidos de conexión antes de bloquear la cuenta. Asimismo, se recomienda definir en 1440 minutos (24 horas) el contador de intentos fallidos y en 4320 minutos (72 horas) el tiempo que durará bloqueada una cuenta de usuario. – Activar el historial de contraseñas en los servidores evaluados, definiendo en diez (10) el número de contraseñas distintas que deberán ser cambiadas antes de repetir la primera. – Aumentar la longitud mínima de las contraseñas a ocho (8) caracteres en los servidores evaluados. – Configurar en los servidores evaluados el tiempo mínimo para poder cambiar contraseñas en tres (3) días y el tiempo máximo que podrá permanecer con la misma contraseñas en treinta (30) días.
Las bondades de auditoría no se encuentran configuradas en el servidor de "Active Directory" acorde a las mejores prácticas y se encuentra inactiva en los servidores de correo, Web y Proxy.	Activar las opciones de auditoría en el servidor de "Active Directory" siguiendo los lineamientos que se mencionan a continuación: – Audit account logon events (Success / Failure) – Audit account management (Success / Failure) – Audit directory service access (Success / Failure) – Audit logon events (Success / Failure) – Audit object access (Failure) – Audit policy change (Success / Failure) – Audit privilege use (Success / Failure) – Audit system events (Success / Failure) – Audit process tracking Asimismo, para el caso de los servidores de correo, proxy y Web, se

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
	recomienda activar las opciones de auditoría como se describe a continuación: – Audit account logon events (Success / Failure) – Audit account management (Success / Failure) – Audit directory service access – Audit logon events (Success / Failure) – Audit object access (Failure) – Audit policy change – Audit privilege use (Failure) – Audit system events (Success / Failure) – Audit process tracking
Se detectaron usuarios con contraseñas de fácil deducción en los servidores evaluados.	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: – Activar el uso de contraseñas robustas del sistema operativo Windows 2000, colocando en "Enabled" la opción "Password must meet complexity requirements" de las políticas de seguridad de Windows 2000. – Emplear métodos efectivos, como por ejemplo, crear una frase y utilizar la primera letra de cada palabra en la contraseña. – Emplear letras y números mezclando con caracteres especiales. Esto constituye un grado de complejidad aun mayor en la contraseña. – Para el caso de cuentas con privilegios administrativos, se considera que su longitud mínima para la contraseña, debe ser de 12 caracteres. – 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".
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en los servidores evaluados.	Para disminuir la posibilidad de acceder en forma remota al registro del sistema ("registry") se recomienda deshabilitar el servicio "Remote Registry" mediante el acceso a la ventana de servicios de Windows 2000.
Existen deficiencias en la administración de los controles de acceso asignados	Optimizar los controles de acceso definidos a las cuentas de usuarios creadas en el servidor Windows 2000 de "Active Directory" acorde a las siguientes especificaciones y considerando que las mismas no

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
a las cuentas de usuarios definidas en el servidor de "Active Directory".	aplican para cuentas de servicio: – Definir en treinta (30) días el tiempo máximo en que una contraseña puede permanecer invariante. – Permitir a los usuarios que cambien sus contraseñas en el momento que lo consideren conveniente entre el plazo mínimo de tres (3) días y el máximo de treinta (30) días. – Deshabilitar aquellas cuentas de usuarios que se encuentren inactivas por más de noventa (90) días.
El protocolo "Netbios" se encuentra activo en los servidores Windows 2000 evaluados.	Deshabilitar el servicio "SMB", evaluando las siguientes alternativas: – Deshabilitar el servicio de sesión "NetBIOS" (Puerto TCP 139), marcando la opción "Deshabilitar NetBIOS sobre TCP/IP" en la pestaña "Wins" de la ventana "Configuración avanzada de TCP/IP" en aquellos servidores que no requieran de este servicio. Esta recomendación aplica sólo si los servicios "SMB" no son necesarios. – Deshabilitar la opción de compartir impresoras y archivos para redes Microsoft (Puerto TCP 445). Esta configuración debe realizarse mediante la pestaña "Adaptadores y enlaces", de la ventana "Configuración avanzada" para conexiones de red y acceso telefónico. Con esta opción deshabilitada no se podrán compartir archivos ni directorios. Esta recomendación aplica sólo si los servicios "SMB" no son necesarios. En caso que sea necesario el servicio "SMB", se puede habilitar la "firma" de los paquetes "SMB", destacando que esta opción no elimina la posibilidad de enumerar cierta información de los equipos, pero minimiza algunos de los riesgos asociados. Para habilitar la firma de los paquetes "SMB", es necesario seguir los siguientes pasos: – Modificar en el registro de Windows 2000 la clave: **Ruta:** HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services\ LanmanServer\Parameters **Clave:** RequireSecuritySignature **Tipo:** REG_DWORD **Valor:** Uno (1)

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
	– Modificar en el registro de Windows 2000 la clave: **Ruta:** HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services\Rdr\Parameters **Clave:** RequireSecuritySignature **Tipo:** REG_DWORD **Valor:** Uno (1)
Los servidores evaluados responden al nombre "Public" de la comunidad del protocolo SNMP.	El nombre de la comunidad del protocolo "SNMP" debe ser modificado de su valor original ("public") por una denominación no trivial, que dificulte su deducción por parte del intruso. En caso de que no sea necesario este protocolo en los servidores, se recomienda desactivarlo. Para implantar esta recomendación, se deben seguir los siguientes pasos: – Editar el Registro de los servidores mediante la ejecución del archivo "\Winnt\System32\regedit.exe" y modificar la siguiente entrada: **Ruta:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\ SNMP\ Parameters\ **Clave:** ValidCommunities **Tipo:** REG_SZ **Valor:** Nombre distinto a "public", "admin" o "private" – Adicionalmente, en la opción del menú "Security | Permissions" del editor de registro, se pueden establecer permisos para el acceso a usuarios autorizados.
Los recursos compartidos administrativamente al instalar el sistema operativo no han sido removidos.	Con el fin de mitigar los riesgos asociados con esta debilidad, se recomienda eliminar la compartición administrativa en los servidores Windows 2000, mediante la modificación desde el editor del registro "regedt32", de la siguiente clave: **Ruta:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services \LanmanServer\ Parameters **Clave:** AutoShareServer **Tipo:** REG_DWORD **Valor:** Cero (0)

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
No ha sido desactivado el cifrado "LANMAN" de contraseñas en los servidores evaluados.	Para mitigar el riesgo que esta situación representa, se recomienda modificar la siguiente clave del registro: **Clave:** HKEY_LOCAL_MACHINE\System \CurrentControlSet \control\LSA **Tipo:** REG_DWORD **Valor:** LMCompatibility = 2 Es importante denotar que el nivel más restrictivo lo representa el valor cinco (5), sin embargo, este pudiera afectar la operatividad y entorpecer la utilización de aplicaciones por parte de los usuarios.
Existen servicios activos que no son requeridos por los servidores evaluados.	Con el fin de evitar que un intruso atente contra la operatividad de los servidores evaluados, se recomienda deshabilitar los servicios no requeridos como son: – Remote Procedure Call (RPC) – Alerter y Messenger – Schedule – WinVNC
No han sido renombradas las cuentas "Administrator" y "Guest" en los servidores evaluados.	Las cuentas con privilegios administrativos son el principal blanco de los ataques por parte de usuarios no autorizados, por este motivo se recomienda renombrar la cuenta "Administrator" en los servidores evaluados a fin de minimizar el riesgo que sus contraseñas sean descubiertas. Asimismo, la cuenta "Guest" aun cuando no posee privilegios administrativos y se encuentra bloqueada en los servidores, se recomienda de igual forma que sea renombrada por ser conocida públicamente.
No han sido habilitados los esquemas de seguridad para puertos en los servidores Windows 2000.	Windows 2000 permite establecer un esquema de filtrado de puertos TCP y UDP, para ello se debe: – Identificar la totalidad de puertos activos en los servidores Windows 2000 mediante la ejecución de un "port scanner". – Identificar la razón y uso de cada puerto activo y proceder a inhabilitar los servicios innecesarios. Activar los puertos a ser utilizados por las aplicaciones instaladas en los servidores Windows 2000, mediante la opción provista por el sistema operativo.

Tabla N° 21. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Windows 2000 – Servidores)	
Vulnerabilidad	**Recomendación**
Existen vulnerabilidades del servicio IIS que permiten la ejecución de código en los servidores Web.	Debido a la necesidad de mantener tanto el software como el sistema operativo actualizados a la última versión disponible, se recomienda definir e implantar un procedimiento cuyo objetivo debe ser la localización de las actualizaciones más recientes y su oportuna implantación, este procedimiento debe tener en consideración los siguientes aspectos: – Monitorear la información de los proveedores con el fin de detectar nuevas actualizaciones. – Descargar las actualizaciones. – Implantación de las actualizaciones. Debido a las debilidades asociadas con el servicio IIS, se recomienda actualizar estos a sus versiones mas recientes. Para mayor información ver la página Web http://www.microsoft.com/ technet/ y los boletines de seguridad Microsoft correspondientes.

Tabla N° 22. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Unix)	
Vulnerabilidad	**Recomendación**
Las contraseñas de las cuentas definidas en el servidor Unix del ambiente de desarrollo son 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 métodos efectivos, como por ejemplo, crear una frase y utilizar la primera letra de cada palabra en la contraseña. – Emplear letras y números mezclando con caracteres especiales. Esto constituye un grado de complejidad aun mayor en la contraseña. – Para el caso de cuentas con privilegios administrativos, se considera que su longitud mínima para la contraseña, debe ser de 12 caracteres. – 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".
Existen relaciones de confianza entre los servidores Unix evaluados.	Eliminar la relación de confianza existente entre el servidor Unix de producción y desarrollo, y robustecer la contraseña del super usuario "root" en ambos equipos. Adicionalmente, se recomienda supervisar periódicamente los archivos de confianza del ambiente Unix, particularmente los archivos "/etc/hosts.equiv" y "HOME$/.rhosts".

Tabla N° 22. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Unix)	
Vulnerabilidad	**Recomendación**
El Banner de los protocolos "FTP", "Telnet" y "SMTP" presentan información para identificar características de los servidores evaluados.	Editar los archivos de configuración de los demonios "Telnetd", "Ftpd" y "smtpd", eliminando o definiendo un mensaje de conexión que no revele información sobre el nombre de red asignado a los servidores, el tipo de sistema operativo, proveedor y la versión del servicio que se encuentra instalado.
No se están empleando mecanismos seguros de conexión y transferencia de información mediante los servicios "Telnet" y "FTP".	Para evitar que la información de usuarios y contraseñas viajen en texto claro por la red al establecer sesiones "telnet" o "ftp", se recomienda la implantación de un protocolo seguro como "Secure Shell" ("ssh"), el cual permitirá realizar conexiones seguras y cifradas. En este sentido, aprovechando las bondades del "ssh" se preserva la confidencialidad de los usuarios a la hora de autenticarse mediante los servicios mencionados, ya que introduce un método más robusto de transferencia de archivos o datos. Para implantar esta recomendación, se deben seguir los siguientes pasos: – Adquirir e implantar los clientes y servidores de "ssh", destacando que de los clientes "ssh", existen diversas implementaciones, entre las cuales se encuentran las siguientes: • www.ssh.com • http://www.chiark.greenend.org.uk/ ~sgtatham/putty/* • http://www.networksimplicity.com/ openssh* • www.openssh.com* – En cuanto a los servidores de "ssh", podemos encontrar algunas de las implementaciones más populares en las siguientes direcciones: • www.ssh.com • www.openssh.com* * Productos gratuitos
La totalidad de los usuarios del ambiente Unix pueden utilizar el protocolo "FTP".	En función de evitar accesos no autorizados a los servidores por parte de personas no autorizadas, se recomienda limitar el acceso al comando "ftp" a sólo aquellos usuarios que sus funciones ameriten la actualización o extracción de archivos del servidor mencionado. Para limitar el acceso es necesario incluir en el archivo "/etc/ftpusers", a aquellos usuarios que no deben utilizar el servicio.
El servicio "SendMail" se	Deshabilitar el servicio "SendMail" editando el archivo

Tabla N° 22. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Unix)	
Vulnerabilidad	**Recomendación**
encuentra activo en los servidores evaluados.	"/etc/inetd.conf" y comentar la línea correspondiente al servicio "smtp" y posteriormente aplicar el comando "kill –HUP <pid del demonio inetd>" o bien deshabilitar el servicio con el comando "kill – 9 <pid del servicio de correo>", evitando de esta manera una posible interrupción de las operaciones en los servidores Unix.
Se detectaron servicios activos sin ser requeridos por los servidores acorde a sus funcionalidades.	Restringir los servicios que no son requeridos para la operatividad de los servidores Unix. Para implantar esta recomendación, se debe colocar el caracter "#" en el archivo "inetd.conf" al inicio de la línea donde se encuentran configurados los servicios ya mencionados, luego reiniciar el demonio "inetd" enviándole la señal "SIGHUP" con la orden "kill –HUP inetd.pid".
La cuenta del super usuario "root" en los dos servidores Unix evaluados, no están restringidos para conexiones remotas.	Asignar a cada administrador una cuenta de usuario sin privilegios administrativos y con posibilidad de ejecutar el comando "su", el cual permitirá autenticarse con el Super-usuario "root", permitiendo registrar en los logs la persona que está asiendo uso de esta cuenta. Adicionalmente, la contraseña de la cuenta "root" debe guardarse en un sitio seguro, con un procedimiento sencillo que describa la frecuencia de cambio (rotación de la contraseña) y las características de ésta. Adicionalmente, se recomienda definir los terminales seguros desde donde la cuenta "root" puede establecer conexión, mediante la definición y configuración del archivo "/etc/securettys".
No se encuentra limitado la ejecución del comando "su" en los servidores evaluados.	Con la finalidad de evitar que usuarios finales como los operadores, puedan hacer uso del comando "su" y tratar de deducir la contraseña del usuario "root", se recomienda restringir el uso de este comando para ser utilizado sólo por los administradores de dicho ambiente.

Tabla N° 23. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Oracle y SQL Server)	
Vulnerabilidad	**Recomendación**
La contraseña de la cuenta "sa" (System Administrator) del manejador de base de datos SQL Server en los servidores Web es trivial.	Cambiar la contraseña de la cuenta "sa" a una denominación no trivial, fácil de recordar por el propietario y difícil de deducir por el intruso. En este sentido, la misma debe estar enmarcada por letras mayusculas, minusculas, numeros y caracteres especiales, con una longitud mínima de ocho caracteres.
El manejador de bases de	Aplicar la actualización o "Patch" de seguridad liberado por el

Tabla N° 23. Recomendaciones para mitigar riesgos de acceso desde la red interna (Ambiente Oracle y SQL Server)	
Vulnerabilidad	**Recomendación**
datos "SQL Server" presenta vulnerabilidades que permiten accesos no autorizados.	proveedor "Microsoft", el cual se hace referencia en su boletín de seguridad MS02-039.
Las claves por defecto de los usuarios preestablecidos en el manejador de base de datos ORACLE no han sido cambiadas.	Cambiar las contraseñas definidas por defecto en las cuentas "System", "Sys", "Internal", "Scott", "DBSNMP", "Clark", "Ordsys" y "Mtssys", por denominaciones robustas que dificulten ser deducidas por intrusos y fáciles de recordar por los custodios.
Se detectaron cuentas de usuarios definidas en el grupo "DBA" sin ser requeridas.	Eliminar las cuentas de usuarios definidas en el grupo "ORADB" de los servidores UNIX. Asimismo, en caso de requerir algunas de las cuentas definidas en este grupo, se recomienda que las mismas cuenten con contraseñas de longitud mínima de doce (12) caracteres y se realice monitoreos constante sobre las cuentas definidas en dicho grupo.
Los permisos de acceso a nivel de sistema operativo sobre los directorios, archivos y utilitarios no han sido adecuadamente configurados.	Evaluar la posibilidad de restringir los permisos de acceso "World Writable" al grupo "others" sobre los recursos críticos, aplicaciones y utilitarios del manejador de base de datos Oracle. En este sentido, dicha actividad debe ser ejecutada en paralelo con la consulta y opiniones del proveedor sobre los cambios a realizar.

CAPITULO VI

IMPLANTACION DE LAS RECOMENDACIONES

1. Estrategias de implantación de las recomendaciones por períodos (Corto, Mediano y Largo plazo) y niveles de riesgo (Bajo, Medio y Alto)

A continuación, se presentan las estrategias de implantación de las recomendaciones emitidas para mitigar las vulnerabilidades detectadas, las cuales no representan un modelo rígido a seguir, sino una guía para facilitar el establecimiento de prioridades tomando en cuenta la complejidad y costo de implantación, así como el nivel de riesgo que representa cada brecha para los activos de información de la Compañía.

1.1. Estrategias de implantación de las recomendaciones para mitigar los riesgos de posibles accesos no autorizados a los activos de información desde Internet

Tabla N° 24. Implantación de las recomendaciones (Internet)

Vulnerabilidad	Período de Implantación de la Recomendación	Nivel de Riesgo hacia los Activos de Información o la operatividad
El Router de Internet posee un nombre trivial de comunidad SNMP.	Corto Plazo	
Se detectaron puertos del Router evaluado abiertos a Internet que pudieran comprometer su operatividad.	Corto Plazo	
El Router de Internet acepta conexiones externas vía “Telnet” desde cualquier dirección IP.	Corto Plazo	

Tabla N° 24. Implantación de las recomendaciones (Internet)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
El Firewall permite el flujo de paquetes "ICMP" ("Internet Control Message Protocol") desde Internet hacia los equipos ubicados en la "DMZ".	Corto Plazo	
El Firewall responde a conexiones externas por varios puertos abiertos desde Internet por donde se obtiene información confidencial.	Corto Plazo	
El servidor de correo electrónico y WEB muestra hacia Internet información confidencial para la Compañía.	Corto Plazo	
El servidor de correo no restringe los ataques de tipo "spam".	Corto Plazo	

Riesgo Bajo 	Riesgo Medio 	Riesgo Alto 

1.2. Estrategias de implantación de las recomendaciones para mitigar los riesgos de posibles accesos no autorizados a los activos de información desde la red interna o privada

Tabla N° 25. Implantación de las recomendaciones (Ambiente de Red)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
No se encuentran deshabilitados los puntos de red que no están siendo utilizados y no se han configurado los que se requieren con la	Mediano Plazo	

Tabla N° 25. Implantación de las recomendaciones (Ambiente de Red)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
dirección física de la estación de trabajo conectada.		
El Firewall no restringe el flujo de paquetes ICMP desde la red Interna hacia la Zona Desmilitarizada "DMZ" y viceversa.	Corto Plazo	
No existen mecanismos o sistemas de detección de intrusos en red (NIDS).	Mediano Plazo	
No se cuenta con mecanismos de seguridad para restringir el redireccionamiento de "Mac Address" en los equipos críticos de la Institución.	Corto Plazo	
Los Routers y Switches responden al nombre de comunidad "Public" del protocolo SNMP.	Corto Plazo	
Las contraseñas de acceso a los Routers y Switches de la Institución son de conocimiento público (Por defecto).	Corto Plazo	

Riesgo Bajo	Riesgo Medio	Riesgo Alto

Tabla N° 26. Implantación de las recomendaciones (Ambiente Wireless)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
La configuración de los componentes activos de la red inalámbrica ("Access Points") puede ser accedida en forma	Corto Plazo	

Tabla N° 26. Implantación de las recomendaciones (Ambiente Wireless)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
anónima desde la red fija o cableada.		
No existen mecanismos para controlar el flujo de información desde la red inalámbrica hacia la red fija o cableada.	Corto Plazo	
El "Access Point" no tiene configurado la opción de cifrado de información.	Corto Plazo	

Riesgo Bajo 	Riesgo Medio 	Riesgo Alto 

Tabla N° 27. Implantación de las recomendaciones (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
No han sido restringidas las consultas anónimas hacia las estaciones de trabajo.	Corto Plazo	
La contraseña de la cuenta de administración local es común en varias estaciones de trabajo, siendo ésta de fácil deducción.	Corto Plazo	
El orden de inicio de las estaciones de trabajo permite utilizar discos de arranque para omitir el proceso de carga del sistema operativo y la contraseña de configuración del "BIOS" no está definida.	Corto Plazo	
No ha sido removida la compartición administrativa en las estaciones de trabajo.	Corto Plazo	

Tabla N° 27. Implantación de las recomendaciones (Ambiente Windows 2000 – Estaciones de Trabajo)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
No se detectaron mecanismos para el control de aplicaciones instaladas de manera no autorizada en las estaciones de trabajo.	Mediano Plazo	
El protocolo "Netbios" se encuentra activo en las estaciones de trabajo.	Corto Plazo	
Las estaciones de trabajo responden al nombre "Public" de la comunidad del protocolo SNMP.	Corto Plazo	
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en las estaciones de trabajo.	Corto Plazo	
No ha sido desactivado el cifrado "LanMan" en las estaciones de trabajo.	Corto Plazo	

Riesgo Bajo 	Riesgo Medio 	Riesgo Alto 

Tabla N° 28. Implantación de las recomendaciones (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
La solicitud de consulta de usuarios anónimos mediante el uso del servicio "Lan Manager" en los servidores no ha sido restringida.	Corto Plazo	
Las políticas de contraseñas de usuarios definidas en el servidor de "Active Directory" no cumplen las mejores prácticas de seguridad.	Corto Plazo	

Tabla N° 28. Implantación de las recomendaciones (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
Las bondades de auditoría no se encuentran configuradas en el servidor de "Active Directory" acorde a las mejores prácticas y se encuentra inactiva en los servidores de correo, Web y Proxy.	Corto Plazo	
Se detectaron usuarios con contraseñas de fácil deducción en los servidores evaluados.	Corto plazo	
El acceso remoto al registro del sistema ("registry") no se encuentra restringido en los servidores evaluados.	Corto Plazo	
Existen deficiencias en la administración de los controles de acceso asignados a las cuentas de usuarios definidas en el servidor de "Active Directory".	Corto Plazo	
El protocolo "Netbios" se encuentra activo en los servidores Windows 2000 evaluados.	Corto Plazo	
Los servidores evaluados responden al nombre "Public" de la comunidad del protocolo SNMP.	Corto Plazo	
Los recursos compartidos administrativamente al instalar el sistema operativo no han sido removidos.	Corto Plazo	
No ha sido desactivado el cifrado "LANMAN" de contraseñas en los servidores evaluados.	Corto Plazo	
Existen servicios activos que no son requeridos por los servidores evaluados.	Corto Plazo	
No han sido renombradas las cuentas "Administrator" y "Guest" en los servidores	Corto Plazo	

Tabla N° 28. Implantación de las recomendaciones (Ambiente Windows 2000 – Servidores)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
evaluados.		
No han sido habilitados los esquemas de seguridad para puertos en los servidores Windows 2000.	Mediano Plazo	
Existen vulnerabilidades del servicio IIS que permiten la ejecución de código en los servidores Web.	Corto Plazo	

Riesgo Bajo	Riesgo Medio	Riesgo Alto

Tabla N° 29. Implantación de las recomendaciones (Ambiente Unix)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
Las contraseñas de las cuentas definidas en el servidor Unix del ambiente de desarrollo son de fácil deducción.	Corto Plazo	
Existen relaciones de confianza entre los servidores Unix evaluados.	Corto Plazo	
El Banner de los protocolos “FTP”, “Telnet” y “SMTP” presentan información para identificar características de los servidores evaluados.	Corto Plazo	
No se están empleando mecanismos seguros de conexión y transferencia de información mediante los servicios “Telnet” y “FTP”.	Corto Plazo	
La totalidad de los usuarios del ambiente Unix pueden utilizar el protocolo “FTP”.	Corto Plazo	

Tabla N° 29. Implantación de las recomendaciones (Ambiente Unix)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
El servicio "SendMail" se encuentra activo en los servidores evaluados.	Corto Plazo	
Se detectaron servicios activos sin ser requeridos por los servidores acorde a sus funcionalidades.	Corto Plazo	
La cuenta del super usuario "root" en los dos servidores Unix evaluados, no están restringidos para conexiones remotas.	Corto Plazo	
No se encuentra limitado la ejecución del comando "su" en los servidores evaluados.	Corto Plazo	

Riesgo Bajo 	Riesgo Medio 	Riesgo Alto 

Tabla N° 30. Implantación de las recomendaciones (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
La contraseña de la cuenta "sa" (System Administrator) del manejador de base de datos SQL Server en los servidores Web es trivial.	Corto Plazo	
El manejador de bases de datos "SQL Server" presenta vulnerabilidades que permiten accesos no autorizados.	Corto Plazo	
Las claves por defecto de los usuarios preestablecidos en el manejador de base de	Corto Plazo	

Tabla N° 30. Implantación de las recomendaciones (Ambiente Oracle y SQL Server)		
Vulnerabilidad	**Período de Implantación de la Recomendación**	**Nivel de Riesgo hacia los Activos de Información o la operatividad**
datos ORACLE no han sido cambiadas.		
Se detectaron cuentas de usuarios definidas en el grupo "DBA" sin ser requeridas.	Corto Plazo	
Los permisos de acceso a nivel de sistema operativo sobre los directorios, archivos y utilitarios no han sido adecuadamente configurados.	Mediano Plazo	

Riesgo Bajo	Riesgo Medio	Riesgo Alto

CONCLUSIONES

Basado en los resultados de la evaluación de seguridad mediante la ejecución de un estudio de penetración interno y externo a la Institución "XXX" y estando en conocimiento de las vulnerabilidades y riesgos que posee su plataforma tecnológica, ha tomado conciencia en relación a la necesidad de implantar controles de seguridad que mitiguen los riesgos de acceso no autorizado e interrupción de su continuidad operativa producto de posibles intrusos que busquen de obtener acceso a sus activos de información, afectar su imagen e incursionar en problemas de índole legal.

En este sentido, la Institución Financiera "XXX" se ha enmarcado bajo una actitud proactiva, donde no se conforma con la seguridad ofrecida por su situación actual, sino que trabajará en función a predecir y prepararse para disminuir los riesgos, siendo su objetivo principal el logro de un ambiente más seguro y adelantarse en ingenio al agresor tanto como sea posible.

Por lo dicho anteriormente, hoy en día son muchas las compañías en Venezuela que presentan vulnerabilidades de seguridad en su plataforma tecnológica que las expone a posibles accesos no autorizados o ataques especializados en interrumpir su continuidad operativa tanto desde Internet como internamente por su personal. Es importante destacar, que esta situación se debe en mayor parte al grado de desinformación y carencia de conciencia y cultura de riesgos y seguridad para proteger sus activos de información.

Por último, cada día son mayores las empresas que apoyan sus procesos de negocio en la tecnología y no conforme con ello, ofrecen servicios vía Internet con el fin de ser más competitivos y adaptarse a las demandas de los mercados globales. Es por ello, la necesidad de evaluar continuamente sus controles de seguridad y la adopción de estrategias para crear conciencia de seguridad a todos los niveles.

RECOMENDACIONES

En función de mitigar los riesgos asociados a las vulnerabilidades detectadas con la evaluación de seguridad de la Institución Financiera "XXX" mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica, se recomienda emprender acciones para implantar los controles de seguridad descritos en el Capítulo V (Situación Propuesta), tomando en consideración las estrategias definidas en el Capítulo VI (Implantación de las recomendaciones).

Por otra parte, se recomienda definir una Función de Seguridad de Activos de Información (FSAI), donde su misión sea 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.

Por último, con la finalidad de mantener adecuados controles de seguridad en el tiempo, se recomienda evaluar los mismos en frecuencia trimestral, tomando en cuenta las nuevas brechas de seguridad que se generan por los continuos cambios y administración de la plataforma tecnológica, rotación de personal, surgimiento de nuevas amenazas como virus y publicación en la Internet de herramientas y vías de acceso no autorizado por parte de Hackers.

GLOSARIO DE TERMINOS

A

Address (dirección): En la Internet dícese de la serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: "dirección de correo electrónico" (*email address*); "IP" (dirección internet); y "dirección hardware" o "dirección MAC" (*hardware or MAC address)*.

Alias (apodo): Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de recordar.

Anonymous FTP (FTP anónimo): El FTP anónimo permite a un usuario de Internet la captura de documentos, archivos, programas y otros datos contenidos en archivos existentes en numerosos servidores de información sin tener que proporcionar su nombre de usuario y una contraseña (*password*). Utilizando el nombre especial de usuario *anonymous*, o a veces *ftp*, el usuario de la red podrá superar los controles locales de seguridad y podrá acceder a archivos accesibles al público situados en un sistema remoto.

Apache (Apache): Servidor HTTP de dominio público basado en el sistema operativo Linux. Apache fue desarrollado en 1995 y es actualmente uno de los servidores http más utilizados en la red.

API (Interfaz de programación de aplicaciones): Conjunto de rutinas que permiten a un programador usara funciones de una computadora. La interfaz de programación de conectores y la interfaz de la capa de transporte son API para la programación en TCP/IP.

Applet: Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

Application: Un programa que lleva a cabo una función directamente para un usuario. WWW, FTP, correo electrónico y Telnet son ejemplos de aplicaciones en el ámbito de Internet.

Appz: En la Internet existen miles de páginas bajo este nombre. En ellas se albergan programas completos, evidentemente crackeados. Para acceder a un Appz, dichas paginas te exigen visualizar otras paginas de contenido sexual. Los Appz son a todas luces, programas ilegales que a menudo contienen Virus embebidos.

Armouring: Se trata de una técnica utilizada por algunos virus informáticos, mediante la cual se impide su examen por medio de otros programas, como por ejemplo un antivirus.

ARP (Address Resolution Protocol): Protocolo de Resolución de Direcciones a nivel de la capa de enlace, utilizado para encontrar dinámicamente la dirección física de un sistema mediante su dirección de IP.

Authentication: Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

AVR: Los Hackers conocen por estas siglas, las tarjetas electrónicas que permiten emular el funcionamiento de una tarjeta inteligente. En USA esta tarjeta ha sido empleada para abrir los canales de DishNet y Expresvu. En España se están empleando para abrir Vía Digital. Se denominan AVR también, porque el microcontrolador que poseen estas tarjetas es una AVR de Atmel.

B

Backbone (columna vertebral, eje central, eje troncal): Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (*stub*) y de tránsito (*transit*) conectadas al mismo eje central están interconectadas.

BackDoor: Se conoce como puerta trasera que puede estar presente en cualquier tipo de Software, ya sea un sistema operativo o el software de un microcontrolador. Los Hackers por ejemplo, hacen uso de los Backdoors para leer y escribir en tarjetas inteligentes cuando se habla de televisiones de pago.

Banner (anuncio, pancarta): Imagen, gráfico o texto de carácter publicitario, normalmente de pequeño tamaño, que aparece en una página web y que habitualmente enlaza con el sitio web del anunciante.

Baud (baudio): Cuando se transmiten datos, un baudio es el numero de veces que cambia el "estado" del medio de transmisión en un segundo. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo, medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

Bit (bit, bitio): Unidad mínima de información digital que puede ser tratada por un computador. Proviene de la contracción de la expresión *binary digit* (dígito binario).

Bomba lógica: La bomba lógica es conocida también como bomba de activación programada. La bomba lógica es un tipo de Caballo de Troya que se deja olvidado en el interior de un sistema informático como un archivo más del sistema. Después de pasado un tiempo, cuando se cumplen las condiciones de activación, la bomba lógica despierta de su largo letargo. Se sabe que las bombas lógicas fueron bautizadas así,

dado que fueron desarrolladas por trabajadores informáticos que en su día fueron despedidos, pero que esperaba vengarse tarde o temprano de sus jefes. Después de pasado un tiempo la bomba lógica se activaba y dejaba sin sospecha al trabajador despedido como presunto autor del programa.

Bounce (rebote): Devolución de un mensaje de correo electrónico debido a error en la entrega al destinatario.

Browser (hojeador, navegador, visor, visualizador): Aplicación para visualizar documentos WWW y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet; cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

Bucaneros: Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "Crackeados " pasan a denominarse " piratas informáticos " así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

Bug (error, insecto, gazapo): Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por Grace Murria Hooper, una de las pioneras de la programación moderna, al descubrir como un insecto (*bug*) había dañado un circuito del computador Mark.

Bug 34/32: Los Hackers llaman así, a un fallo que las tarjetas de SecaMediaguard poseen. Esto les permite Crackear dicha tarjeta.

Business Software Alliance -- BSA (Alianza del Sector del Software): Organismo creado en 1988 por diversas empresas del sector del software para defender sus derechos de propiedad intelectual sobre los programas que desarrollan.

Byte (byte, octeto): Conjunto significativo de ocho bits que representan un carácter.

Bloquer: Se trata de un artilugio que permite "bloquear" como su nombre indica, distintos comandos EMM de un canal de pago. Así, los Hackers pueden proteger una tarjeta de acceso inteligente, frente a los cambios del contenido de dicha tarjeta por parte de la plataforma digital.

C

Caballo de Troya: También denominados Troyanos, se trata de programas de comportamiento similar a los virus en algunos casos, dado que los caballos de Troya están diseñados para "robar" datos importantes de una maquina remota. El caballo de Troya se oculta en nuestro sistema como una aplicación de función requerida. Por ejemplo si se desea capturar una contraseña, el caballo de Troya se comportara como la aplicación Conexión telefónica a redes, para " robarnos " la contraseña, ya que al introducir esta, se realiza una copia que será enviada mas tarde por correo electrónico al autor.

Cellular phone (teléfono celular, móvil, telefónico, teléfono móvil): Teléfono portátil sin hilos conectado a una red celular y que permite al usuario su empleo en cualquier lugar cubierto por la red. Una red celular, y los teléfonos a ellos conectados, puede ser digital o analógica. Si la red es digital el teléfono puede enviar y recibir información a través de Internet.

Chat (conversación, charla, chateo, tertulia) Comunicación simultánea entre dos o más personas a través de Internet. Hasta hace poco tiempo sólo era posible la "conversación" escrita pero los avances tecnológicos permiten ya la conversación audio y vídeo.

Clipper chip: Dispositivo de cifrado que el Gobierno de los EE.UU. intentó hacer obligatorio mediante ley en 1995 para poder controlar el flujo de transmisiones criptografiadas a través de redes digitales de telecomunicación.

Copyhackers: Es una nueva raza solo conocida en el terreno del crackeo de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año más de 25.000 millones de pesetas solo en Europa. En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los "bucaneros". Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

Cookie (cuqui, espía, delator, fisgón, galletita, pastelito, rajón, soplón): Conjunto de caracteres que se almacenan en el disco duro o en la memoria temporal del computador de un usuario cuando accede a las páginas de determinados sitios web. Se utilizan para que el servidor accedido pueda conocer las preferencias del usuario. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los cookie.

Crackers: Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers. En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante. Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica. Mas adelante hablaremos de los Cracks más famosos y difundidos en la red.

Cryptography (Criptografía): Término formado a partir del griego *kruptos*, "oculto" ... significa, según el diccionario académico, "Arte de escribir con clave secreta o de un modo enigmático" ... Es criptográfico cualquier procedimiento que permita a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, tras haberlo descifrado.

Cryptology (Criptología): Es la parte de la Criptografía que tiene por objeto el descifrado de criptogramas cuando se ignora la clave.

Cyber- (ciber-): Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio,

cibernauta, etc.). Su origen es la palabra griega "cibernao", que significa "pilotar una nave".

Cybercop (ciberpolicía): Funcionario policial especializado en la Internet o en utilizar la red para sus investigaciones.

Cyberculture (Cibercultura): Conjunto de valores, conocimientos, creencias y experiencias generadas por la comunidad internáutica a lo largo de la historia de la red. Al principio era una cultura elitista; más tarde, con la popularización de Internet, la cibercultura es cada vez más parecida a la "cultura" a secas, aunque conserva algunas de sus peculiaridades originales.

Cybernaut (cibernauta): Persona que navega por la red.

Cyberspace (Ciberespacio): Término creado por William Gibson en su novela fantástica "Neuromancer" para describir el "mundo" de los computadores y la sociedad creada en torno a ellos.

Cybertrash (ciberbasura): Todo tipo de información almacenada o difundida por la red que es manifiestamente molesta o peligrosa para la salud mental de los internautas. Dícese también de quienes arrojan basura la red.

Cyberzapping (ciberzapeo): Acción de pasar de forma rápida y compulsiva de una página a otra dentro de un sitio web o de un sitio web a otro.

D

Dark Avenger: Seudónimo de uno de los creadores de virus más famoso de todos los tiempos.

Daemon (Daemon): Aplicación UNIX que está alerta permanentemente en un servidor Intenet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página web. "Daemon" es una palabra latina que significa "espíritu" (bueno o malo) o "demonio".

Data Encryption Standard -- DES (Estándar de Cifrado de Datos): Algoritmo de cifrado de datos estandarizado por la administración de EE.UU.

Datagrama IP: Es la unidad de datos enrutada por el protocolo IP.

De-encryption (descifrado, deencriptación): Recuperación del contenido real de una información cifrada previamente.

Defense Advanced Research Projects Agency -- DARPA (Agencia de Proyectos de Investigación Avanzada para la Defensa): Organismo dependiente del Departamento de Defensa norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET.

Dialup (conexión por línea conmutada): Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre computadores por línea telefónica normal. Dícese también del hecho de marcar un número de teléfono.

Digital signature (firma digital): Información cifrada que identifica al autor de un documento electrónico y autentifica que es quien dice ser.

Dirección de IP: Número de 32 *bits* que identifica una interfaz de red.

Download (bajar, descargar): En la Internet proceso de transferir información desde un servidor de información al propio computador.

Dropper Un Dropper es un programa que no es un virus, pero que posee la capacidad de crear virus informáticos cuando se ejecuta. El Dropper así, consigue burlar los antivirus, puesto que su código no contiene nada malicioso en un principio.

E

Echelon: Sistema de satélites norteamericanos que permiten " espiar " al usuario de a pie. El sistema Echelon permite interceptar comunicaciones de teléfono, radio o de Internet. Los satélites de Echelon no son los únicos elementos de este sistema de espionaje, además de ellos, podemos encontrarnos con sistemas "caputadores" de señales de radio, escaners y sistemas informáticos.

Encryption (cifrado, encriptación): El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Enfopol: Se trata de la versión Europea de Echelon.

Enrutadores o Rourters: Dispositivos inteligentes que interconectan redes. Estos poseen algoritmos para poder elegir la ruta a seguir para conectar diferentes segmentos de red.

F

FTP (File Transfer Protocol): Protocolo de Transferencia de Archivos.

Finger (apuntar con el dedo, dedo): Programa que muestra información acerca de un usuario(s) especifico(s) conectado(s) a un sistema local o remoto. Habitualmente se muestra el nombre y apellidos, hora de la ultima conexión, tiempo de conexión sin

actividad, línea del terminal y situación de éste. Puede también mostrar archivos de planificación y de proyecto del usuario.

Firewall (cortafuegos): Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Free Software (Software Libre): Programas desarrollados y distribuidos según la filosofía de dar al usuario la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar dichos programa (Linux es un ejemplo de esta filosofía). El software libre no es siempre software gratuito (equivocación bastante habitual que tiene su origen en que la palabra inglesa *free* significa ambas cosas).

Freeware (programas de libre distribución, programas gratuitos, programas de dominio público): Programas informáticos que se distribuyen a través de la red de forma gratuita.

Funcard: Se trata de una variante de tarjeta electrónica basada en un microcontrolador de Atmel. Esta tarjeta electrónica esta siendo utilizada para emular sistemas de televisión de pago como SecaMediaguard o Nagra.

G

Gateway (pasarela): Hoy se utiliza el término *router* (direccionador, encaminador, enrutador) en lugar de la definición original de *gateway*. Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes. No debería confundirse con un convertidor de protocolos.

Guru (gurú): Persona a la que se considera, no siempre con razón, como el sumo manantial de sabiduría sobre un determinado tema. Nicholas Negroponte es considerado el máximo gurú en lo que se refiere a Internet y la llamada Sociedad de la Información.

H

Hackers: El primer eslabón de una sociedad " delictiva " según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en computadores remotos, con el fin de decir aquello de " he estado aquí " pero no modifican ni se llevan nada del computador atacado. Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad. El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. emplea muchas horas delante del computador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso. Este grupo es el mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Heurística: Se trata de una técnica mediante la cual se examina el código de un archivo ejecutable en busca de funciones o acciones que son generalmente asociadas

con la actividad vírica. Este método, utilizado por los Antivirus, a veces hacen saltar la alarma en archivos que no están realmente afectados.

Hoax (bulo, camelo): Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

Host: termino en inglés que define a un computador principal.

I

IDS (Intrusion detection system): dispositivo de seguridad que inspecciona todas las actividades de entrada y salida en una red e identifica patrones sospechosos que indicar{ian que una red o sistema es atacado por alguien que intenta romper o comprometer un sistema.

IETF (Internet Engineering Task Force): Conjunto de grupos de trabajo creados por voluntarios para desarrolla en implementar protocolos de Internet.

IP (Internet Protocol): Protocolo de Internet, éste trabaja a nivel de la capa de red según el modelo OSI responsable del transporte de datagramas por Internet.

IP address (dirección IP): Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345

Irdeto: Sistema de encriptación de señales digitales, de algunas plataformas de televisión alemanas. Actualmente los Hackers han dado con el algoritmo de este sistema, consiguiendo así, emular dicho sistema.

ISO: Organización Internacional para la Estandarización fundada para promover el

comercio internacional y el progreso en la cooperación en ciencia y tecnología.

ISP (Internet Service Provider): Proveedor de Servicios de Internet.

J

Joke: Se trata de una aplicación que al principio uno cree que esta ante la infección de un malicioso virus, pero en realidad se trata de una broma pesada con final feliz.

K

Key (clave): Código de signos convenidos para la transmisión de mensajes secretos o privados. En los sistemas de televisión de pago, las Keys, son las encargadas de desencriptar las señales de televisión.

Keyword (clave de búsqueda, palabra clave) Conjunto de caracteres que puede utilizarse para buscar una información en un buscador o en un sitio web.

KeyGenerator Se denominan así, a los programas creados por Crackers, los cuales son capaces de generar las claves de registro de un programa Shareware. Estos generadores de registro, normalmente muestran el número de serie a introducir en la aplicación que se quiere registrar. Cad KeyGenerator responde a un algoritmo especifico.

Kbps: unidad de medida de velocidad de transmisión o ancho de banda, kilobyte por segundos.

L

Lamers: Este grupo es quizás el que más número de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son

individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en la Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro computador, le fascinan enormemente. Este es quizás el grupo que más peligro acontece en la red ya que ponen en práctica todo el Software de Hackeo que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se mofa autodenominandose Hacker. También emplean de forma habitual programas sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el computador esta apagado. Toda una negligencia en un terreno tan delicado.

LAN (Local Area Network): Red de Área Local de datos que se utiliza para dar servicio a un área de pocos kilómetros cuadrados y consiste en una red única privada. Se usan para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información.

Línea Discada: conocida como Dial-up, estas líneas sirven para conectar los aparatos de teléfonos que comúnmente se usan para las llamadas telefónicas, estas líneas pueden transmitir datos mediante la conexión de modems.

M

MAC (Media Access Control): Control de Acceso al Medio, protocolo que controla el acceso de una estación a una red.

Mail bombing (bombardeo postal): Envío indiscriminado y masivo de mensajes de correo electrónico. En la actualidad existe en la Internet buena cantidad de aplicaciones que con solo pulsar un botón, permite hacer Mailbombing.

Malware: Los Malware son todo tipo de software que implica una función maliciosa, como lo son los virus informáticos, los Caballos de Troya o las bombas lógicas, por citar algunos.

Máscara de direcciones: Número binario de 32 *bits* para identificar las partes de una dirección de IP para la numeración de redes y subredes. Todos los *bits* de los campos de red o subred se fijan a 1.

Mbps: unidad de medida de velocidad de transmisión o ancho de banda, megabyte por segundos.

MBR: Es el sector de arranque propio de un disco duro, dentro de la cual se define la estructura del resto de la información contenida en el mismo. En este sentido, cada disco duro independientemente del numero de particiones que posea, si contiene un MBR único, aunque cada unidad "cítese C: D: E:" tiene su propio sector lógico de arranque.

MOSC: Los Hackers denominan así, al arte de modificar una tarjeta de acceso inteligente. El MOSC permite a los Hackers, recuperar el funcionamiento de una tarjeta de televisión de pago, que ha sido dada de baja. El MOSC también permite modificar los paquetes contratados en las plataformas digitales. Actualmente los Hackers son capaces de hacer MOSC en tarjetas del sistema Irdeto, Nagra y SecaMediaguard

Modchip: El Modchip es un microcontrolador que instalado en una consola Playstation, permite leer sin problemas juegos piratas. Estos juegos se denominan piratas porque son copias alteradas de un juego original. El Modchip identifica el disco pirata y entrega a su salida el código de un disco original. Este código se denomina Boot de arranque del disco.

N

Nagravision: Sistema de encriptación empleado por la plataforma digital Via Digital. Su creador, Kudelski, es también el creador del sistema Nagra empleado por C+ terrestre. Ambos sistemas están Hackeados en la actualidad. Los Hackers han dado, recientemente, con el algoritmo de dichos sistemas, que en ambos casos es totalmente diferente. Nagra analógico emplea un método DES 3 y Nagra Digital un método RSA.

NAT (Short for Network Address Translation): estándar de la Internet que permite a una LAN trasladar un rango de direcciones IP internas a un segundo rango de direcciones para el tráfico externo..

Newbie: Es un novato o más particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, si no que aprende.

NCSA: Son las siglas de unos de los organismos mas conocidos e importantes en el campo de la lucha antivirus. Estas siglas responden a la frase de National Computer

Security Association. La NCSA esta especializada en virus, evolución de los mismos y estudio para combatir a estos gérmenes de la era de la informática.

Ñ y O

OSI (Open Systems Interconection): Interconexión de Sistemas Abiertos, conjunto de estándares de ISO relativos a la comunicación de datos.

OSPF (Open Shortest Patch First): Algoritmo Abierto de Primero la Trayectoria más Corta. Protocolo de enrutamiento de Internet con buena capacidad de escalado, que enruta el tráfico por varios caminos y usa su conocimiento sobre la topología de Internet para realizar precisas decisiones de enrutamiento

P

Pasarela (Gateway): Es un sistema de comunicaciones entre dos redes heterogéneas, que permite la transmisión de datos en ambas direcciones entre los dispositivos situados en los extremos del enlace.

Pacht: Es una aplicación bajo DOS o Windows que permite añadir un trozo de código a una aplicación Shareware. El código que se añade, permite registrar dicha aplicación saltándose las protecciones del Software.

Payload o Payload Activation date: Los Payloads se conocen como funciones de activación de la carga explosiva. Los Payloads provienen o se emplean mucho en el campo militar, de hay la palabra de activar la carga explosiva. La función Payload aplicada a un virus informatico, implica que este se activara independientemente de la fecha en la que se infecto el PC. De esta forma se reconoce que una computadora puede infectarse un día distinto al de la reproducción de virus. Dicha activación puede ir en función de la fecha o por un determinado numero de ordenes o acciones

del PC. Una vez alcanzado dichos parámetros de activación, el virus hace efecto en el PC.

Phreaker: Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Poliformismo: Se trata de la capacidad que poseen algunos tipos de virus que permiten mediante esta técnica, modificar la forma del propio virus cada vez que se reproduce. Con esta técnica se logra crear miles de versiones diferentes del mismo virus en tan solo unas horas. Esto implica, que el antivirus apenas puede detectarlo con seguridad. Para ello un virus polimórfico, cuenta con una pequeña cabecera que se modifica en cada infección. El resto del código no se altera, sino que simplemente se encripta por motivos de "ocultación". El algoritmo de encriptación varia de una infección a otra, mientras que la cabecera siempre actúa de activador del propio virus.

PPP (Point to Point Protocol): Protocolo Punto – Punto para la transferencia de datos por enlaces seriales. Permite multiplexar por el enlace tráfico de varios protocolos.

Pretty Good Privacy -- PGP (Privacidad Bastante Buena, Privacidad de las Buenas): Conocido programa de libre distribución, escrito por Phil Zimmermann, que impide, mediante técnicas de criptografía, que archivos y mensajes de correo electrónico puedan ser leídos por otros. Puede también utilizarse para firmar

electrónicamente un documento o un mensaje, realizando así la autentificación del autor.

Protocolos de Comunicación: está definido como un juego o conjunto de reglas y procedimientos que proporcionan una técnica uniforme para gobernar una línea de comunicaciones. Estas reglas y procedimientos proveen la administración, asignación y control, de los recursos involucrados, así como establecen métodos para enviar y/o solucionar problemas acontecidos por situaciones de excepción, ocurridas en cualquiera de los elementos intervinientes.

O yR

RAS (Remote Access Services): facilidad construidad dentro del Windows NT para habilitar a usuarios la entrada a la LAN usando modem, conexión X.25 o un enlace WAN. El RAS trabaja con la mayoría de los protocolos de red, incluyendo TCP/IP, IPX y Netbeui.

RFC (Resquest For Comments): Solicitud de Comentarios.

RIP (Routing Information Protocolo): protocolo de enrutamiento de información, el cual utiliza el algoritmo de vector de ruta que reporta el camino más corto entre dos puntos de una red.

S

Serials: Los Serials están disponibles en paginas Underground en la Internet. Estas páginas contienen miles de Serials que no son otra cosa que números de registros de aplicaciones informáticas.

Shareware (programas compartidos): Dícese de los programas informáticos que se distribuyen a prueba, con el compromiso de pagar al autor su precio, normalmente bajo, una vez probado el programa y/o pasado cierto tiempo de uso.

Skid Kiddies (Scripts kiddies): Personas que normalmente se pasan todo el día navegando por la ReD con la sola intención de bajarse de ella todo tipo de aplicaciones. Después, sin detenerse a leer los manuales o archivos Leeme, ejecutan todas las aplicaciones, mientras están conectados a Internet. Esta acción, a menudo conlleva a colapsar la ReD, ya que es posible que ejecute un programa muy dañino. Un ejemplo de lo que se pretende explicar es el reciente ataque de Negación Dos.

Sniffers: Llaman así, a las aplicaciones capaces de vigilar una conexión o sistema electrónico. También pueden recibir el nombre de caza-puertos o escaneador de puertos.

SNMP (Simple Network Management Protocolo): protocolo simple para el manejo de red, el cual define un conjunto de reglas y protocolos para el intercambio de información en red, este provee formatos comunes para dispositivos y equipos de red como: puentes, concentradores, enrutadores, etc. Cada programa manejador puede controlar el manejo de elementos a través de agentes localizados en diferentes puntos de la red.

Spam (bombardeo publicitario, buzonfia): Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir "loncha de mortadela".

SSH: desarrollado por SSH Communications Security Ltd., Secure Shell es un programa para permitir la entrada a otro computador sobre una red de datos, para ejecutar comandos en una máquina remota, y mover los archivos de una computadora a la otra. Este provee una robusta autenticación y comunicación segura sobre canales

con poca seguridad reemplazan los conocidos comandos: rlogin, rsh, rcp y rdist de UNIX. SSH protege a la red de ataques como IP spoofing, IP source routing y DNS spoofing ya que su sesión es protegida mediante la encriptación de la misma. SSH está disponible para Windows, Unix, Macintosh y OS2.

SSL (Secure Sockets Layer): desarrollado por Netsacape para la transmisión de documentos privados vía Internet. SSL trabaja a través del uso de clave pública para encriptar la data que es transferida sobre una conexión SSL. Tanto como el navegador de Netscape como el Explorer soportan SSL y muchos sitios WEB usan el protocolo para obtener información confidencial, como saldos de cuentas y tarjetas de créditos. Por convención los URL que requieren una conexión SSL comienzan con *https* en vez de http.

Stealth: Es la técnica que permite a algunos tipos de virus permanecer ocultos en un sistema operativo y en consecuencia a cualquier aplicación Antivirus.

T

TCP *(*Transmission Control Protocol*)*: protocolo del Control de la Transmisión de la capa 4 de la suite TCP/IP, que ofrece una transmisión fiable de datos orientada a conexión, entre un para de aplicaciones.

TELNET (Terminal Emulation): es un programa de emulación de terminal para redes TCP/IP. Este corre sobre computadores personales para conectarlos a servidores y se pueden introducir comandos tan igual como si se estuvieran realizando desde la consola misma del servidor.

Tempest: Los Hacerks son capaces de obtener información de un PC, aun si este no esta conectado a la ReD. La técnica denominada Tempest permite recuperar la señal RF irradiada por un monitor, para así, tener delante de sí, una copia de lo que tiene en

el monitor el espiado. Los métodos Tempest son muy sofisticados y caros, por lo que su uso esta limitado a espionajes industriales y militares.

Terminate and Stay Resident (TSR): Un TSR es un programa capaz de ejecutarse e instalar en memoria una extensión residente del mismo, la cual permanecerá activa durante todo el tiempo que el PC este activo. Después de esto, el programa finaliza su función. Los TSR no tienen porque ser especialmente dañinos, ya que por citar un ejemplo, cada vez que enciende su computador, este carga varios tipos de TSR, como por ejemplo el dríver del ratón.

TFTP (Trivial Filie transfer): es una simple forma de realizar FTP, este el protocolo usa el UDP para transporte de paquetes y a menudo es usados por los servidores para arrancar estaciones de trabajos que no usan discos duros (X-terminals y routers).

Trigger Como su nombre indica, es un disparador, el cual permite a un programador de virus informáticos, controlar la fecha de activación del mismo.

Trojan Horse (Caballo de Troya) Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

Tunneling: El Tunneling es la técnica con la cual es posible que un virus informático pueda pasar desapercibido frente a los módulos de detección, mediante punteros directos a los vectores de interrupción. Este efecto, es también empleado por los propios Antivirus actuales.

U

Underground: Se conoce como Underground todo lo que esconde métodos de Hacking, Cracking o Phreaking en general. En realidad el término Underground es

empleado por los escritores para referirse a este nuevo mundo que puebla las nuevas tecnologías, y sobre todo la comunidad Internet.

UDP (User Datagram Protocol): Protocolo de Datagramas de Usuario utilizado a nivel de la capa de transporte del modelo TCP/IP.

UTP (Unshielded Twisted Pair): es un tipo popular de cables que consiste de dos alambres trenzados sin protección. Debido a su bajo costo, UTP es usado extensivamente para LAN y conexiones telefónicas. Este no ofrece un buen ancho de banda como lo ofrece una fibra óptica, pero es mucho mas económico y fácil de trabajar.

V

Virus (virus): Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

VPN (Virtual Private Network): Red Privada Virtual.

W

WAN (Wide Area Network): Red de Área Amplia que cubre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas (*hosts*) dedicada a ejecutar programas de usuario (aplicaciones).

WardCard: Se trata de una guerra abierta en la que intervienen únicamente tarjetas electrónicas que emulan a otras tarjetas inteligentes. En la actualidad el WardCard se basa en los ataques continuos mediante ECM, que envían las plataformas digitales como CSD o Vía, hacia las tarjetas no oficiales. Estos ataques modifican o invalidad

dichas tarjetas también denominadas piratas. Después los Hackers las reactivan de nuevo. Esto es en definitiva la WardCard.

Warez: Los Warez son programas completos que se ofrecen a través de CD. Existen multitud de páginas que contienen Warez. Los Warez incumplen los derechos de autor.

Wetware (materia húmeda) En la jerga de los piratas informáticos significa "cerebro".

Wildlist: Bajo este nombre se esconde una lista de todos los virus conocidos. Dicha lista permite comprobar el tipo de amenazas que sufren los usuarios de computadoras.

Worm (gusano): Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en "ACM Communications" (Marzo 1982). El gusano de Internet de Noviembre de 1988 es quizás el más famoso y se propagó por si solo a más de 6.000 sistemas a lo largo de Internet.

REFERENCIAS BIBLIOGRAFICAS

- Boletines mensuales emitidos por Espiñeira, Sheldon y Asociados – Firma miembro de PricewaterhouseCoopers.

- SCAMBRAY, Joel. **Hackers 2 - Secretos y soluciones para la seguridad en redes.** Osborne McGraw-Hill. España 2001. Segunda edición.

- PricewaterhouseCoopers. **Microsoft Windows NT – Seguridad, auditoría y control.** Osborne McGraw-Hill. España. 1999.

- SCAMBRAY, Joel. **Hackers en Windows 2000 - Secretos y soluciones para la seguridad en Windows.** Osborne McGraw-Hill. España 2002.

- SHAH, Steve. **Manual de administraciòn de Linux.** Osborne McGraw-Hill. España 2001.

- BOBROWSKI, Steve. **Oracle 8i para Windows NT.** Osborne McGraw-Hill. España 2000.

- MENDILLO, Vincenzo. **Seguridad de Redes y Criptografía**. CD-ROM. Universidad Central de Venezuela, Caracas 2001.

- MENDILLO, Vincenzo. **Gestion de Redes**. CD-ROM. Universidad Central de Venezuela. Caracas 2002.

- Manual de **Soporte a protocolo TCP/IP.** Corporación LANSOFT, C.A. Caracas 2001.

- Manual de preparación al examen **CISA "Certified Information Systems Auditor".** ISACA. United States of America 2002.

- MCCLURE, Stuart. **Hacking Exposed – Network Security Secrets & Solutions.** Osborne McGraw-Hill.Berkeley, California 2001

- Anonymous. **Maximum Security – Second Edition.** SAMS. United States of America 1998.

- Microsoft eBook. **MCSE Designing Security for a Microsoft Windows 2000 Network Study Guide.** United States of America 2002.

- Fay, J. (1993) **Encyclopedia of Security Management Techniques & Technology**. E.E.U.U., Butterworth-Heinemann.

- Farley, M., Hsu J. y Stearms, T. (1997) **Guía de Seguridad e Integridad de Datos.** España, McGraw Hill.

- Hare, C. y Siyan, K. (1995) **Como diseñar una de red?. En: Internet y Seguridad en Redes.** México, Prentice-Hall.

- Holzbaur, H y Seachrist, D. (1997, Abril 21). **Internet Firewall Software: for companies with web sites, this software is essential for keeping unauthorized visitors out of LANs.** Computer Dealer New.[Online] Vol. 13. Pp. 1-4. Disponible: http://www.elibrary.com [1998, Noviembre 25]

- Klaus, C. y Ranum, M. (1996, Julio 29). **ONE ON ONE: Does scanning for vulnerabilities mean your firewall is safe?.** InfoWorld. [Online]. Vol. 18. P.p 1-2. Disponible: http://www.elibrary.com [1998, Noviembre 25]

- CISCO SYSTEM Co. (1999). **Management Cisco Network Security**

- COMER , D. (1996). **Redes Globales de Información con Internet y TCP/IP.** Tercera Edición. México. Editorial Prentice-Hall Hispanoamericana, S.A.

- CRAIG, H. (1997).**TCP/IP Network Administration**, Eyrolls, Ediciones Gestión 2000 S.A.

- Enciclopedia Temática de Informática. (1987). Maveco de Ediciones, S.A.

- GONZALES, N. (1980). **Comunicaciones y Redes de Procesamiento de Datos**. Mc Graw Hill. Segunda Edición. México.

- KARANJIT, S. (1995). **Internet y Seguridad en Redes**. Prentice Hall.

- STALLINGS, W. (1997). **Data and Computer Communications.** Fifth Edition.

Prentice Hall.

- TANENBAUM, A. (1997).**Redes de Computadoras.** México, Prentice-Hall Hispanoamericana, S.A.

- U.N.A. (1985). **Introducción a la Ingeniería de Sistemas.** Tercera Edición. Caracas-Venezuela.

- U.N.A. (1989). **El Campo Profesional : Conceptos y Procedimientos para su Estudio.** Cuarta Edición.Caracas-Venezuela.

- U.P.E.L. (1990). **Manual de Trabajos de Grado de Maestría y Tesis Doctorales**. Primera Edición. Caracas-Venezuela.

FUENTES ELECTRONICAS

www.cert.org/tech_tips/unix_configuration_guidlines.html#intro

www.nwc.com/1012/1012ws1.html

http://www.soscorp.com/products/BS_FireIntro.html#Firewall_types

http://www.interhack.net/pubs/fwfaq/

http://www.phrack.com/search.phtml?view&article=p55-10

http://www.cisco.com/warp/customer/707/advisory.html

http://www.freelabs.com/~whitis/isp_mistakes.html

http://www.checkpoint.com

http://www.checkpoint.com/~joe

http://www.checkpoint.com/opsec/partners/framework/realsecure.html

http://www.opsec.com

http://www.enteract.com/~lspitz/pubs.html

http://www.phoneboy.com/fw1

http://search.securepoint.com

http://fw1.netrex.com/faqcgi/ShowCats.cgi

http://www.cert.org

ftp://info.cert.org/pub/cert_advisories/

http://www.securityfocus.com

http://www.ciac.org

http://us-support2.external.hp.com/atq/bin/doc.pl/sid=4d5dfc4b0e8063ed12/screen=atqSecBul

http://www.rootshell.com

http://www.anticode.com

http://www.nessus.org

http://www.wwdsi.com/saint

http://www.l0pht.com/~weld/netcat

http://www.2600.com

http://www.dnaco.net/~kragen/security-holes.html

http://www.redhat.com

http://www.netscape.com

www.delitosinformaticos.com

www.hispasec.com

www.itpapers.com

www.cert.org

www.microsoft.com

www.sun.com

www.ibm.com/servers/aix

www.hackers.com

www.astalavista.com

www.technet.com

www.google.com.ve

Hecho el Depósito de Ley.
Depósito Legal lft487200400440