INSTITUTO PROFESIONAL INACAP LA SERENA

“METODOLOGÍA DE MEDICIÓN DE VULNERABILIDADES EN REDES DE DATOS DE ORGANIZACIONES”

Trabajo seminario de título conducente a Ingeniero en Conectividad y Redes

PROFESOR GUÍA:

Raúl Astorga Barrios

AUTORES:

Alfonso Antonio Berenguela Castro

Juan Pablo Cortes Collado

Diciembre 2006

AGRADECIMIENTOS

Agradecemos a nuestros padres quienes estuvieron, están y seguirán estando en nuestras metas y desafíos.

Nuestros tutores, cimientos de nuestro conocimiento.

Al soporte emocional de las familias.

A Dios Padre, guía y apoyo espiritual en el transcurso de nuestras vidas.

A todos ellos muchas gracias por su cariño y comprensión.

ÍNDICE GENERAL

INTRODUCCIÓN

La seguridad es una necesidad básica para el hombre, entendiendo ésta dentro del contexto de la prevención de la vida y las posesiones, esto se aprecia a lo largo de la historia de la humanidad, la que registra los primeros conceptos de seguridad a inicios de la invención de la escritura con los sumerios (3000 AC) quienes implementaron sus propias leyes para mantener la seguridad de los individuos, usaban el código de Hammurabi, este código se encargaba de llevar el orden en la vida y de castigar los delitos, pero su esencia era hacer al agresor lo mismo que el hizo a la victima. Se puede apreciar también en la Biblia, cuando los cristianos creaban sus propios sistemas de seguridad para que los romanos no los descubrieran al predicar la palabra del señor. Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los pueblos antiguos. Las pirámides egipcias con sus sin fin de trampas, aun en estos tiempos no se ha podido descubrir como funcionan algunas de ellas, todas las trampas fueron creadas para proteger lo mas preciado que ello poseían y en o que creían, su Faraón, y la vida eterna, el palacio de Sargon, el templo Karnak en el valle del Nilo, el dios egipcio Anubis representado con una llave en la mano, son algunos ejemplos de Seguridad.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos que los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alerta, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos. Como todo concepto, la Seguridad se ha desarrollado y ha seguido evolucionando dentro de las organizaciones sociales. La sociedad se constituye en estructuras de familias las que se agrupan proporcionando más seguridad al individuo y sus pertenencias, además de concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las perdidas eran inaceptables contra las posibles ganancias.

El próximo paso de la seguridad fue la especialización. Así nace la seguridad externa a la organización (es aquella que se preocupa por la amenaza que se encuentra fuera de la organización); y la seguridad interna a ella (aquella que se preocupa por la amenaza al interior de la organización); está comprobado por estudios que cerca del 80% de los ataques se encuentran en la clasificación de Amenazas Internas. Hoy en día, la seguridad, desde el punto de vista legislativo esta en manos de los políticos, a quienes les toca decidir sobre la importancia, de los delitos que se puedan cometer y su castigo. En esto se han conseguido logros bastante importantes, en el área de la prevención de crímenes, terrorismo y riesgo, más que en el pensamiento general sobre seguridad en las Tecnologías de la Información. Este ultimo punto esta en manos de las propias organizaciones, y en nosotros mismos.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros. Gracias a las tecnologías de información hoy en día se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas o reducir la ventaja de los rivales. La información que se maneja es vital para las instituciones, se debe mantener de acuerdo a lo deseado por la institución. Siendo hoy en día la Tecnología de la Información una herramienta tan importante para el desarrollo, ¿se encuentran éstas completamente seguras?, lamentablemente de acuerdo a la realidad no existen sistemas completamente seguros, es necesario buscar todas los posibles aspectos de vulnerabilidad. Es imperante crear conciencia a los usuarios de la necesidad de la seguridad, puesto que la mayor cantidad de ataques se produce por usuarios internos, ya sea conciente o inconscientemente. Los empleados

deben ser entrenados en políticas de seguridad a fin de internalizar las implicancias que esto significa.

Centrando el tema de la seguridad en nuestro país, se sabe de acuerdo a una encuesta que dos tercios de las empresas que cuentan con políticas de seguridad sienten estar en condiciones de detectar o responder efectivamente ante el ataque de intrusos. En tanto, el 68 % de los ejecutivos afirman que los riesgos a la seguridad de datos se han incrementado en los últimos tres años, y el 29 % dice haber sufrido algún tipo de ataque. Sin embargo, menos del 35 % de los ejecutivos considera que la seguridad es una cuestión de alta prioridad[1].

En Chile se espera que el mercado de las Tecnologías de la Información crezca en un 9,7 % en los próximos cuatro años, es por esto que se hace sumamente necesario difundir una cultura de seguridad, creando y aplicando nuevos sistemas y metodologías de seguridad, y por sobre todo crear conciencia a los individuos, ya que las Tecnologías de la Información son solo una herramienta al servicio del hombre, y es responsabilidad de éste velar por su buen desempeño.

Por todo esto ayudaremos a la seguridad de las organizaciones creando este proyecto.

[1] Noticia publicada en www.informatica.cl

DESCRIPCIÓN DE LA PROBLEMÁTICA

Es deber del administrador de red realizar la búsqueda de las vulnerabilidades existentes en la red de datos, pero la mayoría de las veces no se sabe por donde comenzar, que investigar o que preguntar. Además el problema mayor que tienen estos es que no atacan el problema de fondo, sino que aplican parches superficiales, como instalando programas en los equipos y así disminuyendo el rendimiento de las maquinas. En la actualidad un administrador de red no se preocupa mucho de la seguridad, pero cuando llega a tener problemas el tiempo que emplea es mucho mayor al que podría demorar si existiera alguna política o procedimiento para el uso correcto de los recursos informáticos. Sin la búsqueda de vulnerabilidades, las empresas crean una idea errada de su seguridad, piensan que la seguridad de su información es muy poco vulnerable, ya sea porque nunca se han visto afectados o tal vez lo están siendo sin saberlo.

DESCRIPCIÓN DE LA SOLUCIÓN

Para resolver el problema de seguridad de las organizaciones de hoy se creará una metodología de análisis de seguridad para redes de datos que facilite a las instituciones conocer las vulnerabilidades de esta, esto se logra gracias a la respuesta de cuestionarios y otras herramientas que midan los riesgos y vulnerabilidades. Con los datos obtenidos se clasificará la debilidad de la red dentro de un rango y luego se entregará la información suficiente para crear políticas de seguridad que se adapten a la empresa, adoptando las políticas los riesgos serán considerablemente disminuidos.

OBJETIVOS

Objetivo general

Crear una metodología para medir la seguridad de redes de datos que facilite al administrador de red conocer las vulnerabilidades de esta, y que se obtenga la información suficiente para crear políticas de seguridad que minimicen o eliminen todos los posibles riesgos.

Objetivos específicos

- Investigar sobre las herramientas que existan para medir debilidades de una red.

- Diseñar guías y herramientas para medir los riesgos y vulnerabilidades de la red de la empresa u organización.

- Crear las políticas de seguridad de acuerdo a la información obtenida.

- Determinar los costos del análisis.

DELIMITACIÓN DE LA TEMÁTICA

El proyecto será enfocado a la búsqueda de vulnerabilidades en las redes de datos de las organizaciones, tratando la seguridad en la red de la manera más sencilla posible, para facilitar el análisis de riesgos, aplicado en: los procesos y directivas que adopta la institución. No se profundiza en equipos y software existentes, por lo cual se excluyen del estudio.

METODOLOGÍA

El método a utilizar será el empírico-analítico, debido a que es un sistema auto correctivo y progresivo, es decir, el método esta abierto a la incorporación de nuevos conocimientos y procedimientos.

RESUMEN

Este documento muestra la elaboración de una metodología que permite realizar análisis de riesgos a las redes de datos de las organizaciones. Esta consta de cuatro capítulos, en el primer capítulo se dan a conocer los fundamentos de la seguridad, como la definición de un sistema de seguridad, la importancia de la información de las organizaciones y su seguridad física y lógica, además de exponer lo que representa un delito desde el punto de vista legal, tanto nacional como internacional. Una vez que se tienen estos conceptos claros, se da paso al capítulo dos.

El capitulo dos expone el análisis de riesgos planteado por los autores y además se explica que es el riesgo. El procedimiento creado para esto comienza por la determinación de los activos, a modo de averiguar que proteger. Posteriormente se aplican cuestionarios tanto al administrador de red como a los usuarios finales, las preguntas están enfocadas a la recopilación información básica de la organización, también a la seguridad que poseen en su infraestructura, aplicaciones, operaciones y con el personal. Además debemos poner a prueba su seguridad en busca de vulnerabilidades, esto se lleva a cabo con algunas técnicas como la ingeniería social.

El capítulo tres muestra como elaborar Políticas de Seguridad, para la creación de estas se toman en cuenta los elementos que la componen, esto implica la forma en que se deben crear, asignación de responsabilidades, determinación del uso y control de los recursos de las redes, el manejo de la información sensible, la respuesta en el caso que ésta sea violada y la estrategia que se debe usar para que sean válidas dentro de la organización.

En el cuarto capítulo se muestra el desarrollo del proyecto, se exponen datos de la organización donde fue puesto en marcha, se da a conocer la situación actual de

la entidad, según los datos obtenidos con los instrumentos desarrollados, como los cuestionarios y visitas a terreno. Con estos se crean políticas de seguridad acordes con la organización. Además cuenta con el estudio financiero del proyecto, este está orientado a todas las organizaciones, tanto pequeña, mediana y grande, para cada una de estas existe un valor distinto, el que clasificamos de acuerdo a el número de computadores que poseen.

SUMMARY

This document shows the elaboration of a methodology that is able to make an analysis of risks to the data networks of the organizations. It consists on four chapters, in the first one, the fundamentals of security are shown, as the definition of a security system, the importance of the information of the organizations, its physical and logical security and also what is and what is not a crime on a national and international level. Once these concepts are clear, the second chapter begins.

The chapter two exhibits the analysis of risks proposes for the author and explains what a risk is. The procedure created begins by the determination of the belongings, this we will know what to protect. Later questionnaires were applied to the network administrator and also to the end users, the questions are focused to compile basic information of the organization, also to the security that they have in its infrastructure, applications, operations, with the personnel. In addition we must try its security looking for vulnerabilities; this is carried out with some techniques like social engineering.

The chapter tree display who elaborated Policies of security, for the creation of these take into consideration the elements that compose it, the way they must be created, to see that they have a person in charge, determine the use and control of the resources of the network, the handling of the important information, the answer in the case this was violated, the strategy that must be used to make them worth within the organization.

In chapter four the development of the project is shown, expose data of the organization where project was started, itself known the present situation of the organization, in accordance with the results got with tools developed, as the questionnaires and visit land. With the collected data could create the agreed policies of security with the organization. Moreover it has the financial study of the project, this is oriented to all the organizations, small, medium and big, for each

one of these it exist a different value, the one that we classified according to the number of computers that they have.

1. CAPÍTULO I: Fundamentos de Seguridad

1.1. Sistema de Seguridad

Un sistema de seguridad es un conjunto de elementos tanto físicos como lógicos que se encarga de prevenir o remediar posibles riesgos o problemas que se puedan presentar en un determinado momento, una de sus principales características es ser proactivo, un buen sistema de seguridad ayuda bastante en el trabajo y la producción, ya que se minimiza la tarea de corrección.

Para que exista un sistema de seguridad debe haber algo que proteger, he ahí la pregunta, ¿Que debemos proteger?, esta es la primera pregunta que se debe hacer, con esta podemos determinar lo importante o mas bien lo que debemos resguardar de los peligros. En las organizaciones existen activos[1] tangibles e intangibles, en un comienzo lo importante para estas era lo tangible sobre lo intangible, con el tiempo la prioridad de cada uno fue cambiando, para algunas organizaciones es más importante su información que su equipamiento o infraestructura.

1.2. La Información de Las Empresas

Para poder aplicar seguridad a la información debemos conocer las características de esta:

"Un dato es una representación simbólica (numérica, alfabética, etc.), de un atributo o característica de una entidad"[2]

[1] Todo lo que la empresa posee o le deben.

[2] http://es.wikipedia.org/wiki/Dato

"La información es un conjunto de datos organizados, que constituyen un mensaje sobre un determinado ente o fenómeno"[1]

La información no siempre es privada, existe información pública y privada, el análisis de seguridad se centrara en esta última, la información se puede clasificar de la siguiente forma:

- **Critica:** es indispensable para la continuidad de la organización.
- **Valiosa:** es parte importante de la organización.
- **Sensitiva:** sólo debe ser conocida por las personas que la manejan

Existen 3 conceptos que se deben tener en cuenta para la protección de la información: integridad, disponibilidad y confidencialidad.

- **Integridad**: es la característica de permanecer intacta en su origen, a menos que sea modificada por personas con permiso para hacerlo, esta se puede ver afectada por problemas de hardware, software, virus o personas mal intencionadas.
- **Disponibilidad**: característica de estar siempre disponible para su uso por personas autorizadas, también se ve afectada por los mismos problemas que la integridad.
- **Confidencialidad**: es la privacidad y se refiere a que la información solo puede ser conocida por individuos autorizados.

1.3. Seguridad Física

Se encarga del área de protección de los sistema informáticos como hardware, dispositivos de red, dispositivos electrónicos; todo el entorno que los rodea en el lugar que se hallan ubicados (edificios, sistemas eléctricos, seguridad en las

[1] http://es.wikipedia.org/wiki/Información

cerraduras), además de controlar a las personas que están encargadas de la vigilancia de estos, y tanto de los sistemas informáticos como del entorno.

Podemos tomar en cuenta algunos puntos como por ejemplo:

- **Desastres naturales**: está catalogado como desastre natural toda anomalía de la naturaleza. Ejemplos: los maremotos, terremotos, etc.
- **Malas instalaciones**: las instalaciones son un punto bastante importante, como los cables mal ubicados o en mal estado, la infraestructura en malas condiciones, un ejemplo bastante común de esta es que los cables eléctricos y de red estén muy juntos.
- **Ataques hostiles**: el 80% de los ataques a los sistemas de información provienen desde su interior, los entes más peligrosos son los empleados disconformes, éstos están dispuestos a vulnerar la seguridad de la organización.
- **Control de acceso**: con este se pueden manejar bitácoras, llevando un registro del ingreso a las instalaciones, viendo quien, a que hora, lo que hizo y si esta permitido su acceso al lugar.

1.4. Seguridad Lógica

Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."[1], estos son los puntos que la seguridad lógica debe proteger.

- Restringir el acceso a los programas y archivos.

[1] http://www.segu-info.com.ar/logica/seguridadlogica.htm .

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.5. Delitos Informáticos

Al mismo tiempo que Internet supuso un increíble avance en el complejo universo de las nuevas tecnologías, también se configuró como un nuevo instrumento y un medio para la comisión de delitos, singularmente estafas y fraudes. Igualmente trajo consigo la vulneración de los sistemas de seguridad y la invasión en la intimidad de las personas (acceso a bases de datos, intromisiones ilegítimas en las cuentas de correo electrónico, etc.)

Existen multitud de amenazas y ataques que se los puede clasificar en:

1. Ataques Pasivos: el atacante no altera la comunicación, sino que únicamente la “escucha” o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

• Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.

• Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
• Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se verán posteriormente.

2. Ataques Activos: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

• **Interrupción:** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
• **Intercepción:** si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
• **Modificación:** si además de conseguir el acceso consigue modificar el objeto.
• **Fabricación:** se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
• **Destrucción:** es una modificación que inutiliza el objeto.

En la figura 1 se describen gráficamente estos ataques.

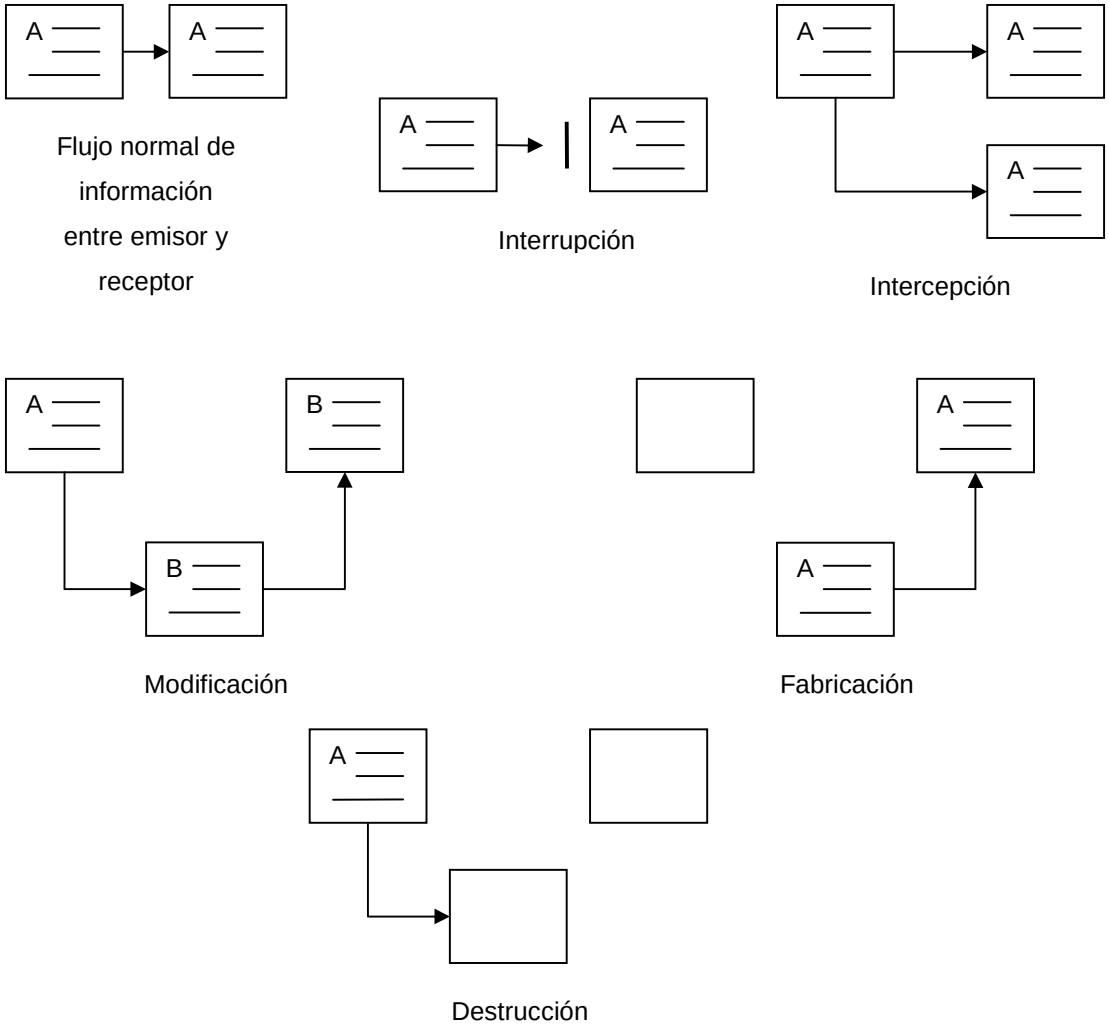

Figura 1: Tipos de ataques activos.

En múltiples ocasiones, los delitos son cometidos por auténticos especialistas, los llamados "piratas informáticos". Según sus objetivos, podemos clasificarlos en dos tipos, por un lado, los hackers, aquellos intrusos que acceden a los equipos de los usuarios con la sola intención de demostrar sus habilidades; generalmente no es su intención dañar los sistemas informáticos de los usuarios, sino simplemente burlar los sistemas de seguridad de los mismos.

Por otra parte y de forma opuesta a los anteriores, los crackers se introducen de forma ilegítima en los equipos con el fin, no sólo de acceder a la información que estos poseen, sino también con la intención de destruirla o de alterarla.

Ambas conductas, tanto la del hacker como la del cracker, son consideradas delitos informáticos dado que suponen una intromisión ilegítima en sistemas y ordenadores ajenos.

1.5.1 Delitos informáticos definidos por la ONU

La Organización de Naciones Unidas (ONU) reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras

    - Manipulación de los datos de entrada, este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

    - La manipulación de programas, consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertido, ya que, el delincuente tiene conocimientos técnicos concretos de informática y programación.

    - Fraude efectuado por manipulación informática, aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada, en que transacciones financieras, apenas perceptibles, van sacando repetidamente de una cuenta, dinero y

transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.

2. Manipulación de los datos de entrada

    - Como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada.
    - Como instrumento, las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial

3. Daños o modificaciones de programas o datos computarizados

    - Sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización, funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

    - Acceso no autorizado a servicios y sistemas informáticos, estos accesos se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.

    - Reproducción no autorizada de programas informáticos de protección legal, esta puede producir una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es una propiedad intelectual.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Ellas son:

- Fraude en el campo de la informática
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.

1.5.2 Legislación Chilena sobre delitos informáticos

Ya que el proyecto esta enfocado a organizaciones chilenas se debe mencionar la Ley de Delitos Informáticos, Ley Nº 19.223 que fue promulgada el 28 de Mayo de 1993, la que consta de tan solo cuatro artículos, ellos son:

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

La pena establecida es presidio menor en su grado mínimo a medio, esto es, de 61 días y hasta 3 años. También se sanciona como delito contra un sistema de información si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, y se aplicará la pena señalada en el inciso anterior en su grado máximo, es decir, de 3 años y 1 día a 5 años.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio o de 61 días y hasta 3 años.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio o de 541 días a 3 años.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio 541 días a 3 años. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado, de 3 años y 1 día hasta 5 años.

En conclusión, la legislación chilena en cuanto a la seguridad informática, deja muchos agujeros y diversas interpretaciones, así la mayoría de los delitos informáticos no son sancionados, es por eso, que cada empresa debe hacer lo posible por mantener seguro su sistema, agregando leyes o normas internas.

Todo documento de seguridad en redes de datos muestra la importancia de realizar análisis de riesgos y la creación de políticas de seguridad, el estándar de seguridad internacional está plasmado en las ISO 17799 e ISO 27001, además existen metodologías para realizar análisis de seguridad, entre los más importantes se encuentran OSSTMM 2.1., que es una metodología abierta de

testeo de seguridad, y Microsoft Security Assessment Tool herramienta que a través de una serie de preguntas pretende determinar el estado de seguridad de la red.

En el capítulo siguiente se plantea la metodología desarrollada por los autores de este documento, el cual muestra los pasos detallados para la realización de un análisis de riesgos.

2. CAPÍTULO II: Análisis de Riesgos

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué protecciones se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas que se relacionan según el siguiente esquema de la figura 2.

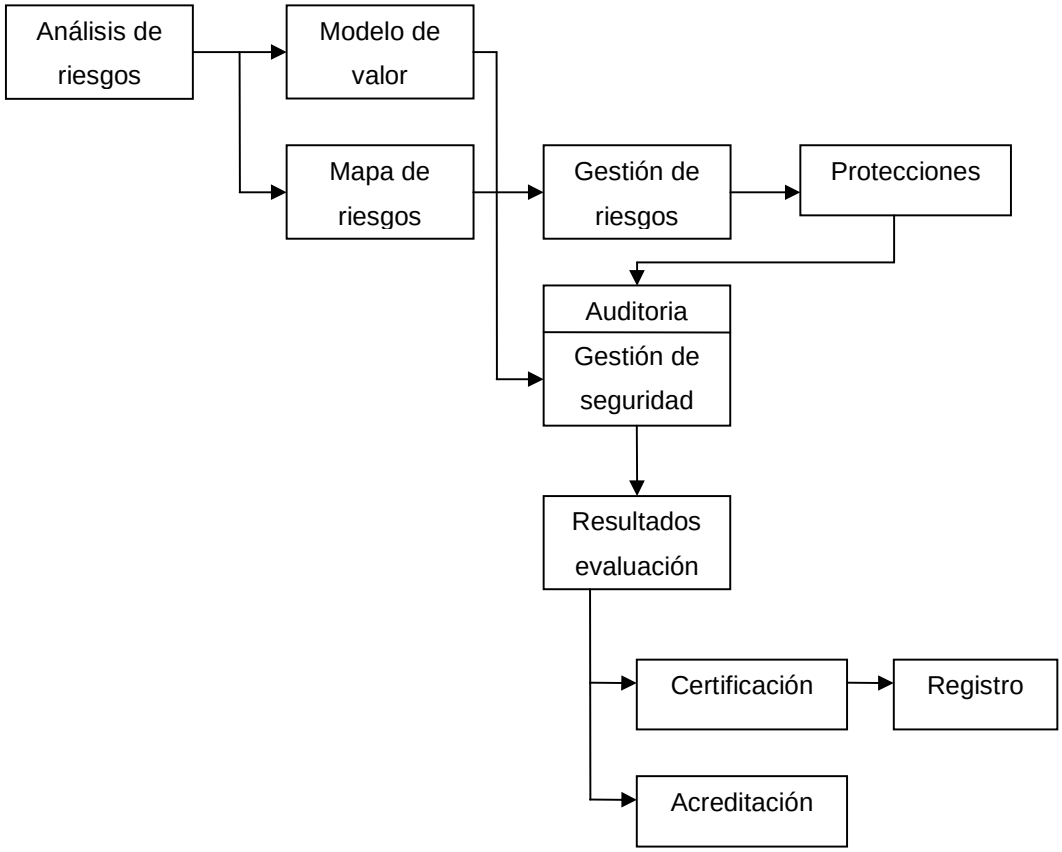

Figura 2: Esquema de auditoria de seguridad

Realizar un análisis de riesgos es laborioso y costoso. Levantar un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la Organización, desde los niveles de gerencia hasta los técnicos. Y no solo es que haya que involucrar a muchas personas, sino que hay que lograr una uniformidad de criterio entre todos, si es importante cuantificar los riesgos. Y esto es así, porque típicamente en un análisis de riesgos aparecen multitud de datos. La única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo riesgo) y obviar lo que es secundario o incluso despreciable. Pero si los datos no están bien ordenados, su interpretación es imposible.

En resumen, un análisis de riesgos no es una tarea menor que realiza cualquier persona en sus ratos libres, esta es una tarea que requiere esfuerzo y coordinación, por lo tanto, debe ser planificada y justificada.

Un análisis de riesgos es recomendable en cualquier Organización que dependa de los sistemas de informaciones y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para asegurar la continuidad de la actividad, pasando por las decisiones de adquisición de protecciones técnicas y de selección y capacitación del personal.

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones. Las que pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo de las aplicaciones y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en descenso de la imagen prestada por la Organización y puede suponer, en

último extremo, la pérdida de confianza en su capacidad. Siempre se ha dicho que es mejor prevenir que curar y aquí se aplica.

Algunos elementos que necesitamos identificar para el análisis son:

1. Activos, son los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización.

2. Amenazas, son elementos que les pueden pasar a los activos causando un perjuicio a la Organización.

3. Protecciones (Políticas de seguridad), son elementos de defensa desplegados para que aquellas amenazas no causen daño.

Con estos elementos se puede estimar:

1. El impacto: la pérdida que se provocaría.
2. El riesgo: lo que probablemente pase.

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

La herramienta desarrollada por los autores del documento para determinar las vulnerabilidades se divide en cuatro secciones, que son:

- Determinación de activos
- Cuestionario al administrador de red
- Preguntas a usuarios
- Búsqueda de vulnerabilidades

En el mercado existe la idea general de lo que se debe realizar para determinar las vulnerabilidades, pero en los pasos anteriormente nombrados se describe claramente el qué preguntar y qué observar.

2.1 Determinación de activos

Es de suma importancia determinar cuales son los activos importantes de la organización y cual seria el impacto que produciría si llegasen a faltar. Se debe crear una lista de los activos que posee la organización, todo aquel que tenga que ver con la red de datos y su desempeño, una vez obtenidos, estos se clasifican en una tabla de importancia, para ello utilizando el esquema de la figura 3, se tiene una guía para determinar el impacto que tiene el activo, la pregunta para poder clasificarlos es: ¿qué efecto tendría en la red si el activo faltase? Al clasificarlos podemos agrupar los activos y así hacer la tarea del análisis menos complicada, es más fácil porque se pueden concentrar los esfuerzos en los activos de mayor importancia en la red. La técnica es concentrarse primero en los que su falla es inaceptable o muy importante y luego los de menor jerarquía

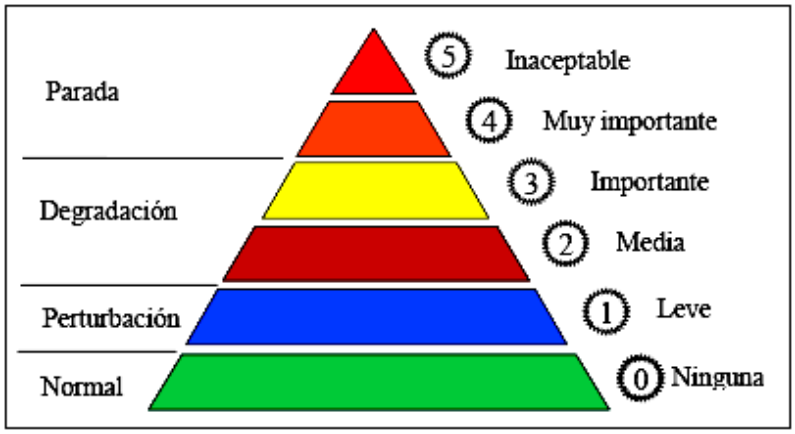

Fig. 3: Clasificación de activo

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan protección para asegurar las correctas operaciones del negocio y la continuidad de la empresa

Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:

1. Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad,
2. Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio,
3. Activos de software: Software de aplicación, software de sistemas, herramientas de desarrollo,
4. Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos,
5. Personas: Personal, clientes, suscriptores,

La tarea de clasificar los activos debe ser lo más ordenada posible, es por eso que se utiliza la tabla 1 para listar los activos y la importancia asignada. En la primera fase, de clasificación de activos, se rellenarán las primeras tres columnas, las siguientes se rellenarán al desarrollar las otras etapas de la metodología. En el campo Código se utiliza un número interno, este es solo para mantener el orden. El campo Importancia se rellenará según criterio y observando el esquema de la figura 3, es decir, con escala de 0 a 5.

Activo			**Usuario**	**Posibilidad de ataque**	**Medidas de seguridad**
Código	**Nombre**	**Importancia**			

Tabla 1: Lista de activos.

2.2 Cuestionario al administrador de red

Esta evaluación se ha diseñado para identificar el riesgo en la red de la empresa y las medidas de seguridad utilizadas para mitigar dicho riesgo. Se han desarrollado preguntas con las que es posible realizar una evaluación de alto nivel de las tecnologías, los procesos y el personal de la empresa.

2.2.1 Información básica de la empresa

En primera instancia es necesario obtener una visión general del funcionamiento de la red en la empresa, es por esto que la primera sección de preguntas al administrador se enfoca en determinar si existen conexiones hacia Internet, el tipo de esta, los datos que procesan y quienes acceden a estos. En otras palabras se pregunta por:

- Si la empresa posee una conexión, tales como T-1, línea DSL, cable módem, o cualquier conexión que siempre este activa, ya que esto es una puerta abierta a intrusos y virus.
- El tipo de uso de la conexión y el acceso a páginas útiles al trabajo, es recomendable bloquear las peligrosas y las innecesarias. Conocer también los permisos en las estaciones de trabajo y los servidores, que los usuarios ejecuten servicios no autorizados aumenta el riesgo de un ataque.
- El acceso a la red, conocer quienes acceden a los recursos de la red.
- La existencia de conexiones remotas, esto abre puertas por donde atacar el sistema.
- También es importante conocer el tipo de aplicaciones que se alberga, aplicaciones para socios o clientes aumenta los riesgos en la infraestructura debido a la posibilidad de un robo, pérdida de dato o la no disponibilidad de servicios.

- La existencia de segmentación de la red, los recursos en el mismo segmento aumenta los riesgos porque, un ataque podría causar daños a ambos.
- Conocer si la empresa comparte sus oficinas con otras entidades, el compartir el entorno con empleados de otras empresas presenta un grave peligro, se puede producir daños a materiales y datos.
- Y por supuesto, averiguar si la empresa sería capaz de operar sin ningún equipo, por ejemplo, se produjese un incidente viral grave que dejase fuera de línea todos los sistemas.

El detalle de estas preguntas se encuentra en el anexo I, en las siguientes secciones se analiza más a fondo en el manejo de la red y del personal.

2.2.2 Seguridad de la infraestructura

La seguridad de las infraestructuras se centra en cómo debe funcionar la red, los procesos comerciales, cómo se crean y utilizan los hosts, la gestión y el mantenimiento de la red. La seguridad de la infraestructura efectiva puede ayudar a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. Con esta sección de preguntas se podrá identificar las áreas de riesgos y desarrollar métodos para reducir las amenazas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para mitigar el riesgo de la infraestructura enfocándose en las áreas que siguen:

- Defensa del perímetro
- Autenticación
- Gestión y control

2.2.2.1 Defensa del perímetro

En esta sección se obtiene información acerca de la seguridad del perímetro de la red, donde la red interna se conecta con el exterior, aquí debe estar el primer escudo protector contra los intrusos externos.
Se busca información de firewalls, DMZ, IDS, antivirus, redes inalámbricas, segmentación de la red, asignaciones de direcciones, VPN, y de esta última la utilización de autenticación de factores múltiples, esta requiere dos o más de las categorías siguientes: algo que sepa el usuario (ejemplo: contraseña), y algo que sea propio del usuario (ejemplo: huella digital, retina).

El detalle de estas preguntas se encuentra en el anexo II.

2.2.2.2 Autenticación

Los procedimientos estrictos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos. Además se debe velar por el cumplimiento de las normas de seguridad, sin los mecanismos adecuados para aplicarlas, las normas para las contraseñas generalmente se ignoran. Las políticas para las contraseñas deben cumplirse en todas las cuentas, no sólo en las de los administradores.

El acceso a aplicaciones y datos sensibles debe limitarse conforme a los privilegios de cada cuenta. Es importante disponer de mecanismos para el cumplimiento de estas limitaciones a fin de evitar traspasos de información no autorizados.

Para proteger el sistema frente a ataques de fuerza bruta, las cuentas deben configurarse para que no permitan el acceso después de una cantidad

determinada de intentos fallidos. La mayoría de los sistemas de autenticación permite la aplicación automatizada de normas referente a la longitud, la complejidad y el vencimiento de las contraseñas, entre otros.

Un punto de vital importancia es validar los datos de entrada para evitar que las aplicaciones procesen información peligrosa o incorrecta; de lo contrario, los datos podrían estar sujetos a daños, robos, o incluso se podría ejecutar código binario.

El detalle de estas preguntas se encuentra en el anexo III.

2.2.2.3 Administración y control

La gestión, supervisión y el registro adecuados son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.

Es importante utilizar imágenes documentadas para mantener la uniformidad entre todos lo equipos de escritorio y las terminales de trabajo. Esta uniformidad permitirá una mayor eficacia en la detección y paralización de ataques potenciales. Así también configurar los equipos, ya que la configuración predeterminada con la que llegan se crea para maximizar las características disponibles y por lo general no se da importancia a la seguridad.

También se debe robustecer los hosts, esto implica actualizar sistema operativo. Aplicar los parches adecuados, reforzar las configuraciones y auditar el acceso y las vulnerabilidades de los sistemas.

Las medidas de seguridad física incluyen cables de bloqueo para equipos portátiles, armarios o racks con llave para servidores/equipos de red y guardias de seguridad.

El detalle de estas preguntas se encuentra en el anexo IV.

2.2.3 Aplicaciones

Este segmento estudia las aplicaciones que son esenciales para la empresa y las valora desde el punto de vista de la seguridad y disponibilidad, además se examinan tecnologías utilizadas para aumentar el índice de defensa en profundidad.

Se cuestiona sobre el tipo de dato que se maneja en la empresa, uso de macros para Microsoft Office, adquisición de software, actualizaciones y parches, y si la empresa esta al tanto de sus vulnerabilidades.
El detalle de estas preguntas se encuentra en el anexo V.

2.2.4 Operaciones

En esta sección se valora las prácticas de funcionamiento y las normas que siguen la empresa para aumentar las estrategias de defensa en profundidad a fin de emplear más que meras defensas tecnológicas. Se estudian áreas relacionadas con la creación de sistemas, la documentación de la red, las copias de seguridad y la restauración de datos en el entorno.

- La revisión contempla los siguientes procedimientos:
- Entorno, creación del sistema, documentación de la red, flujo de datos de aplicaciones.
- Directiva de seguridad, protocolos y servicios, gestión de cuentas de usuarios
- Actualizaciones y gestión de actualizaciones, firmas de virus
- Copias de seguridad y recuperación, almacenamiento y pruebas.

2.2.4.1 Entorno

La seguridad de la empresa depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. La capacidad de los equipos de operaciones para mantener la seguridad del entorno depende en forma crucial de la documentación exacta del entorno y de las pautas.

El detalle de estas preguntas se encuentra en el anexo VI.

2.2.4.2 Directiva de seguridad

Al asignar niveles de prioridad a los componentes, una empresa estará más preparada para centrar sus esfuerzos de seguridad en aquellos sistemas que necesitan acceso. Disponer de una lista de este tipo también asigna una prioridad para la recuperación cuando se producen apagones.

Las directivas son reglas y prácticas que especifican cómo se puede utilizar de forma adecuada un entorno informático. Si no existen directivas, no existe mecanismo alguno para definir o hacer cumplir los controles dentro del entorno.
La política corporativa del uso aceptable regula el uso adecuado de los recursos corporativos, aplicaciones de red y sistemas incluidos.

La sección de preguntas en el anexo VII cuestiona acerca de las directivas para todos los aspectos de seguridad, como usuarios, los sistemas y los datos.

2.2.4.3 Gestión de actualizaciones y revisiones

Los procesos de gestión de cambios y configuraciones permiten asegurar que los cambios en el entorno de producción, se han probado y documentado exhaustivamente antes de utilizarse.

La aparición de nuevos virus es constante, por lo que resulta imprescindible mantener una lista actualizada de firmas de virus. Su solución antivirus será tan eficaz como lo permita su lista de firmas de virus.

La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque. Las preguntas que se encuentran en el anexo VIII indagan en este campo.

2.2.4.4 Copias de seguridad y recuperación

Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallos de hardware o software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad.

Las preguntas del anexo IX intentan averiguar las medidas de respaldo que posee la empresa actualmente.

2.2.5 Personal

Es necesario revisar los procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la formación y el grado de conocimientos de los empleados sobre la seguridad. También el centrarse en la seguridad en las operaciones diarias. Las preguntas que se encuentran en las siguientes subsecciones ayudan a valorar cómo se mitigan los riesgos del área de personal. Aquí se observa información como subcontratar la implantación de la infraestructura

2.2.5.1 Requisitos y evaluaciones

Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. Las evaluaciones periódicas realizadas por terceros pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras.

Las preguntas referentes a este campo se encuentran en el anexo X.

2.2.5.2 Directiva y procedimientos

Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos. Por eso es bueno contar con los procedimientos claros y prácticos, se intenta determinar como se encuentra la empresa en campo con las preguntas realizadas en el anexo XI. Estas preguntas toman en cuenta, entre otros, lo siguiente:

- Comprobar el historial personal de aspirantes para identificar asuntos que puedan afectar a la seguridad de su empresa.

- Cuando los empleados dejan la empresa, existe la posibilidad de que lo hagan de forma hostil. Para reducir los riesgos, se debe mantener un proceso formal para los empleados que dejan la empresa.

2.2.5.3 Formación y conocimiento

Un programa de divulgación de las medidas de seguridad mantiene a los empleados al corriente de los riesgos y vulnerabilidades presentes. Los empleados que son conscientes de su importancia benefician la seguridad general de la empresa.

La formación basada en roles y el aprendizaje continuo garantizan que todos los empleados entiendan qué se espera de ellos. Para conocer como se desarrolla la empresa en este campo se dispone de un conjunto de preguntas que se encuentran en el anexo XII.

2.2.6 Evaluación del cuestionario

Una vez obtenidas las respuestas por parte del administrador se procede a evaluarlas convencionalmente, traspasando las respuestas a la herramienta EXCEL para confeccionar gráficos. En esta metodología se otorga un valor de vulnerabilidad y de seguridad para cada una de las preguntas, tal como se aprecia en la tabla 2, posteriormente se agrupan los valores vulnerabilidad y protección de la sección a la que corresponde para desarrollar con ellos gráficos, a modo de visualizar de mejor forma los resultados.

Vulnerabilidad	Escala	Respuesta
-	0 o 2	Sí - No lo sé

Protección	Escala	Respuesta
-	0 o 2	No

Tabla 2: Formato escala de evaluación de pregunta tipo.

La tabla 2 muestra la escala de evaluación de la pregunta número 4 de la sección Información básica de la empresa, anexo I, esta es:

¿Los usuarios internos y externos usan los recursos del mismo segmento de red?

- Sí
- No
- No lo sé

Dependiendo de la respuesta que entregue el administrador se asignará el valor máximo a la alternativa elegida y mínimo a la rechazada. Por ejemplo, si el administrador en la pregunta 4, responde “sí comparten el mismo segmento los usuarios”, lo que es un peligro para los datos de ambas parte, la tabla quedaría de la forma que se muestra en la tabla 3, el caso contrario se muestra en la figura 4. Por defecto se entregan como vulnerabilidad las respuestas “No lo sé”.

Vulnerabilidad	Protección
2	0

Tabla 3: Evaluación pregunta 4

Vulnerabilidad	Protección
0	2

Tabla 4: Evaluación pregunta 4.

Existen algunas preguntas que dependiendo del resultado permiten contestar subpreguntas, la evaluación cambia en estos casos, observar tabla 5, se otorga mayor cantidad de puntos según la respuesta obtenida de las subpreguntas. Utilizando como ejemplo la pregunta número 1 de la sección Defensa del perímetro, la cual si obtiene como respuesta Sí, se es posible contestar otras dos preguntas.

Vulnerabilidad	Escala	Respuesta	Protección	Escala	Respuesta
-	0 o 2	No - No lo sé	-	0 a 4	Sí

Tabla 5: Formato escala de evaluación pregunta 1.

1. ¿Su empresa utiliza firewall u otros controles de acceso en los perímetros de la red para proteger sus recursos?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

1.1. ¿Su empresa aplica estos controles en todas las oficinas?

- o Sí
- o No
- o No lo sé

1.2. ¿Su empresa usa una red DMZ para separar redes internas y externas de los servicios albergados?

- o Sí
- o No
- o No lo sé

En caso de responder “No”, la tabla se rellena de forma normal, tal como se muestra en tabla 6. Esto se debe a que no se debe contestar las subpreguntas.

Vulnerabilidad	Protección
2	0

Tabla 6: Evaluación pregunta 1.

En caso de responder “Sí” a la pregunta 1, se adicionan los resultados de las subpreguntas, si los resultados son negativos en las subpreguntas, se evalúa solo con un puntaje de 2. Si la empresa posee estos equipos en todas las sedes, se adiciona 1 a la columna “protección”, si posee una red DMZ, se adiciona

nuevamente 1 al puntaje. Por ejemplo, si tan posee firewall en todas sus sedes, pero no posee una red DMZ, la evaluación luciría como observa en la tabla 7.

Vulnerabilidad	Protección
0	3

Tabla 7: Evaluación pregunta 1.

Las distintas evaluaciones se encuentran al final de cada anexo de preguntas.

2.3 Preguntas a usuarios

Para obtener una visión general de la seguridad de la red es necesario recurrir a quiénes la utilizan a diario, el personal de la empresa, los que poseen la mejor apreciación del funcionamiento de la red. A continuación se presenta un grupo de preguntas que se realizan a los usuarios, esto ayudara de manera importante a la evaluación de la seguridad de la red.

1. ¿Sólo usted accede a este equipo?
2. ¿Ha sido notificado de políticas de seguridad que debiese cumplir?
3. ¿Tiene permisos para instalar cualquier tipo de programas en su estación de trabajo?
4. ¿Utiliza contraseña para iniciar sesión en su equipo?
5. ¿Cambia regularmente su contraseña?
6. ¿Cada cuánto tiempo cambia la contraseña?
7. ¿Existe alguna norma o formato para la creación de la contraseña?
8. ¿Bloquea el equipo cuando debe ausentarse?
9. ¿Ha sido capacitado en seguridad en informática, ya sea en el cuidado al descargar archivos o programas desde Internet?
10. ¿Su estación de trabajo ha sufrido ataques de virus?
11. ¿Ha sufrido pérdida de información en su estación de trabajo?
12. ¿Procesa información de la empresa fuera de ella?

13. ¿Tiene acceso ilimitado hacia Internet en su estación de trabajo?
14. ¿Utiliza programas que no tienen relación con su labor?
15. ¿Utiliza el correo corporativo para fines ajenos a la empresa?
16. En caso de fallar el equipo ¿existe algún procedimiento para la reparación?

2.3.1 Evaluación preguntas a usuario

Las preguntas realizadas a usuarios van en directa relación con el cuestionario realizado al administrador de red, ya que dependiendo de las respuestas obtenidas de esta sección se procederá a mantener o disminuir el puntaje de preguntas que tengan relación con ellas en el cuestionario.

Por ejemplo si el administrador en la pregunta 1.1 de la sección Autenticación, anexo III, respondió que existen controles para usuarios.

1.1. Seleccione las cuentas para las cuales existen controles que hagan cumplir las políticas de seguridad por contraseña.
- o Administrador
- o Usuario
- o Acceso remoto

Pero al realizar la pregunta 7 a los usuarios, estos responden “No”, esto implica que no se está dando cumplimiento a los controles. En la evaluación de la pregunta 1 de la sección Autenticación se descontará puntaje, tal como se muestra en la tabla 8. El puntaje a descontar depende del impacto de la vulnerabilidad, la escala variará desde 1 a 3, en caso de respuesta satisfactoria se conservará la puntuación.

Evaluación primaria			Evaluación final	
Vulnerabilidad	Protección		Vulnerabilidad	Protección
0	4		0	3

Tabla 8: Descuento de puntaje en la evaluación

2.4 Búsqueda de vulnerabilidades

Una vez realizado los pasos anteriores se posee bastante información que sin duda ayuda a realizar un buen análisis de riesgos, pero ¿la información respondida por el administrador y usuarios es completamente fiable?, es por esto que es necesario realizar una serie de pruebas básicas para verificar las respuestas obtenidas y determinar si se da cumplimiento a las políticas existentes. Esto es claramente parte de la etapa de visita en terreno, una de las técnicas más utilizadas y efectiva es la ingeniería social[1] ésta es aplicable tanto al administrador de red como a los usuarios finales, a veces a las personas el responder un cuestionario no les es completamente agradable, por ello es mejor hacer una especie de entrevista o conversación amena después de que halla respondido el cuestionario así se puede determinar con claridad si sus respuestas son sinceras.
Las pruebas que a continuación se presentan son alguna que se pueden realizar para verificar las respuestas y determinar otras posibles vulnerabilidades.

1. Observar si el acceso es restringido a lugares de trabajo.
2. Observar si el acceso es restringido a lugares críticos, como un cuarto de telecomunicaciones.
3. Observar si los puntos de red son accesibles a extraños.

[1] Ingeniería Social es persuadir a otra persona (a través de diversas formas) para que nos de un dato útil para cumplir un objetivo.

4. Revisar los programas existentes en las estaciones de trabajo, a fin de encontrar programas que no pertenecen a la labor del usuario, por ejemplo MSN, Ares.
5. Observar si la estación posee las últimas actualizaciones en el software que utiliza.
6. Revisar equipos de trabajo en momentos en que no se encuentre el usuario, para determinar si este cumple con algunas forma de seguridad básica como por ejemplo el bloqueo del equipo.
7. Poner a prueba la reacción de los usuarios, por ejemplo, intente extraer algún equipo del lugar de trabajo, previo aviso solo a los jefes de área.
8. Conéctese a la red, utilizando un Sniffer rescate paquetes y observe si estos están encriptados o si puede extraer datos importantes.
9. Observar si existen contraseñas a la vista, como por ejemplo, el uso de papeles adheridos en los equipos.
10. Observar si el lugar de trabajo esta limpio, para que no exista algún riesgo para los equipos.
11. Conectarse directamente a la red y enumerar los puertos, para esto se puede ejecutar el comando nmap –sS -o, ó en caso de contar con herramientas especializadas realizar una de las siguientes operaciones:
    - Usar escaneo SYN TCP (Half-Open) para enumerar puertos abiertos, cerrados o filtrados para aquellos puertos TCP utilizados por defecto en el test, en todos los servidores de la red.
    - Usar escaneo TCP full connect para escanear todos los puertos por encima del 1024 en todos los servidores de la red.

En el anexo XIII se encuentra un listado de los puertos que utilizan virus troyanos para ingresar a los sistemas.

Las acciones antes mencionadas serán necesarias para demostrar a la jefatura de la empresa algunas de las vulnerabilidades a las que está expuesta. Estas acciones de igual forma podrán ayudar a corroborar las respuestas de los

cuestionarios realizados. Si se demuestra que hay respuestas erróneas, sus puntajes serán modificados.

3. CAPÍTULO III: Políticas de Seguridad

Una política es un protocolo documentado que describe el sistema de seguridad concerniente a una red de una organización. Este documento describe los pasos a seguir para generar un sistema seguro y estable, que permita tanto a usuarios como al sistema en si, mantener sus bienes de información seguro de cualquier tipo de ataque intencional como casual.

El gestor de una política de seguridad contempla reglas orientadas a la identificación de recursos, amenazas, responsabilidades de los usuarios en la red, planes de acción cuando la política de seguridad es violada. Además entrega procedimientos de administración de la red.

A continuación se presenta las normas básicas para desarrollar correctamente las políticas de seguridad.

3.1. Elementos de una política de seguridad informática.

Una PSI (política de seguridad informática) debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos

así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que alberga el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.
- Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Hay que considerar que una organización puede tener una red compuesta de múltiples subredes y fuentes de información, siendo controladas estas subredes por diferentes administradores, los cuales pueden tener diferentes metas y objetivos para las redes que administran. Si estas redes no están interconectadas, cada administrador puede tener sus propias políticas de seguridad. Si son parte de una red central, estos administradores deben de seguir las políticas centrales de seguridad, las cuales no irán en contra de políticas internas que los administradores, de las subredes, implementen para aumentar la seguridad de estas. Lo importante es mantener metas comunes de seguridad.

Las metas deben contemplar la seguridad de todos los elementos y recursos que forman la red y las subredes como:

- Estaciones de trabajo
- Servidores
- Dispositivos de interconexión: Router, Hub, Switches. etc.

- Terminales de servidores.
- Software de aplicaciones y de sistemas de redes.
- Cable de redes.
- Información en archivos y bases de datos.

La PSI debe de tomar en cuenta la protección de estos elementos.

Debido a que una red puede estar conectada a otras redes (ej: redes bibliotecarias), la política de seguridad debe considerar las necesidades y requerimientos de todas las redes interconectada. Este es un punto importante a considerar, ya que al proteger los intereses de la red que se administra se puede perjudicar a otras redes.

3.2. Metodología de generación de la política de seguridad.

Definir una política de seguridad de una red significa desarrollar procedimientos y planes que resguarden los recursos de la red en contra de la pérdida y daño de esta. La metodología para desarrollarla es examinando las siguientes preguntas:

- ¿Qué recursos son los que se tratan de proteger?
- ¿De quiénes se deben proteger?
- ¿Cuáles son las probables amenazas?
- ¿Cuan importante es el recurso a proteger?
- ¿Qué medidas se pueden ejecutar para proteger los bienes de forma efectiva?
- Examinar periódicamente la red para observar si deben cambiar los objetivos de trabajo de la política de seguridad

Se debe considerar que el costo de implementación de seguridad debe ser menor al costo que tiene el recobrar los bienes afectados ante un ataque de seguridad. Puede llegar a ser difícil la implementación de una política de seguridad si no

cuentan con los conocimientos necesarios sobre lo que se desea proteger y de los orígenes de amenazas. Para lograrlo se deberá pedir ayuda a otros que tengan mayor conocimiento para lograrlos.

3.3. Asegurar las responsabilidades de la política de seguridad.

Un aspecto importante en la política de seguridad de una red es asegurar que cada involucrado conozca su responsabilidad para el mantenimiento de la seguridad. Es difícil que una política de seguridad anticipe todas las posibles amenazas.

Deben existir varios niveles de responsabilidad asociados con la política de seguridad. Cada usuario de la red debe ser responsable de resguardar su contraseña. Un usuario que facilite su cuenta aumentada la posibilidad de comprometer otras cuentas, así como recursos. Por otro lado, los administradores de redes y de sistemas de administración son responsables de mantener toda la seguridad de la red.

La organización debe facilitar los instrumentos necesarios para comprometer y obligar a los usuarios y administradores a mantener las políticas de seguridad. Firmar documentos, contratos o compromisos donde se estipulan compromisos y sanciones a los infractores, son herramientas que permiten el correcto uso de los recursos, permitiendo disminuir los riesgos que un usuario podría generar.

La prohibición del uso de equipos para uso personal, no descargar información que no sea relacionada a la organización, la no utilización de software no autorizado por la organización, son algunas reglas que son parte de una política de seguridad.

Al crear la responsabilidad en la política de seguridad, hay que tener en cuenta que cada red o subred tiene reglas o políticas distintas. El análisis de riesgos entrega la información que indica la o las redes con mayor riesgo e importancia, por lo que la responsabilidad de un usuario que utiliza estas redes es mucho mayor a uno que utiliza una red de menor importancia para la organización.

3.4. Responsabilidades y uso de la red.

Existe un número de asuntos que deben ser cubiertos cuando se desarrolla una política de seguridad:

- ¿Quién tiene permitido el uso de los recursos?
- ¿Cuál es el uso apropiado del recurso?
- ¿Quién está autorizado para conceder acceso y aprobar el uso?
- ¿Quién tendrá privilegios de administrador?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?
- ¿Cuáles son los derechos y responsabilidades del administrador de sistemas versus aquellas de un usuario?
- ¿Qué se debe hacer con información sensible?

3.5. Autorizaciones para el uso de los recursos de red.

Se debe elaborar una lista de usuarios que necesiten acceder a los recursos de la red. Los usuarios pueden ser parte de grupos de cuentas como usuarios abogados, ingenieros, administradores, etc. Se debe incluir una clase de usuarios, llamados usuarios externos, los cuales acceden a la red de otro lugar, siendo estos miembros de la empresa, accediendo remotamente.

3.6. Identificación del uso apropiado de un recurso.

Después de identificar a los usuarios que accederán a los recursos de la red, se debe proveer los lineamientos para un uso responsable de ese recurso. Estos lineamientos dependerán de la clase de usuario, como desarrolladores de software, estudiantes, facultativos, usuarios externos, etc.

Para cada tipo de usuario existirá un alineamiento distinto. La política deberá declarar que tipo de uso de la red es aceptable, y que tipo de uso es restringido. La política que se desarrolla es llamada “Política de uso aceptable” (PVA) para la red. Si el acceso a recursos de la red es restringido, se debe considerar el nivel de acceso de las distintas clases de usuarios que se tienen.
La PVA debe ser clara que al irrumpir en una cuenta o eludir la seguridad, no está permitido, de esa forma se evitan problemas legales por parte de los miembros de la organización que hayan eludido la seguridad de la red ya que ellos pueden acusar de que no fueron informados apropiadamente o no fueron entrenados en la política de la red.

La siguiente lista de temas debe ser cubierta cuando se desarrolla una PVA:

- ¿Es permitido irrumpir en otra cuenta que no sea la propia?
- ¿Es permitido descifrar password?
- ¿Es permitido deteriorar el servicio?
- ¿Se permitirá a los usuarios modificar archivos que no les pertenecen, aun si ellos tuvieran permisos de escritura?
- ¿Podrán los usuarios compartir sus cuentas?

A menos de que se tengan una necesidad inusual, la respuesta a estas preguntas es No. Es bueno agregar a las políticas una declaración concerniente a las licencias y derechos de software.

3.7. Determinar quien autoriza acceso y aprueba el uso.

La política de seguridad deberá identificar quien está autorizado a conceder acceso a los servicios, además de determinar el tipo de acceso que puede conceder. De no suceder lo indicado, es difícil mantener un control de quién utiliza la red.

Al cumplir lo anterior, se pueden encontrar los tipos de accesos o controles que se han concedidos. Esto es útil para la identificación de las causas de agujeros de seguridad como resultado de la entrega de privilegios excesivos a usuarios.
Si a los usuarios que se le han entregado privilegios, no son responsables y confiables, se corre el riesgo de crear agujeros de seguridad en el sistema y conceder privilegios inconsistentes a un usuario. Un sistema en esta situación regularmente dificulta su administración.

En una red, pueden existir un gran número de subredes y administradores de sistemas, lo cual dificulta el mantener un registro de los permisos que se han concedido a los recursos de la red. Se debe utilizar un sistema formal para los requerimientos de privilegios o permisos. Después de que un usuario realiza una petición y que esta ha sido autorizada por un supervisor, el administrador del sistema deberá documentar las restricciones de seguridad o los accesos que se le han concedido al usuario.

3.8. Determinación de las responsabilidades de los usuarios.

La política de seguridad debe definir los derechos y responsabilidades de los usuarios al utilizar los recursos y servicios de la red.

Se deben considerar temas concernientes a las responsabilidades de los usuarios.

- Directrices concernientes al uso de recursos de red como la restricción de usuarios y el tipo de restricciones.
- Que constituye abuso en términos de uso de los recursos de red y del funcionamiento de la red.
- Permitir o no a un usuario compartir su cuenta.
- ¿Un usuario podrá revelar su contraseña para acceder a una cuenta para permitir a otros usuarios trabajar en un proyecto?
- ¿Cuán frecuentemente los usuarios cambian sus contraseñas y otros requerimientos relacionados a ella?
- ¿Es responsable el usuario de proveer respaldo de su información o es responsabilidad del administrador?
- Repercusión para usuarios que revelen información propietaria.
- Acciones legales o castigos deben ser implementadas.
- Declaración de la privacidad de los correos electrónicos.
- Política concerniente a listas de correos, grupos de discusión.
- Política relacionada a la falsificación de e-mail.

La asociación de correos electrónicos (EMA), recomienda que se deba poseer una política sobre la protección de la privacidad de los miembros de una organización. La organización debe establecer políticas de privacidad que no limiten el correo electrónico. La asociación de correos electrónicos (EMA) sugiere cinco criterios para la evaluación de una política:

1. ¿La política cumple con la ley y con los deberes de terceros?
2. ¿Compromete la política innecesariamente el interés del trabajador, el empleador y a terceros?
3. ¿Es la política factible como un asunto práctico y probable de ser impuesta?
4. ¿La política tratará apropiadamente con las diferentes formas de comunicación y conservación de registro en una oficina?
5. ¿La política ha sido anunciada en acuerdo por todos los que les concierne?

3.9. Responsabilidades de los administradores de sistemas.

Los administradores de sistemas, recogen información contenida en los directorios privados de los usuarios para diagnosticar problemas de sistema. El usuario, por otra parte, tiene el derecho de mantener su privacidad, por consiguiente existe una interrelación entre los derechos de privacidad y las necesidades de los administradores de sistemas. Cuando se ha efectuado un ataque a la seguridad de la red, el administrador del sistema podrá tener la necesidad de obtener información de archivos del sistema, incluyendo los directorios raíces de los usuarios.

La política de seguridad deberá especificar el nivel al cual el administrador podrá examinar los directorios privados de un usuario para diagnosticar problemas del sistema e investigar las violaciones de seguridad.
Si la seguridad de la red está en riesgo, la política deberá permitir mayor flexibilidad a los administradores de los sistemas para corregir los problemas de seguridad. Se deben responder algunas preguntas a este respecto:

- ¿Puede el administrador del sistema monitorear o leer los archivos del usuario por alguna razón?
- ¿El administrador de la red tendrá el derecho de examinar el tráfico de la red o del servidor?
- ¿Que obligaciones tendrán los usuarios, administradores de sistemas y la organización para obtener acceso no autorizado a la información privada de otros individuos?

3.10. Manejo de información sensible.

Se debe determinar que tipo de información sensible puede ser almacenada en un sistema específico. Desde el punto de vista de seguridad, información muy sensible como planillas de pago, calificaciones, investigaciones, deben ser

restringidos a pocos servidores, por ende, a pocos administradores. Antes de considerar el conceder acceso a un usuario a un servicio en un servidor. Se debe considerar que información y servicios se ha proporcionado al usuario para entregar más acceso. Si el usuario no tiene necesidad de trabajar con información sensible, el usuario no deberá tener acceso a una cuenta en el sistema que contenga ese material.

La seguridad de un sistema involucra hardware, software y costos de administración adicional.

3.11. Plan de acción cuando es violada la política de seguridad.

Cada vez que es violada la política de seguridad, el sistema queda abierto a amenazas de seguridad. Si no ocurre un cambio en la seguridad de la red cuando es violada esta deberá ser modificada para remover aquellos elementos que no son seguros.

Independiente de que tipo de políticas de seguridad es implementada, existe una tendencia de algunos usuarios a violarlas. Los procedimientos de seguridad que se implementen deben minimizar las posibilidades de violación para ser indetectable. Al detectarse una violación a la política de seguridad, se debe clasificar si la violación ha ocurrido debido a la negligencia de un usuario, accidente o error, ignorancia sobre la actual política, o por ignorar deliberadamente la política. En el último caso, la violación puede ser ejecutada por solo un individuo.

3.12. Respuesta a la violación de la política.

Cuando ocurre una violación, la respuesta puede depender del usuario responsable de ella. El responsable puede ser local o externo, determinando el

tipo de respuesta que se puede generar ante la violación de seguridad. Estas pueden ser desde una advertencia o reprimenda verbal, una carta formal o presentando una acusación legal.

Se deben definir las acciones basando en el tipo de violación. Deben ser claramente definidas, basadas en la clase de usuario que ha violado la política de seguridad. Tanto un usuario local como externo, deben estar advertidos de las políticas de seguridad.

El documento de la política de seguridad debe incluir procedimientos para manejar cada incidente de violación. Una apropiada bitácora debe ser mantenida y ser revisada periódicamente para observar alguna tendencia, ajustando la política de seguridad en caso de cualquier amenaza.

3.13. Respuesta a la violación de las políticas por usuarios internos.

Se pueden generar violaciones a la política de seguridad en la cual un usuario local viola la política, generando las siguientes situaciones:

- Un usuario local viola un sitio local.
- Un usuario local viola un sitio remoto.

En el primer caso, se puede tener mayor control sobre el tipo de respuesta sobre la violación.

En el segundo caso, la situación es más compleja por el hecho de que otra organización es afectada, y cualquier respuesta que se tome debe ser discutida con la organización cuya seguridad ha sido violada.

3.14. Estrategia de respuesta.

Existen dos tipos de estrategias de respuesta a incidentes que involucren la seguridad:

- Proteger y Proceder
- Perseguir y Acusar

Si el administrador de la política de seguridad siente que la organización es vulnerable, elegirá la estrategia de Protección y Proceder. La meta de esta política es proteger inmediatamente la red y restaurarla a su estado normal para poder continuar con su utilización.

En el caso de no poder restaurar de inmediato, se debe aislar el segmento de red y apagar los sistemas con el objetivo de prevenir un mayor acceso no autorizado al sistema.

La segunda estrategia, Perseguir y Acusar, su principal objetivo es permitir al intruso seguir su acción, permitiendo vigilar sus acciones, sin que este se de cuenta de que esta siendo monitoreado. De esta forma se obtienen las pruebas necesarias para poder entablar una acusación legal. Esta última estrategia es la recomendada por las agencias de seguridad y la policía, ya que se obtienen los medios de prueba sin que el atacante se entere.

4. CAPÍTULO IV: Desarrollo del Proyecto

4.1. INACAP

INACAP La Serena es la institución seleccionada para poner a prueba la metodología creada.

4.1.1. Antecedentes Generales

”Con 40 años de experiencia, más de 50.000 alumnos, 25 sedes distribuidas de Arica a Punta Arenas, más una sede virtual, INACAP es hoy la institución de Educación Superior más grande del país. Nuestra amplia oferta de más de 130 programas de estudio técnicos y profesionales, hace que año a año numerosos jóvenes decidan dar aquí sus primeros pasos conducentes a un futuro profesional.”

INACAP La Serena ubicada en Francisco de Aguirre #389, cuenta con una infraestructura de 9200 mt^2 construidos, cuenta con laboratorios para cada carrera que sea necesario, con 6 laboratorios de computación y una biblioteca para el acceso a Internet y otros recursos para los alumnos, además cuenta con una red especial para el área de administrativos y profesores que se encuentra aislada de la red de los alumnos, cada red cuenta con las restricciones que cada caso lo amerite.

4.2. Situación actual

INACAP La Serena cuenta con tecnología de punta bajo un excelente diseño de red, la topología de esta institución se muestra en la figura 4, INACAP cumple con los estándares internacionales de diseño de redes y normas de seguridad internas, además posee políticas de seguridad para los usuarios, y aunque están

estipuladas como reglamento interno, no siempre son cumplidas por los mismos, se puede demostrar que en algunos casos las normas no son cumplidas por los usuarios, las políticas de seguridad son obligaciones de los usuarios administrativos no así a los alumnos, no existe reglamento que instruya al alumno a el uso de los equipos por esto mismo, el alumno asume que nada esta prohibido, salvo cuando el sistema en si da una advertencia de no poseer permisos para la ejecución de algún programa o la visita a algún sitio en Internet.

DIAGRAMA LINEAL SEDE LA SERENA

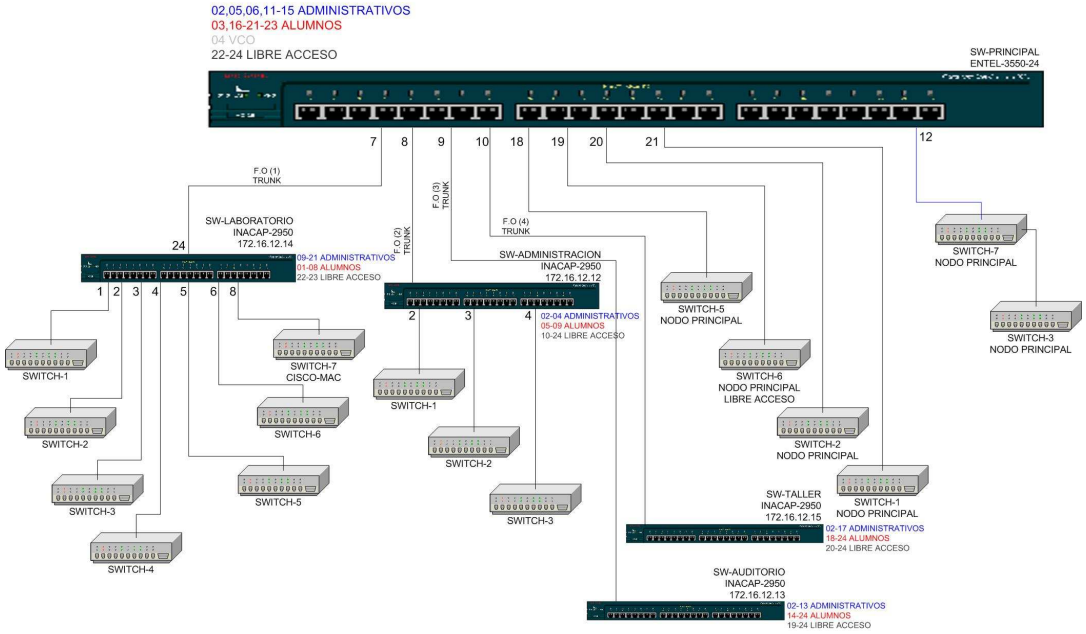

Figura 4: Esquema de topología INACAP La Serena

En la figura 4 se muestra el diagrama lineal de la red, en el Core esta un switch marca CISCO modelo 3550, este pertenece a ENTEL, que es el proveedor de servicios de esta sede y donde existe una clara asignación de puertos para cada segmento de red y pensando siempre en la escalabilidad de la red posee varios puertos libres, desde ahí caen enlaces a los distintos IDFs, estos son switch marca CISCO al igual que el Core pero un modelo menor, los cuales son capaces de soportar Vlan. A su vez desde estos switch salen conexiones a switch solo de acceso, no soportan Vlan.

4.3. Definición del Proyecto

La misión de este proyecto es, mediante una serie de pasos, que aplicados por gente conocedora del área de tecnologías de la información, se logre detectar las vulnerabilidades a la que está expuesta la red de datos. INACAP La Serena será la institución evaluada con la metodología de análisis de riesgos.

Luego de realizar el proceso de análisis de riesgos que plantea la metodología, se obtuvo datos que cuantificados permitieron crear los gráficos que permiten observar más fácilmente el grado de seguridad en que se encuentra la institución. Finalmente se entregarán una serie de sugerencias para mejorar los puntos vulnerables encontrados en el análisis.

4.3. Determinación de activos

Activo			Usuario	Posible ataque	Medidas de seguridad
Código	Nombre	Importancia			
1234-5	DC-Serena	5	ARL[1]	Duplicación de Dominio	Implementación de Proxy en los laboratorios

[1] Administrador de Red Local

4.4. Cuantificación de los resultados

Una vez obtenidas las respuestas de los cuestionarios, estas se evalúan y cuantifican, la serie de gráfico que se presentan a continuación muestran el estado de vulnerabilidad de INACAP La Serena.

En la tabla 9, se observa la tendencia general en las respuestas de los usuarios.

Pregunta	Respuesta
1	No
2	Sí
3	No
4	Sí
5	Sí
6	3 meses
7	No
8	No
9	No
10	No
11	No
12	No
13	No
14	No
15	No
16	Sí

Tabla 9: Resumen preguntas a usuarios

La primera impresión del estado de la red se presenta en el gráfico 1, al realizar un sondeo de preguntas sencillas, sin entrar en detalles específicos, sobre el funcionamiento de la red y las protecciones básicas que posee, se puede apreciar que la institución cuenta con herramientas para minimizar el nivel de vulnerabilidades, pero esto está lejos de un óptimo rendimiento de seguridad.

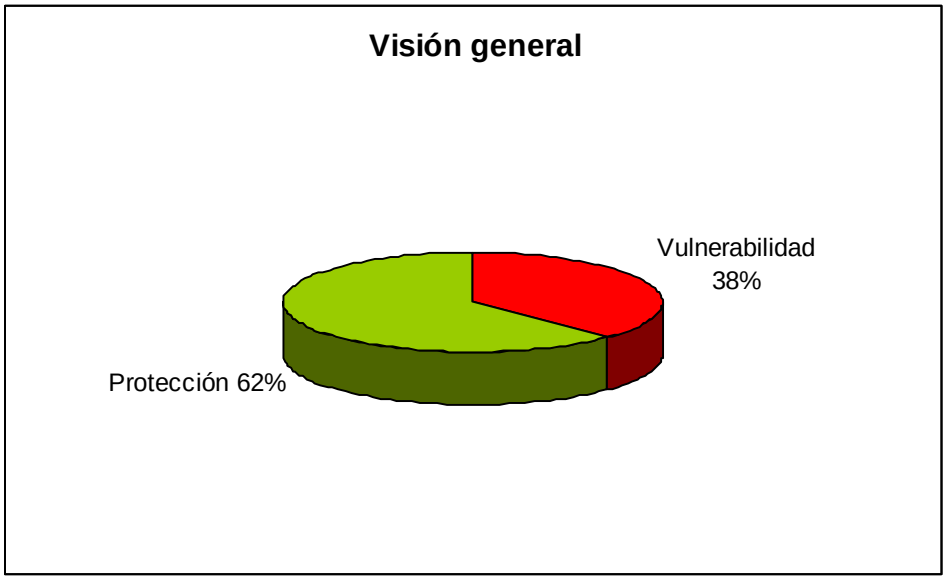

Gráfico 1: Observación básica del estado de la empresa

Los datos que generan el gráfico 2 se enfoca en el perímetro de la red, esto debido al tipo de preguntas realizadas, se aprecia la baja vulnerabilidad en comparación con las medidas de protección existentes, la institución cuenta con firewalls y segmentación de la red entre otras protecciones.

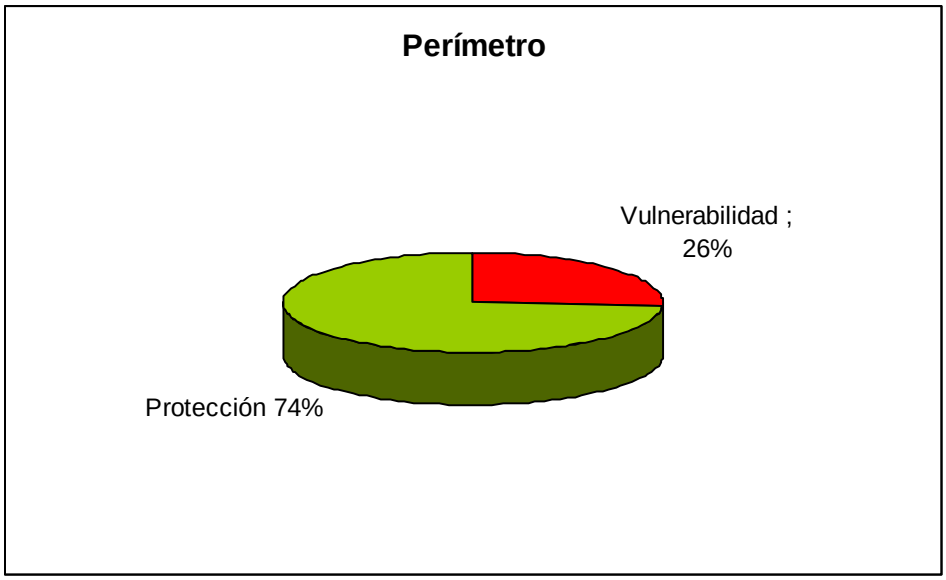

Gráfico 2: Observación del perímetro de la red de la empresa.

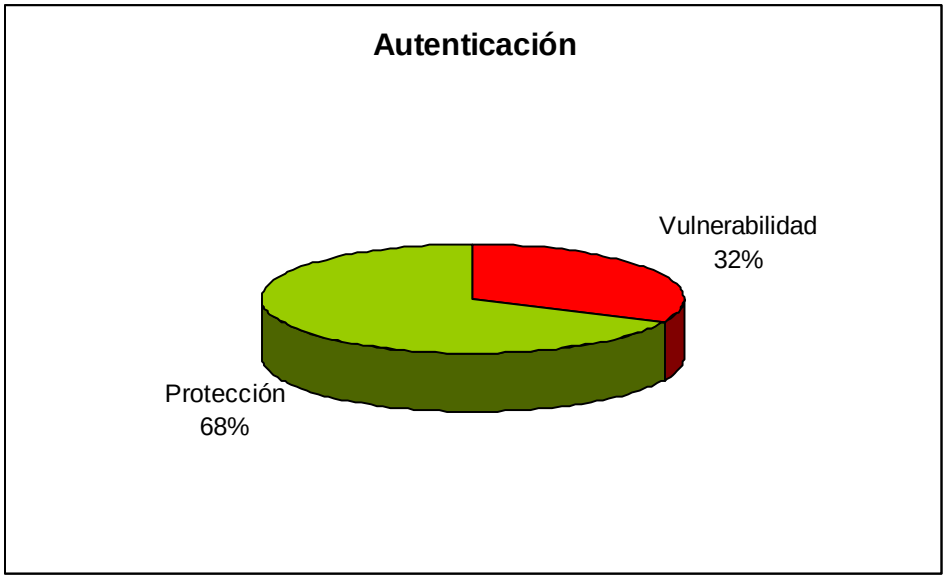

Gráfico 3: Evaluación de la autenticación en la institución.

Con las respuestas obtenidas por parte del administrador se podría decir que la institución cuenta con un buen sistema de autenticación para el acceso a sus sistemas aunque no es el óptimo, pero sin embargo, al observar las respuestas obtenidas por los usuarios se entiende que no se cumplen las normas de creación de contraseñas ni el control de estas, tan solo se realiza el cambio de estas cada tres meses. Otro punto sumamente importante es la falta de encriptación, lo que

deja abierta la información a cualquier persona que explore la red, ésta grave vulnerabilidad es demostrada en el caso práctica. Todos estos puntos modifican la evaluación de la tabla de autenticación, tal como se puede apreciar en el gráfico 3, existe un 55% de vulnerabilidad en lo que a autenticación se refiere.

Sin duda alguna, una de las mayores fortalezas de la institución es la forma de administración y control que posee sobre los sistemas, esto debido a que cuenta con un buen sistema de procedimientos, además de contar con personal interno capacitado para mantener la red, este resultado se expresa en el gráfico 4.

Gráfico 4: Gestión de administración y control.

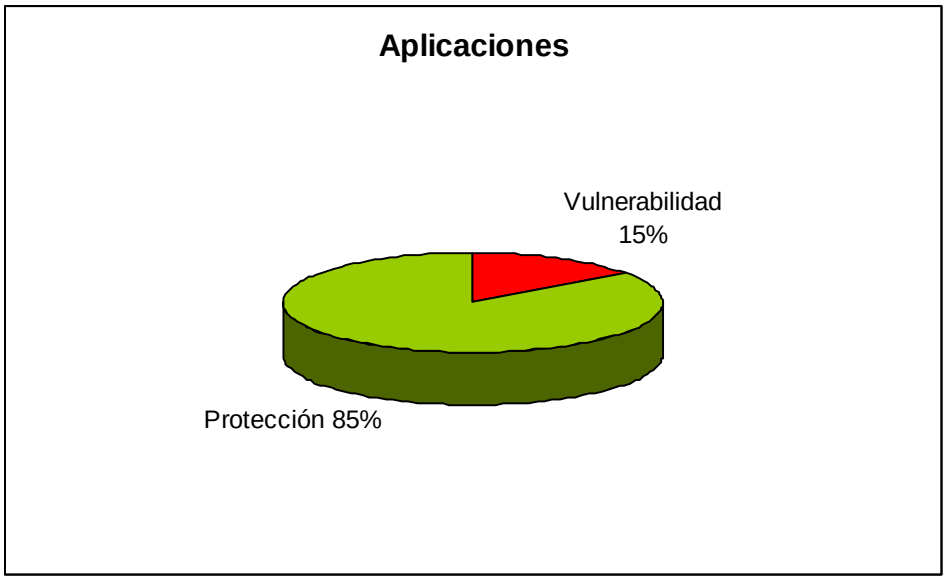

Gráfico 5: Evaluación de las aplicaciones.

Paso importante en toda red es determinar el tipo de aplicaciones que utiliza, el nivel que entrega la evaluación es positivo, tal como se muestra en el gráfico 5. De la misma forma como se ha apreciado en los gráficos anteriores, existe un bajo nivel de vulnerabilidades, lo mismo sucede en el entorno en que se desarrolla la institución, esto queda demostrado al observar el gráfico 6.

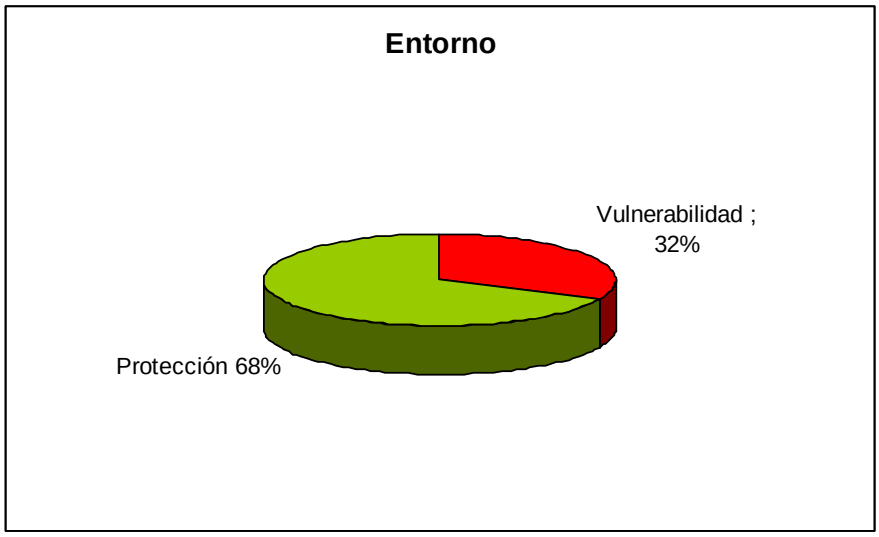

Gráfico 6: Evaluación del entorno.

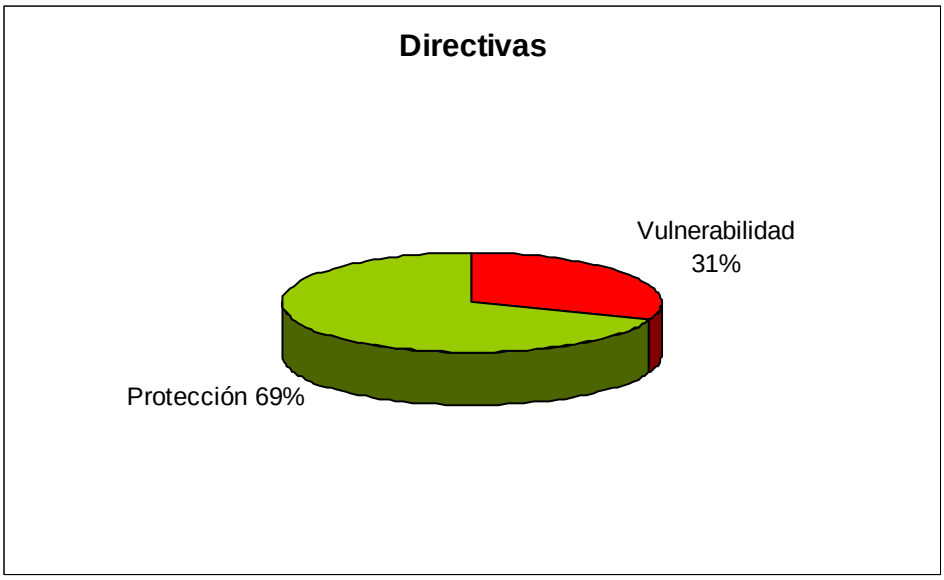

Gráfico 7: Evaluación de las directivas.

Al evaluar como se desempeña la institución en el marco de políticas y directivas se puede observar que esta realiza un buen desempeño en la asignación de los componentes. Sólo el no contar con pautas que indiquen protocolos y servicios permitidos en la red corporativa produce una vulnerabilidad de un 31%, esto se puede observar en el gráfico 7.

En el gráfico 8 se puede apreciar que gracias al nivel de actualizaciones que realiza la institución, se mantiene un bajo nivel de vulnerabilidades, nivel que es generado en laboratorios, los cuales no funcionan al 100% en conjunto con el resto de la infraestructura.

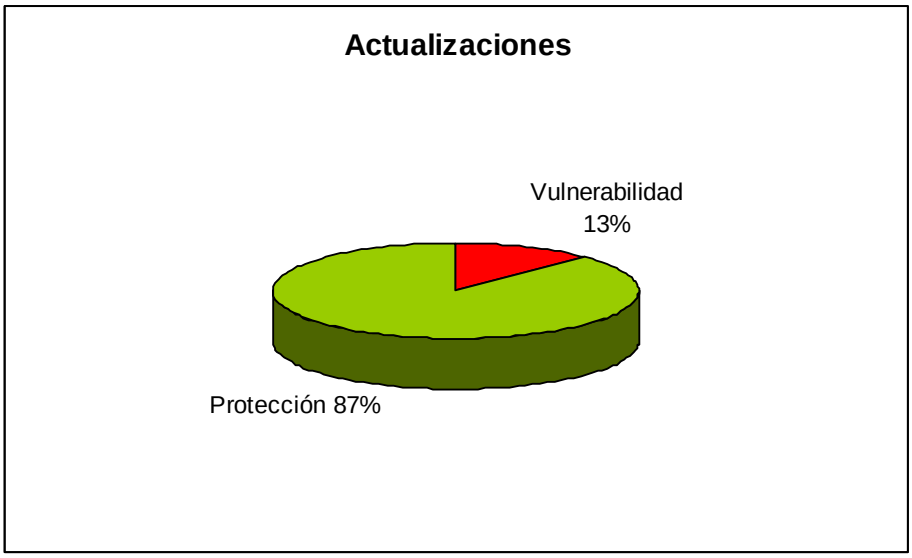

Gráfico 8: Evaluación de las actualizaciones.

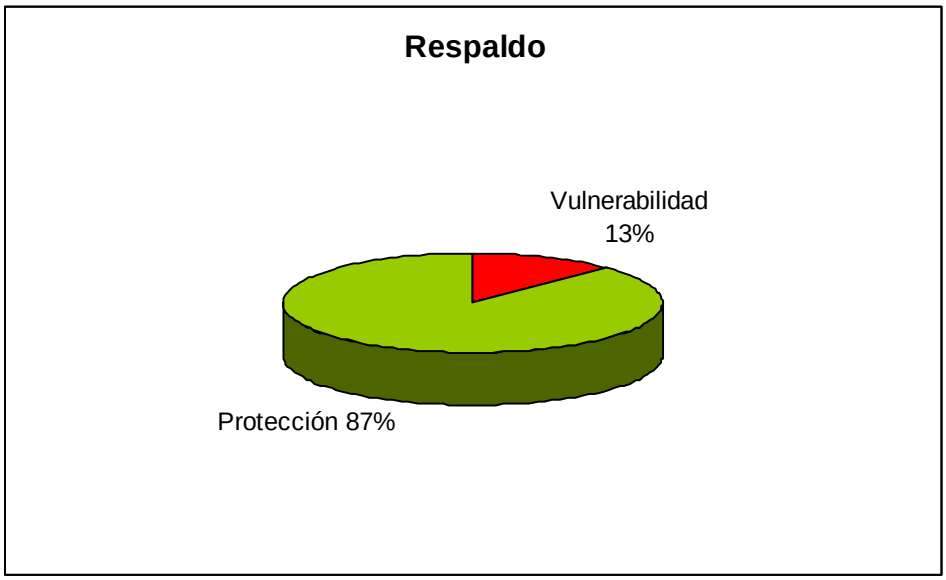

Gráfico 9: Evaluación del respaldo.

Para mantener una buena capacidad de respuesta, toda institución debe contar con un buen sistema de respaldo, así ocurre en INACAP La Serena, la cual envía sus datos a la sede central ubicada en Santiago para el posterior respaldo de

estos. La evaluación no es 100% aceptable, debido a fallas mínimas detectadas, las que generan un 13% de vulnerabilidad, observar gráfico 9.

Una forma de encontrar vulnerabilidades en toda institución es realizando evaluaciones a los sistemas, es aquí donde INACAP La Serena realiza una excelente gestión, logrando un bajo nivel de vulnerabilidad frente a posibles fallas o ataques, esto se puede apreciar en el gráfico 10.

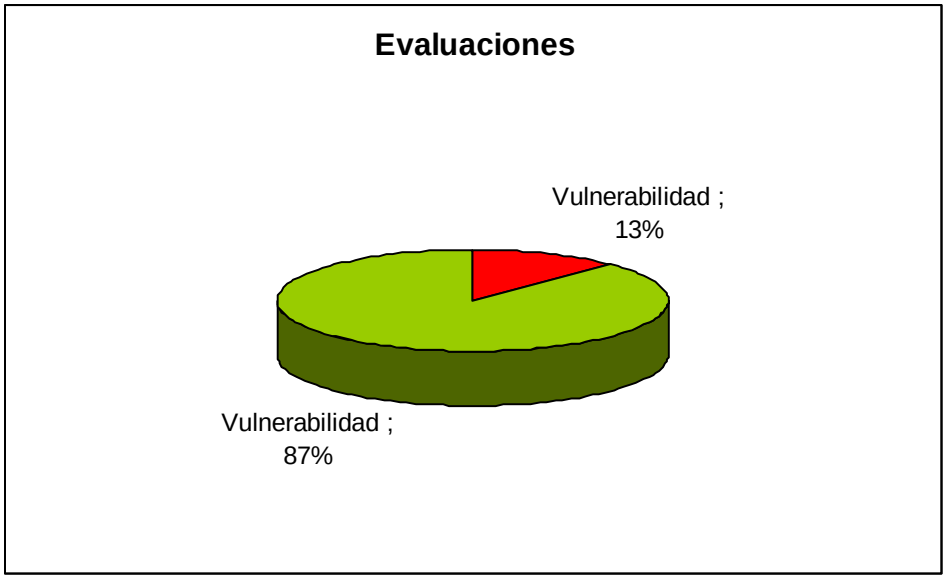

Gráfico 10: Evaluación de las evaluaciones que hace la organización.

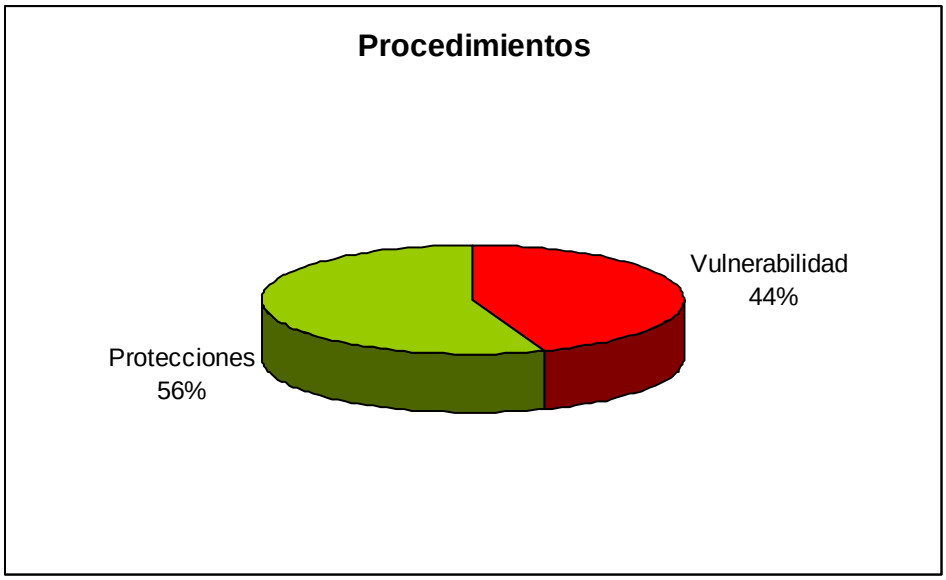

Gráfico 11: Evaluación de los procedimientos.

Los niveles que entregan mayor vulnerabilidad a la red de INACAP La Serena se encuentra en el desarrollo de procedimientos, esto se debe a la poca capacitación que se entrega a los usuarios administrativos en el área de seguridad informática, y la falla en la distribución de políticas de seguridad, este último dato se obtuvo gracias a las respuestas obtenidas de las preguntas a usuarios. Lo anterior proporciona un aumento de vulnerabilidades, tal como se aprecia en los gráficos 11 y 12.

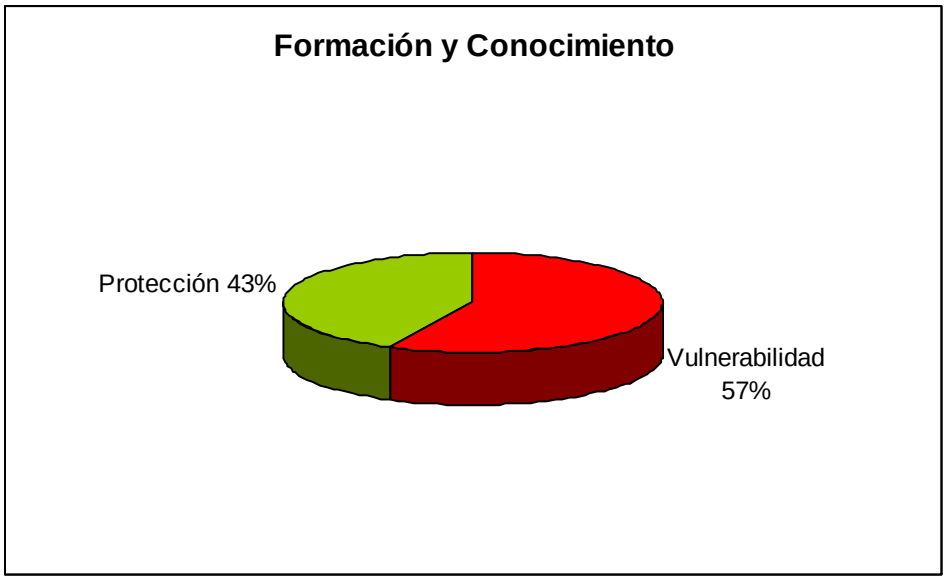

Gráfico 12: Evaluación de la formación y conocimiento.

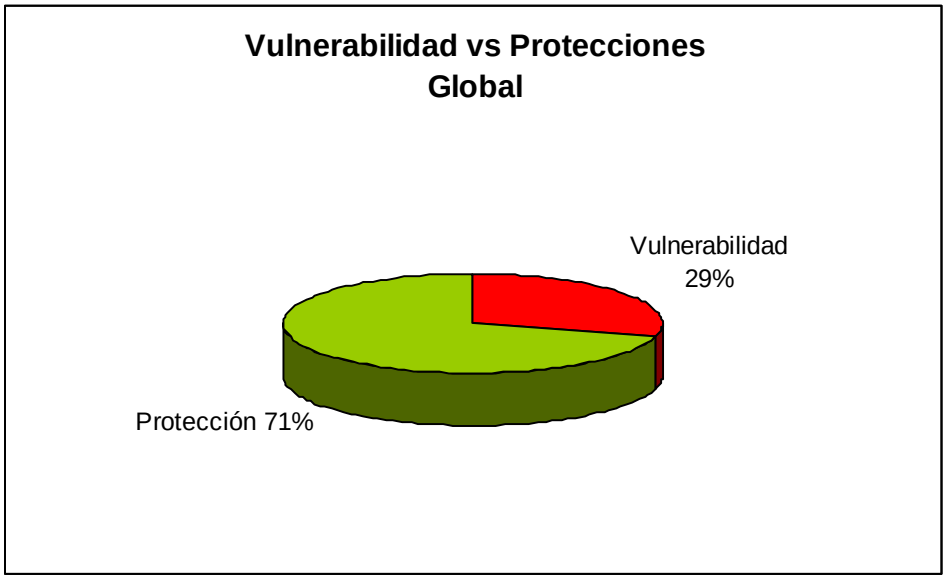

Gráfico 13: Resultado global

En el gráfico 13 se observa el conjunto de todos los resultados, podemos concluir que INACAP La Serena posee una baja vulnerabilidad, pero esto no implica que esté completamente asegurado, tal como se muestra en el gráfico, aún queda un 26% del total examinado que se debe asegurar. Además cabe señalar que si

alguna de estas vulnerabilidades es detectada por atacantes, el sistema se puede ver completamente comprometido.

Ya que se tienen los resultados del análisis se esta en posición de tomar decisiones con respecto al mejoramiento de la seguridad, por los tanto a continuación se muestran algunas políticas y sugerencias para disminuir las vulnerabilidades existentes.

Estas políticas deben quedar estipuladas como reglas internas de la organización, por los tanto al ser violadas deberán tener una sanción, esta última será determinada por los jefes de cada área o algún jefe superior.

4.5. Políticas para la organización

Sin duda alguna el estado de la red de INACAP La Serena se encuentra en un excelente estado de seguridad, pero sin embargo se deben realizar algunos cambios para el mejoramiento de esta, es por esto que se sugiere que se anexen las siguientes políticas a las ya existentes en la institución.

Defensa del perímetro

- El administrador de red debe instalar un firewall de software en los computadores.
- Los usuarios deben usar autentificación múltiple para las conexiones remotas (contraseña y tarjeta inteligente)
- El administrador de red debe activar la función WEP en las conexiones inalámbricas.
- El administrador de red debe activar la restricción por MAC en los puntos de red administrativos.

- El administrador de red debe conectar el punto de acceso a la red inalámbrica fuera del firewall o en un segmento separado de la red cableada.

Autenticación

- El administrador de red debe utilizar el algoritmo 3DES para la transmisión y almacenamiento de los datos en las aplicaciones criticas de la organización

Administración y control

- El administrador de red debe instalar software de firewall en cada Terminal de trabajo y los equipos portátiles de los empleados.
- El administrador de red debe utilizar un software de encriptación de disco en los computadores de la organización.
- El administrador de red debe instalar un software de administración y control remoto en los computadores de la organización.
- Proteger los equipos con cables de seguridad.

Entorno

- La gestión del entorno debe ser hecha por el administrador de red y no por subcontratistas.
- EL administrador de red debe utilizar dispositivos de red para la administración segura de dispositivos de entorno.

Copias de seguridad y recuperación

- El administrador de red debe revisar semanalmente los registros de eventos que produzcan los host o dispositivos de red.

Formación y conocimiento

- El administrador de red debe dar una capacitación para los usuarios con respecto a la seguridad en la red, se deben tocar los temas:
    - Definición de la seguridad
    - Deberes que debe cumplir para una seguridad integral
    - La importancia de las políticas de la organización
    - Directivas y controles de seguridad de la empresa
    - Informes sobre actividades sospechosas
    - Confidencialidad
    - Seguridad del correo electrónico, incluyendo Spam y gestión de adjuntos
    - Seguridad de Internet, incluyendo navegación por la Web y descargas
    - Seguridad informática, incluyendo el uso de cortafuegos particulares y cifrado

- La capacitación debe ser semestralmente
- El administrador de red debe informar al usuario sobre:

    - Seguridad de las operaciones
    - Seguridad de la infraestructura
    - Seguridad de las aplicaciones
    - Preparación para incidentes y reacción

Políticas para el usuario final:

- Cada usuario tiene un equipo computacional asociado, es responsabilidad del usuario realizar un buen uso y cuidado de este.
- Las fallas en los equipos o en la red deben reportarse inmediatamente.
- La pérdida o robo de algún equipo o datos debe reportarse

inmediatamente.

- La divulgación de cualquier información respecto a la organización deberá tener una sanción.
- Cuidar su contraseña, manteniéndola en secreto y evitar que sea vista por otros en forma inadvertida[1].
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y debe ser debidamente aprobada por el ARL.
- Permitir o facilitar el uso de los sistemas a personas no autorizadas queda estrictamente prohibido.
- Debe respetarse y no modificar las configuraciones de hardware y software, además de no instalar nuevos programas sin el consentimiento del administrador de red.
- Queda prohibido reubicar los equipos sin previa autorización del administrador de red.
- No contestar los mensajes SPAM[2], ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes[3]), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.
- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.
- Borre constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.
- No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de

[1] Evitar el uso de etiquetas adheridas en equipos computacionales en los que se señalen contraseñas, así como guardar bajo llave agendas en las que se guarde este tipo de información.

[2] Correo de remitente desconocido.

[3] Tipo de virus.

virus.

- No debe abrir el equipo, ni cambiar el hardware ni el software.

4.6. Estudio Legal

Para aplicar la metodología a empresas se debe ofrecer el servicio como una empresa independiente, lo que conlleva a crear una sociedad, para la formación de esta los pasos a seguir son:

- Determinar la mejor opción para la creación de la sociedad, en este caso se opto por la sociedad limitada, así la responsabilidad de cada socio se limita al capital aportado.
- La construcción de la sociedad ante un abogado (estructura de la constitución de la sociedad).
- Declarar inicio de actividades y obtención de RUT ante el servicio de impuestos internos (SII), llenando el formulario 4415.
- La publicación de extracto de la sociedad en el diario oficial.
- Timbraje de libros, boletas y facturas.

Según el análisis realizado, la ley de delitos informáticos en Chile es bastante pobre, por ello las organizaciones crean sus propias Políticas internas y son validadas en el reglamento interno de la organización, estipulando las buenas conductas y las sanciones en caso que las normas sean violadas

4.7. Estudio Financiero

La herramienta de detección de vulnerabilidades tiene un coste de estudio de $552.510, este valor fue calculado por 15 días de trabajo por dos meses y según la unidad de fomento del mes de octubre que equivale a $18.417.

La herramienta necesita de dos empleados, con un sueldo de $210.000.- mensuales por persona, su función en la empresa será la misma, se contempla acudir a las empresas, entrevistar empleados, utilizar la herramienta y aplicarle mejoras, crear políticas de seguridad, mantener la página Web de la empresa y manejar la parte contable de la empresa.

Existen distintos valores para el servicio, ya que está determinado por dos variables, estas son el tamaño de la empresa y la cantidad de tiempo requerido para desarrollarlo. El tamaño de la empresa se muestra en la tabla 10 y los precios se observan en la tabla 11.

Tamaño	Q equipos
Pequeña	1 a 10
Mediana	11 a 50
Grande	51 a 200

Tabla 10: Clasificación según tamaño de la empresa

Q Semanas	Pequeña	Mediana	Grande
1	150000	170000	190000
2	280000	320000	360000
3	410000	470000	530000
4	540000	620000	700000
5	670000	770000	870000

Tabla 11: Tabla de precios.

El aplicar la metodología en INACAP La Serena, tendrá un costo de $700000, ya que califica como una empresa grande y el tiempo involucrado en el proyecto es de un mes.

Mercado competidor

Para obtener información de cómo se desarrolla el servicio de seguridad en redes datos en el mercado se debió observar el trabajo que realizan las empresas que ofrecen auditorias y asesorías de seguridad en redes de datos o que entregan un servicio similar.

Se realizó una búsqueda de las empresas Chilenas pertenecientes al rubro, el número de estas es bastante reducido, pudiendo mostrarse la totalidad de ellas:

- I-TECHNOLOGY
- LINTEX-LINUX.
- INFOCORP
- NETSECURY
- ETEK ELECTRONICS CORPORATION CHILE LTDA.
- NOVARED

No existen empresas de este rubro en la región, todas las empresas anteriormente nombradas tienen su ubicación en Santiago, sin sucursales en regiones, pero los clientes de estas se encuentran a lo largo del país, entre las cuales encontramos: Banco Estado, BCI, SII, Ministerio Secretaría General de la República, Copec, ENTEL, Shell, AFP Cuprum, Chile.com, Ejercito de Chile, Grupo Antalis, Cementos Bio Bio, Soprole, Comisión Chilena del Cobre, Grupo Madeco y Fonasa. Las empresas locales como Supermercados DECA, tiendas la Elegante y Corporación Municipal Gabriel González Videla no recurren a estos servicios, solo acceden a trabajos de configuraciones realizados por independientes (ingenieros informáticos).

Otras empresas como las que a continuación se nombran, entregan solo una parte de los sistemas de seguridad, la que está asociada con el producto o servicio que entregan, como por ejemplo, seguridad de sitios Web, seguridad en servidores, software de seguridad (antivirus), etc.

- VIALCOM
- DGR INGENIEROS
- INFOSEG S.A.
- MENDOCOM LTDA.
- DINAMIC.COM

Las principales formas que utilizan para llegar al consumidor son mediante avisos publicitarios en Internet, revistas, diarios, además de la participación en eventos, seminarios y la presentación de proyectos a las empresas cuando estas llaman a licitación.

Algunos de estos competidores son sucursales de empresas extranjeras y otras están asociados a proveedores extrajeras de gran renombre, tal como lo son Microsoft, RSA, Trend Micro y Symantec, lo que les entrega un buen respaldo.

Análisis FODA

Este análisis es del proyecto y sus creadores funcionando como empresa, se deben analizar las opciones de vida que tiene y que podría llegar a tener:

- Fortalezas

Contar con una metodología de trabajo propia.
Empresarios jóvenes, con deseos de realizar bien el trabajo.
Contar con personal calificado y especializado para realizar el trabajo.

- Oportunidades

La ausencia de empresas del mismo tipo en la zona.
El amplio campo de trabajo, debido a que la mayoría de las empresas utiliza redes de datos.

- Debilidades

Empresa nueva, sin antecedentes.
Poca importancia de las empresas al tema de seguridad informática, punto en el que Networker-Solutions enfocará su campaña publicitaria, para dar a conocer la importancia de la seguridad.

- Amenazas

Empresas que datan desde 1998 ubicadas en Santiago.
Empresas extranjeras que venden software de seguridad vía Internet.

El aplicar la metodología en INACAP La Serena, tendrá un costo de $700000, ya que califica como una empresa grande y el tiempo involucrado en el proyecto es de un mes.

4.8. Pruebas de Laboratorio

La prueba de laboratorio se basó en la captura de trafico de la red de Inacap y así poner a prueba la reacción que esta pudiera tener frente a este tipo de ataque, se eligió este ataque que es pasivo ya que es el mas común y el menos detectado, el objetivo era capturar todo tipo de información valiosa, como las contraseñas de los usuarios, la primera captura se realizó con un equipo portátil y personal de un alumno, este fue conectado a un punto de red administrativo que no estaba resguardado como se debería, la obtención de dirección ip no fue ningún problema, el inconveniente para esta prueba o mas bien la medida de seguridad que se presentó fue que al intentar acceder a Internet el sistema solicitaba un usuario y contraseña, como la prueba no dependía de la conexión a Internet se pudo continuar con ella, se comenzó determinando que equipos son los importantes, es decir, por el cual haya un tráfico significativo, o sea el Proxy de la red administrativa, por este equipo pasan todas las conexiones, luego se espera hasta capturar la información necesaria, el tiempo que duro la prueba fue 25 minutos, bastó solo este tiempo para lograr el objetivo. En la figura 5 se muestra la captura de una contraseña perteneciente a un docente, así como se puede obtener una password de un docente también se pueden obtener de un administrativo con un cargo alto, que pueda manejar información sensible o confidencial de la organización.

Usuario	Contraseña	Dirección Web

Figura 5: Captura de password de un docente en red administrativa.

La prueba también debía probar la seguridad del otro segmento de la red, red alumnos, el acceso a esta no tiene ningún problema, la prueba se llevó a cabo de la misma forma que para el segmento anterior, al contrario del anterior acá solo

bastaron 10 minutos para lograr el objetivo. La figura 6 muestra la captura de una contraseña de un alumno, así se aprecia que ningún dato en la red esta encriptado. La captura se realizo con un software Sniffer (Cain y Abel), es un software que puede ser detectado como una anomalía en la red, pero aún así no fue detectado por el IDS.

Usuario	Contraseña	Dirección Web

Figura 6: Captura de password en red alumnos

CONCLUSIÓN

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas tecnologías y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa. Pero no se encuentra documento alguno en el que se explique el qué preguntar o el qué analizar al desarrollar un análisis.

Para poder crear una metodología no solo se deben agregar cosas, sino que es necesario entregar un sentido lógico al procedimiento, para ello se debe conocer en primer lugar la existencia de metodologías o formas relacionadas con lo que se quiere hacer, también se deben conocer más a fondo los fundamentos de la seguridad y entenderlos. La seguridad en la información no es posible sin la cooperación del usuario. Se puede tener la mejor tecnología para protegerlos y aún así, sufrir una ruptura de seguridad.

Se pudo apreciar que con el hecho de utilizar un conjunto de preguntas y procedimientos se logra concretar una excelente imagen de las vulnerabilidades a las que es susceptible la red.

Al desarrollar las herramientas del análisis se logró evidenciar que se cuenta con varias herramientas, como por ejemplo, la utilización de ingeniería social, esta es una técnica bastante buena ya que no es tan rígida como llenar un cuestionario de preguntas, aquí las personas responden con muchas mas franqueza y se sienten cómodas conversando y expresándose, esto se pudo comprobar con los usuarios entrevistados. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas. En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Finalmente debe quedar claro que la Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos. Seguridad es un proceso NO un producto.

Elaborar este proyecto proporcionó mucha experiencia en el ámbito profesional, ya que en el mundo laboral es apreciado el profesional que posee conocimientos en el área de seguridad informática, puesto que las organizaciones se están dando cuenta cada vez más de la importancia de contar con un sistema con bajas vulnerabilidades, y los costos que esto implica.

En el ámbito personal las ganancias son invaluables, el trabajo en equipo, las relaciones con las personas, el desarrollo de la personalidad, al enfrentar gente que no conocemos.

BIBLIOGRAFÍA

Tesis

Título: Diseño e implementación de conectividad entre sucursales con tecnología ADSL bajo plataforma Fedora Core 2 para Ópticas Queirolo.
Autor: Pablo Arias Díaz, Mauricio Valdebenito Valdivia.
Año: 2005

Sítios Web

http://es.wikipedia.org/wiki/Información 06/09/2006
www.informatica.cl 14/09/2006
http://www.segu-info.com.ar/logica/seguridadlogica.htm 16/09/2006
http://www.seguridadenlared.org/es/index5esp.html 21/10/2006

GLOSARIO DE TERMINOS

3DES: Triple DES, método de encriptacion de datos.

Cookies: cadena de texto que se instala en el disco duro.

Core: núcleo de la red.

DMZ: zona desmilitarizada es un área de una red de computadoras que está entre la red de computadoras interior de una organización y una red de computadoras exterior.

Firewalls: equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red.

FTP: protocolo de transferência de archivos.

Hub: concentrador para las conexiones de red.

IDS: sistema de detección de intrusos.

MAC: dirección física de la tarjeta de red.

Router: enrutador de redes.

Switch: concentrador para las conexiones de red.

TCP: protocolo de control de transmisión.

Vlan: red Lan virtual.

VPN: red privada virtual.

Web: red a nivel mundial.

WEP: sistema de cifrado em redes inalambricas.

ANEXOS

Anexo I: Información básica de la empresa

1. ¿Tiene conexión permanente a Internet?

- o Sí
- o No

2. ¿Su empresa permite acceso ilimitado a sus empleados para navegar en Internet?

- o Sí
- o No
- o No lo sé

3. ¿Su empresa posee aplicaciones para los clientes?

- o Sí
- o No

4. ¿Los usuarios internos y externos usan los recursos del mismo segmento de red?

- o Sí
- o No
- o No lo sé

5. ¿Los usuarios externos se conectan directamente a los sistemas internos de la aplicación para acceder a los datos, actualizar los registros o gestionar de cualquier otra forma la información?

- o Sí
- o No
- o No lo sé

6. ¿Su empresa permite que los empleados accedan a la red corporativa?

- o Sí
- o No
- o No lo sé

7. ¿Permite que sus empleados utilicen sistemas que no sean de producción, como por ejemplo: servidores Web personales o equipos que actúen como hosts de proyectos personales?

- o Sí
- o No
- o No lo sé

8. Aparte de los medios de respaldo, ¿su empresa permite a los empleados procesar información corporativa fuera de las instalaciones?

- o Sí
- o No
- o No lo sé

9. ¿Puede operar la empresa si la red de datos no está disponible?

- o Sí
- o No
- o No lo sé

10. ¿Su empresa comparte oficina con otras entidades?

- o Sí
- o No

11. ¿Subcontrata su empresa el mantenimiento o la propiedad de alguna parte de su infraestructura?

- o Sí
- o No

Subcontratar la implantación de la infraestructura conlleva un mayor riesgo para el entrono debido a la dependencia generada en recursos externos.

12. ¿Tienes su empresa planificaciones para la selección y utilización de componentes de nuevas tecnologías?

- o Sí
- o No
- o No lo sé

La falla de planificación para la utilización de las tecnologías aumenta la posibilidad de tiempos de inactividad y de ataques.

13. ¿Cree que su empresa participa en la adopción rápida de las nuevas tecnologías?

- o Sí
- o No
- o No lo sé

14. ¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?

- o Sí
- o No

La empresa en rápido auge también experimenta cambios rápidos en su entorno. Estos cambios rápidos y continuos podrían resultar en un entorno inestable.

15. ¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo o equipos portátiles datos corporativos o datos confidenciales de los clientes?

- o Sí

- o No
- o No lo sé

Permitir la descarga de información confidencial en estaciones de trabajo portátiles aumenta el riesgo de robo o de pérdida de datos.

16. ¿Limita su empresa el acceso a la información en función de los roles de los usuarios?

- o Sí
- o No
- o No lo sé

El acceso a los datos y a las aplicaciones confidenciales debe limitarse conforme a los privilegios de las cuentas individuales. Es importante dispones de mecanismos para el cumplimiento de estas limitaciones a fin de evitar traspasos de información no autorizados.

17. ¿Implanta su empresa nuevos servicios o aplicaciones antes de evaluar los posibles riesgos para la seguridad?

- o Sí
- o No
- o No lo sé

Los elementos de una nueva instalación deben analizarse y probarse antes de utilizarse en un entorno de producción para comprobar que no son vulnerables.

18. ¿Cambia su empresa periódicamente las credenciales de las cuentas con privilegios?

- o Sí
- o No
- o No lo sé

Para reducir el impacto del ataque por fuerza bruta sobre la autenticación de cuentas con privilegios, las contraseñas de tales cuentas deben cambiarse regularmente.

19. ¿Cambia su empresa las credenciales de las cuentas con privilegios cuando el personal deja de trabajar en la empresa?

- o Sí
- o No
- o No lo sé

Para reducir los riesgos empresariales, las contraseñas de las cuentas con privilegios deben cambiarse de forma inmediata tras el cese de un empleado con acceso a esas cuentas.

Pregunta	Vulnerabilidad	Escala	Respuesta
1	-	0-1	Sí
2	-	0-1	Sí - No lo sé
3	-	0-1	Sí
4	-	0-2	Sí - No lo sé
5	-	0-1	Sí - No lo sé
6	-	0-1	Sí - No lo sé
7	-	0-2	Sí - No lo sé
8	-	0-2	Sí - No lo sé
9	-	0-3	No- No lo sé
10	-	0-2	Sí
11	-	0-1	Sí
12	-	0-1	No- No lo sé
13	-	0-1	No- No lo sé
14	-	0-1	Sí- No lo sé
15	-	0-2	Sí
16	-	0-2	Sí- No lo sé
17	-	0-3	Sí- No lo sé
18	-	0-2	No- No lo sé
19	-	0-2	No- No lo sé
20	-	0-2	No- No lo sé

Protección	Escala	Respuesta
-	0-1	No
-	0-1	No
-	0-1	No
-	0-2	No
-	0-1	No
-	0-1	No
-	0-2	No
-	0-2	No
-	0-2	Sí
-	0-1	No
-	0-1	No
-	0-1	Sí
-	0-1	Sí
-	0-1	No
-	0-1	No
-	0-2	No
-	0-3	No
-	0-2	Sí
-	0-2	Sí
-	0-2	Sí

Valores de evaluación de la sección.

Anexo II: Defensa del perímetro

2. ¿Su empresa utiliza firewalls u otros controles de acceso en los perímetros de la red para proteger sus recursos?

- o Sí
- o No
- o No lo sé

Los firewalls son un elemento importante para proteger las redes contra ataques. Es por ello que los firewalls, u otros controles de acceso a nivel de red, son imprescindibles para la seguridad de la empresa

En caso de responder Sí:

2.1. ¿Su empresa aplica estos controles en todas las oficinas?

- o Sí
- o No
- o No lo sé

2.2. ¿Su empresa usa una red DMZ para separar redes internas y externas de los servicios albergados?

- o Sí
- o No
- o No lo sé

Una red DMZ es un host o una red pequeña insertado como una zona neutra entre la red privada de la empresa y la red publica, impide que los usuarios externos accedan directamente a un servidor con datos de la empresa.

3. ¿Su empresa usa firewall en los host para proteger los servidores?

- o Sí
- o No
- o No lo sé

El firewall personal implementado en el host proporciona otra capa de defensa frente a las amenazas al extender la funcionalidad del firewall hasta las computadoras de escritorios, equipos portátiles o servidores.

4. ¿Su empresa usa hardware o software de detección de intrusos para identificar los ataques a la seguridad?

- o Sí
- o No
- o No lo sé

Conocido como IDS, monitorea y analiza en forma activa el trafico de la red para determinar si se ha intentado un ataque.

5. ¿Se utiliza antivirus acorde con la cantidad de empleados en la empresa?

- o Sí
- o No
- o No lo sé

Es de vital importancia contar un antivirus para proteger la red contra virus que puedan causar la pérdida de datos o tiempos de inactividad, existen distintos tipos de antivirus tanto para red corporativa así como para media y pequeña empresa.

En caso de responder Sí:

5.1. Seleccione los sistemas que lo usan:

- o Mail Server
- o Host de perímetro (gateway, Proxy,etc)

- o Computador de escritorio
- o Servidores

6. ¿Se puede acceder a la empresa en forma remota?

- o Sí
- o No
- o No lo sé

Las funciones de conexiones remotas también presentan un frente de ataque.

En caso de responder Sí:

6.1. Seleccione quien se puede conectar a la red en forma remota

- o empleados
- o contratistas
- o terceros como fabricantes, socios o clientes

6.2. ¿Se utiliza la tecnología VPN para las conexiones remotas?

- o Sí
- o No
- o No lo sé

Una VPN utiliza una infraestructura pública de telecomunicaciones, como Internet, para proporcionar acceso seguro a la red de la empresa a usuarios y oficinas remotas. La autenticación de factores múltiples requiere dos o mas de las categorías siguientes: algo que sepa el usuario (ejemplo: contraseña), y algo que sea propio del usuario (ejemplo: huella digital, retina).

En caso de responder Sí:

6.2.1. ¿Puede La VPN limitar la conectividad a una red aislada en cuarentena hasta que el cliente haya efectuado todas las comprobaciones necesarias?

- o Sí
- o No

7. ¿Se utiliza autenticación de factores múltiples (vales o tarjetas inteligentes) para usuarios remotos?

- o Sí
- o No
- o No lo sé

La autenticación de factores múltiples requiere dos o más de las categorías siguientes: algo que sepa el usuario (contraseña), algo que tenga el usuario (vales, tarjetas inteligentes), algo que sea propio del usuario (huella digital, retina).

8. ¿La red tiene más de un segmento?

- o Sí
- o No
- o No lo sé

Una red segmentada le ofrece recursos corporativos y a nivel de cliente separados para evitar la pérdida de información. En caso de un ataque, la segmentación limita el daño posible.

En caso de responder Sí:

8.1. ¿La red se segmenta para separar los servicios de usuarios externos y servicios extranet de los recursos corporativos?

- o Sí
- o No

En caso de responder Sí:

8.1.1. ¿Su empresa agrupa los hosts en segmentos de redes según los roles o servicios similares?

- o Sí
- o No

8.1.2. ¿Su empresa agrupa los hosts en segmentos de redes para ofrecer únicamente los servicios necesarios a los usuarios que se conectan?

- o Sí
- o No

8.1.3. ¿Se ha creado y documentado un plan para regular la asignación de direcciones TCP/IP a los sistemas según lo segmentos?

- o Sí
- o No

Un buen plan de asignación de direcciones asegura que la red este debidamente segmentada.

9. ¿La red dispone de conexión inalámbrica?

- o Sí
- o No

Las redes inalámbricas, si se utilizan adecuadamente pueden ayudar a aumentar la productividad. Sin embargo, debido a los puntos débiles que todavía presentan una vez implantadas, pueden ser un foco de entrada propicio para los ataques contra la red.

En caso de responder Sí:

9.1. ¿Cuáles son los siguientes controles que utiliza?

- Cambiar el nombre de la red predeterminado (conocido también como Identificador del conjunto de servicios o SSID) de los puntos de acceso.
- Desactivar la difusión del SSID.
- Activar Wired Equivalent Privacy (WEP).
- Activar restricciones de direcciones MAC (filtrado pos MAC).
- Conectar el punto de acceso a la red fuera del firewall o en un segmento separado de la red cableada.

Pregunta	Vulnerabilidad	Escala	Respuesta		Protección	Escala	Respuesta
1	-	0 o 2	No - No lo sé		-	0 a 4	Sí
2	-	0-2	No - No lo sé		-	0-2	Sí
3	-	0-2	No - No lo sé		-	0-2	Sí
4	-	0-2	No - No lo sé		-	0 a 3	Sí
5	-	0 a 4	Sí- No lo sé		-	0-1	No
6	-	0-2	No - No lo sé		-	0-2	Sí
7	-	0-3	No - No lo sé		-	0 a 5	Sí
8	-	0-1	Sí- No lo sé		-	0-1	No
9	-	0-2	Sí- No lo sé		-	0 a 4	No

Valores de evaluación de la sección.

Anexo III: Autenticación

1. ¿Hay controles para hacer cumplir las políticas de seguridad por contraseña en todas las cuentas?

- o Sí
- o No
- o No lo sé

Sin los mecanismos adecuados para aplicarlas, las normas para que las contraseñas cumplan con los requerimientos generalmente se ignoran. La mayoría de los sistemas de autenticación permite la aplicación automatizada de normas referente a la longitud, la complejidad y el vencimiento de las contraseñas, entre otros.

En caso de responder Sí:

1.1. Seleccione las cuentas para las cuales existen controles que hagan cumplir las políticas de seguridad por contraseña.

- o Administrador
- o Usuario
- o Acceso remoto

Las políticas para las contraseñas deben cumplirse en todas las cuentas, no solo en las de los administradores.

1.2. Indique cuál es la opción de autenticación para el acceso administrativo a cargo de los dispositivos y hosts.

- o Autenticación en factores múltiples
- o Ninguno
- o Contraseña simple
- o Contraseña compleja

Las contraseñas simples no tienen restricciones en cuanto a combinación de caracteres y longitud necesaria, por lo que no se deben usar. Sin embargo, las contraseñas complejas requieren una longitud mínima y el uso de caracteres alfanuméricos y especiales. Además de una contraseña, la autenticación de factores múltiples requiere otros elementos de autenticación como por ejemplo: tarjeta inteligente.

1.3. Indique cuál es la opción de autenticación para los accesos a la red y los hosts internos de los usuarios internos:

- o Autenticación en factores múltiples
- o Ninguno
- o Contraseña simple
- o Contraseña compleja

1.4. Indique cual es la opción de autenticación para el acceso remoto de los usuarios:

- o Autenticación en factores múltiples
- o Ninguno
- o Contraseña simple
- o Contraseña compleja

1.5. ¿El bloqueo de cuentas está activado para impedir el acceso a las cuentas tras una serie de intentos de registro fallido?

- o Sí
- o No

Para proteger frente a ataques de fuerza bruta, las cuentas deben configurarse para que no permitan el acceso después de una cantidad determinada de intentos fallidos.

2. ¿Hay controles para hacer cumplir las políticas de contraseña para las aplicaciones clave?

- o Sí
- o No

2.1. Seleccione los controles de contraseña implementados en las aplicaciones clave:

- o Contraseñas complejas.
- o Vencimiento de contraseñas.
- o Bloqueo de cuentas.

2.2. De la siguiente lista, seleccione el método de autenticación mas común usado en las aplicaciones clave:

- o Autenticación de factores múltiples
- o Contraseña simple
- o Contraseña compleja
- o Ninguno

Las contraseñas simples no tienen restricciones en cuanto a combinación de caracteres y longitud necesaria, por lo que no se deben usar. Sin embargo, las contraseñas complejas requieren una longitud mínima y el uso de caracteres alfanuméricos y especiales. Además de una contraseña, la autenticación de factores múltiples requiere otros elementos de autenticación como por ejemplo, tarjeta inteligente.

3. ¿Las aplicaciones clave del ambiente cuentan con mecanismos para limitar el acceso a las funciones e información critica?

- o Sí
- o No
- o No lo sé

El acceso a aplicaciones y datos sensibles debe limitarse conforme a los privilegios de cada cuenta. Es importante disponer de mecanismos para el cumplimiento de estas limitaciones a fin de evitar traspasos de información no autorizados.

4. ¿Las aplicaciones clave guardan mensajes en archivos con la bitácora del uso para análisis y auditoria?

- o Sí
- o No
- o No lo sé

Los archivos con la bitácora del uso son necesarios para auditar actividades sospechosas y anormales.

En caso de responder Sí:

4.1. Seleccione los tipos de eventos que se registran:

- o Intentos de autenticación fallidos.
- o Autenticaciones correctas.
- o Errores de aplicación.
- o Se denegó acceso a los recursos.
- o Acceso a recursos permitido.
- o Cambios a los datos.
- o Cambios a las cuentas de usuarios.

5. ¿Las aplicaciones utilizadas validan datos de entrada?

- o Sí
- o No
- o No lo sé

Es de vital importancia validar los datos de entrada para evitar que las aplicación procese información peligrosa o incorrecta; de lo contrario, los datos podrían estar sujetos a daños, robos, o incluso se podría ejecutar código binario.

En caso de responder Sí:

5.1. De la siguiente lista, seleccione los tipos de entrada de las aplicaciones que se validan:

- o Usuarios finales.
- o Aplicaciones cliente.
- o Alimentación de datos.

6. ¿La información utilizada por los usuarios es encriptada?

- o Sí
- o No
- o No lo sé

7. ¿Las aplicaciones clave encriptan la información critica y sensible que procesan?

- o Sí
- o No
- o No lo sé

Los datos sin encriptar se transmiten y almacenan en un formato de texto legible, quedando más susceptibles a robo o traspaso de información.

En caso de responder Sí:

7.1. Seleccione las diferentes etapas en que se encriptan los datos:

- o Transmisión y almacenamiento
- o Transmisión
- o Almacenamiento

7.2. ¿Cuáles de los siguientes algoritmos de encriptación utilizan?

- o Estándar de encriptación de datos (DES)
- o DES triple (3DES)
- o RC2, RC4 o RC5
- o Entándar de encriptación avanzada (AES4)/rinjindael
- o Hash MD5
- o Hash SHA-1
- o Twofish
- o Blowfish
- o Algoritmo propio

Pregunta	Vulnerabilidad	Escala	Respuesta
1	-	0-4	No - No lo sé
2	-	0-2	No - No lo sé
3	-	0-4	No - No lo sé
4	-	0-2	No - No lo sé
5	-	0-4	No - No lo sé
6	-	0-4	No - No lo sé
7	-	0-8	No - No lo sé

Protección	Escala	Respuesta
-	0 a 6	Sí
-	0 a 3	Sí
-	0-3	Sí
-	0 a 3	Sí
-	0 a 4	Sí
-	0 a 4	Sí
-	0 a 6	Sí

Valores de evaluación de la sección.

Anexo IV: Administración y control

1. ¿Su empresa es la que configura los sistemas o esta tarea la efectúan otros proveedores o distribuidores de hardware?

- o Configurada por personal interno
- o Configurada por un proveedor o distribuidor de hardware

La configuración predeterminada con la que llegan los sistemas se crea para maximizar las características disponibles y por lo general no se da importancia a la seguridad.

2. ¿Cuáles de los siguientes elementos se han creado basándose en una configuración documentada o en una imagen formal?

- o Terminales de trabajo
- o Servidores
- o Ninguno

Es importante utilizar imágenes documentadas para mantener la uniformidad entre todos lo equipos de escritorio y las terminales de trabajo. Esta uniformidad permitirá una mayor eficacia en la detección y paralización de ataques potenciales.

2.1. ¿Esta configuración incluye procedimientos para robustecer el host?

- o Sí
- o No
- o No lo sé

Robustecer el host implica actualizar sistema operativo. Aplicar los parches adecuados, reforzar las configuraciones y auditar el acceso y las vulnerabilidades de los sistemas.

3. ¿Cuáles de las soluciones siguientes se han instalado en las terminales de trabajo y los equipos portátiles de los empleados?

- o software de firewall personal
- o software de detección y eliminación de spyware
- o software de encriptación de discos
- o software de administración/control remoto
- o protector de pantalla protegido por contraseña
- o MODEM
- o Ninguno

4. ¿Se ha aplicado controles de seguridad físico para garantizar la seguridad de la propiedad de la empresa?

- o Sí
- o No
- o No lo sé

Las medidas de seguridad física incluyen cables de bloqueo para equipos portátiles, armarios o racks con llave para servidores/equipos de red y guardias de seguridad.

4.1. ¿Cuál de los siguientes controles de seguridad utiliza?

- o Sistema de alarma para detectar e informar las intrusiones.
- o Equipos de red (conmutadores, cableado, conexiones a Internet) en lugares cerrados con llaves y con acceso restringido.
- o Los equipos de red se encuentran además en un armario o rack que se pueda cerrar con llave.
- o Los servidores se encuentran en un lugar cerrado con llave y con acceso restringido.
- o Los servidores se encuentran además en un armario o rack que se pueda cerrar con llave.
- o Las terminales de trabajo se protegen con cables de seguridad.

- Los materiales impresos confidenciales se guardan en armarios cerrados con llave.

Preguntas	Vulnerabilidad	Escala	Respuesta
1	-	0-1	Defecto
2	-	0-2	Ninguno
3	-	0-2	Ninguno
4	-	0-3	No - No lo sé

Protección	Escala	Respuesta
-	0-1	Interno
-	0 a 3	Varias
-	0 a 5	Varias
-	0-5	Sí

Valores de evaluación de la sección.

Anexo V: Aplicaciones

Este segmento estudia las aplicaciones que son esenciales para la empresa y las valora desde el punto de vista de la seguridad y disponibilidad, además se examinan tecnologías utilizadas para aumentar el índice de defensa en profundidad.

1. En los procedimientos de la empresa, ¿se requiere que terceros procesen la información?

- o Sí
- o No
- o No lo sé

2. ¿Los datos del cliente se almacenan o procesan en un ambiente compartido con recursos corporativos?

- o Sí
- o No
- o No lo sé

3. ¿Recurre a fabricantes independientes de software para complementar la oferta de servicios empresariales?

- o Sí
- o No
- o No lo sé

4. ¿Su empresa recibe ingresos por ofrecer servicios de procesamiento o minería[11] de datos?

- o Sí

[11] Las técnicas de minería de datos se emplean para mejorar el rendimiento de procesos de negocio o industriales en los que se manejan grandes volúmenes de información estructurada y almacenada en bases de datos.

- o No
- o No lo sé

5. Los datos que procesa su empresa, ¿son considerados sensibles o críticos para las operaciones comerciales de sus clientes?

- o Sí
- o No
- o No lo sé

6. ¿Se ofrecen aplicaciones comerciales críticas a través de Internet?

- o Sí
- o No
- o No lo sé

7. ¿Qué mecanismos tiene su empresa para asegurar una alta disponibilidad de las aplicaciones?

- o Equilibrio de carga
- o Clústeres
- o Pruebas periódicas de recuperación de aplicaciones y datos
- o Ninguno

8. ¿Fabricantes independientes de software han desarrollado algunas aplicaciones clave de la red?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

8.1. ¿Los fabricantes independientes proporcionan periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad? (se mantiene soportada)

- o Sí
- o No
- o No lo sé

9. ¿El equipo interno de desarrollo ha creado algunas de las aplicaciones clave de la red?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

9.1. ¿El equipo interno de desarrollo proporcionan periódicamente actualizaciones y parches de software como la documentación sobre los mecanismos de seguridad? (se mantiene soportada)

- o Sí
- o No
- o No lo sé

10. ¿Su empresa conoce las vulnerabilidades de seguridad que existen para las aplicaciones de la red?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

10.1. ¿Su empresa cuenta con los procedimientos para abordar dichas vulnerabilidades?

- o Sí
- o No

Pregunta	Vulnerabilidad	Escala	Respuesta
1	-	0-3	Sí - No lo sé
2	-	0-1	Sí - No lo sé
3	-	0-1	Sí - No lo sé
4	-	0-1	Sí - No lo sé
5	-	0-1	Sí - No lo sé
6	-	0-2	Sí - No lo sé
7	-	0-3	Ninguno
8	-	0-2	Sí - No lo sé
9	-	0-2	Sí - No lo sé
10	-	0-6	Sí - No lo sé

Protección	Escala	Respuesta
-	0-3	No
-	0-1	No
-	0-1	No
-	0-1	No
-	0-1	No
-	0-1	No
-	0 a 3	Varios
-	0-2	No
-	0-1	No
-	0 a 5	Sí

Valores de evaluación de la sección.

Anexo VI: Entorno

1. ¿La actividad de su empresa se desarrolla en un mercado de gran competencia o de investigación, en el que el robo de material intelectual o el espionaje son temas de gran preocupación?

- o Sí
- o No

2. ¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?

- o Sí
- o No
- o No lo sé

3. ¿Obtiene su empresa ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?

- o Sí
- o No
- o No lo sé

4. En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?

- o Sí
- o No

5. Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los clientes, como un apagón o el fallo de una aplicación o hardware, ¿afectaría significativamente a sus ingresos?

- o Sí
- o No
- o No lo sé

6. Los componentes de infraestructura y las aplicaciones del cliente, ¿dependen del acceso a recursos de su entorno?

- o Sí
- o No
- o No lo sé

7. ¿Comparte su empresa los componentes de infraestructura y aplicaciones entre varios clientes?

- o Sí
- o No
- o No lo sé

8. ¿Cambia muy a menudo el personal técnico en su empresa?

- o Sí
- o No

9. ¿Utiliza su empresa versiones obsoletas de software que ya no cuenten con el servicio técnico del fabricante?

- o Sí
- o No
- o No lo sé

10. ¿Adquiere su empresa el software de fabricantes o proveedores conocidos y fiables?

- o Sí
- o No
- o No lo sé

11. ¿Es la empresa la que gestiona el entorno o se contrata los servicios de un tercero?

- o La empresa gestiona el entorno

- o La empresa subcontrata la gestión

En caso de subcontrato:

11.1. ¿Tiene la empresa acuerdo de servicios establecidos como parte de los contratos con los proveedores de servicios subcontratados?

- o Sí
- o No

11.2. ¿Se han incluido cláusulas específicas sobre seguridades los acuerdos de servicios (SLA)?

- o Sí
- o No

12. ¿Utiliza la empresa hosts de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

12.1. Seleccione los sistemas para los que existen hosts de gestión dedicados:

- o Dispositivos de red
- o Servidores

13. ¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las actividades administrativas o de gestión?

- o Sí
- o No
- o No lo sé

14. ¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?

- o Sí
- o No
- o No lo sé

15. ¿Se comprueba periódicamente el cortafuego para garantizar que funciona según lo previsto?

- o Sí
- o No
- o No lo sé

Pregunta	Vulnerabilidad	Escala	Respuesta		Protección	Escala	Respuesta
1	0	0-1	Sí		1	0-1	No
2	0	0-2	Sí		1	0-1	No
3	0	0-2	Sí		1	0-1	No
4	2	0-2	Sí		0	0-1	No
5	0	0-2	Sí - No lo sé		2	0-2	No
6	2	0-2	Sí - No lo sé		0	0-2	No
7	0	0-1	Sí - No lo sé		1	0-1	No
8	0	0-2	Sí		2	0-2	No
9	0	0-3	Sí - No lo sé		2	0-2	No
10	0	0-3	No - No lo sé		3	0-3	Sí
11	0	0 a 2	Subcontrato		0	0-1	Interno
12	0	0-2	No - No lo sé		2	0 a 3	Sí
13	2	0-2	No - No lo sé		0	0-2	Sí
14	2	0-2	No - No lo sé		0	0-2	Sí
15	0	0-2	Sí - No lo sé		2	0-2	Sí

Valores de evaluación de la sección.

Anexo VII: Directiva de seguridad

1. ¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?

- o Sí
- o No
- o No lo sé

Al asignar niveles de prioridad a los componentes, una empresa estará más preparada para centrar sus esfuerzos de seguridad en aquellos sistemas que necesitan acceso. Disponer de una lista de este tipo también asigna una prioridad para la recuperación cuando se producen apagones.

2. ¿Existen directivas para la regulación del entorno informático?

- o Sí
- o No
- o No lo sé

Las directivas son reglas y prácticas que especifican cómo se puede utilizar de forma adecuada un entorno informático. Si no existen directivas, no existe mecanismo alguno para definir o hacer cumplir los controles dentro del entorno.

En caso de responder Sí:

2.1. ¿Existen directivas de seguridad de información para la regulación de la actividad relacionada con la seguridad de la empresa?

- o Sí
- o No
- o No lo sé

2.1.1. Indique quién desarrolló la directiva:

- o Sólo el departamento de TI
- o Sólo el departamento de representantes comerciales

- El departamento de TI y de representantes comerciales en conjunto

2.2. ¿Hay una directiva corporativa para el uso aceptable?

- Sí
- No
- No lo sé

2.3. ¿Hay directivas para la gestión de las cuentas de usuarios individuales?

- Sí
- No
- No lo sé

En caso de responder Sí:

2.3.1. Seleccione cuáles de las siguientes directivas se aplican a la gestión de las cuentas de usuarios individuales:

- Cuentas de usuarios individuales (no compartidas)
- Cuentas sin y con privilegios para administradores
- Hacer cumplir la calidad de las contraseñas
- Cuando un empleado deja su trabajo, se desactivas sus cuentas?

3. ¿Hay un proceso documentado para la creación de hosts? Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de hosts hay un proceso de creación documentado?)

- Dispositivos de infraestructura
- Servidores
- Estaciones de trabajo y portátiles
- Ninguno

4. ¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:

- Sí

- o No
- o No lo sé

Preguntas	Vulnerabilidad	Escala	Respuesta
1	-	0-3	No - No lo sé
2	-	0-4	No - No lo sé
3	-	0-2	Ninguno
4	-	0-4	No - No lo sé

Protección	Escala	Respuesta
-	0-3	Sí
-	0 a 6	Sí
-	0 a 3	Varios
-	0-4	Sí

Valores de evaluación de la sección.

Anexo VIII: Gestión de actualizaciones y revisiones

1. ¿Hay un proceso de gestión para las configuraciones y los cambios?

- o Sí
- o No
- o No lo sé

Los procesos de gestión de cambios y configuraciones permiten asegurar que los cambios en el entorno de producción, se han probado y documentado exhaustivamente antes de utilizarse.

En caso de responder Sí:

1.1. ¿Dispone la empresa de configuraciones documentadas a modo de referencia?

- o Sí
- o No
- o No lo sé

2. ¿Prueba la empresa los cambios de configuración antes de aplicarlos a los sistemas de producción?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

2.1. ¿Se comprueba y se garantiza de forma centralizada la compatibilidad con las configuraciones (por ejemplo, mediante directivas de grupos)?

- o Sí
- o No
- o No lo sé

3. ¿Existe un proceso establecido para las directivas de actualización y revisión?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

3.1. Seleccione los componentes para los que existan estos procesos:

- o Sistemas operativos
- o Aplicaciones
- o Tanto los sistemas operativos como las aplicaciones

4. ¿Prueba la empresa las actualizaciones y revisiones antes de aplicarlas?

- o Sí
- o No
- o No lo sé

4.1. Indique cuáles de los siguientes elementos se utilizan para aplicar y gestionar las actualizaciones:

- o Actualización automática de Windows
- o Sitio Web de Windows Update
- o Servicios de actualización de Windows Server (WSUS)
- o Otras soluciones de gestión de actualizaciones

4.2. ¿En qué tipos de hosts se utiliza la gestión automática de actualizaciones?

- o Estaciones de trabajo
- o Servidores

5. ¿Existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas?

- o Antivirus
- o Sistema de detección de intrusiones (IDS)

- Ninguno

La aparición de nuevos virus es constante, por lo que resulta imprescindible mantener una lista actualizada de firmas de virus. Su solución antivirus será tan eficaz como lo permita su lista de firmas de virus.

6. ¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los hosts?

- Sí
- No ó han caducado
- No lo sé

7. ¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?

- Sí
- No
- No lo sé

En caso de responder Sí:

7.1. Seleccione los tipos de aplicaciones de las que existen diagramas

- Sólo aplicaciones externas
- Sólo aplicaciones internas
- Tanto las aplicaciones internas como externas

Preguntas	Vulnerabilidad	Escala	Respuesta
1	-	0-3	No - No lo sé
2	-	0-2	No - No lo sé
3	-	0-3	No - No lo sé
4	-	0-2	No - No lo sé
5	-	0-2	Ninguno
6	-	0-3	No - No lo sé
7	-	0-2	No - No lo sé

Protección	Escala	Respuesta
-	0 a 3	Sí
-	0 a 3	Sí
-	0 a 4	Sí
-	0 a 5	Sí
-	0 a 2	Varios
-	0-3	Sí
-	0 a 4	Sí

Valores de evaluación de la sección.

Anexo IX: Copias de seguridad y recuperación

1. ¿Está activado en el entorno el registro de los eventos producidos en los hosts y los dispositivos?

- o Sí
- o No
- o No lo sé

2. ¿Toma medidas la empresa para proteger la información incluida en los registros?

- o El sistema operativo y las aplicaciones están configuradas para no sobrescribir eventos.
- o Los archivos de registro se rotan con frecuencia para asegurarse de que hay suficiente espacio disponible.
- o El acceso a los archivos de registro está restringido a las cuentas de tipo administrador.
- o Los registros se almacenan en un servidor central de registros
- o Ninguno

3. ¿Revisa la empresa periódicamente los archivos de registro?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

3.1. ¿Con qué frecuencia se revisan los registros?

- o Diariamente
- o Semanalmente
- o Mensualmente
- o Según sea necesario
- o No lo sé

4. ¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

4.1. ¿Existen directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

4.1.1. ¿Cuáles de las directivas y procedimientos siguientes se cumplen?

- o Almacenamiento fuera de las instalaciones
- o Almacenamiento en armarios cerrados, a prueba de fuego
- o Acceso limitado a dispositivos de copias de seguridad
- o Rotación y duración de los dispositivos de copias de seguridad

5. ¿Existen directivas para la comprobación periódica de los procedimientos de copias de seguridad y restauración? Estas directivas, ¿están documentadas?

- o Sí, y están documentados
- o Sí, pero no están documentados
- o No
- o No lo sé

Preguntas	Vulnerabilidad	Escala	Respuesta		Protección	Escala	Respuesta
1	-	0-3	No - No lo sé		-	0-3	Sí
2	-	0-2	Ninguno		-	0 a 4	Varios
3	-	0-2	No - No lo sé		-	0 a 3	Sí
4	-	0-2	No - No lo sé		-	0 a 4	Sí
5	-	0-2	No - No lo sé		-	0 a 2	Sí

Valores de evaluación de la sección.

Anexo X: Requisitos y evaluaciones

1. ¿Hay en su empresa individuos o grupos que sean responsables de la seguridad?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

1.1. ¿Tienen estos individuos o grupos experiencia en el tema de la seguridad?

- o Sí
- o No
- o No lo sé

1.2. ¿Estos individuos o grupos se ocupan de establecer los requisitos de seguridad de las tecnologías nuevas existentes?

- o Sí
- o No
- o No lo sé

1.3. ¿Existen responsabilidades y roles definidos para cada individuo que participe en la seguridad de la información?

- o Sí
- o No
- o No lo sé

2. ¿Realiza su empresa evaluaciones de la seguridad del entorno a través de terceros?

- o Sí
- o No
- o No lo sé

Las evaluaciones de seguridad realizadas por terceros facilitan una visión más independiente y objetiva de sus soluciones de seguridad.

En caso de responder Sí:

2.1. ¿Con qué frecuencia se llevan a cabo estas evaluaciones?

- o Trimestralmente
- o Semanalmente
- o Anualmente
- o Cada dos años o menos

2.2. Seleccione las áreas de análisis que comprenden estas evaluaciones:

- o Infraestructura
- o Aplicaciones
- o Directiva
- o Auditoria

3. ¿Realiza su empresa evaluaciones de la seguridad del entorno de forma interna?

- o Sí
- o No
- o No lo sé

En caso de responder Sí:

3.1. ¿Con qué frecuencia se llevan a cabo estas evaluaciones?

- o Trimestralmente
- o Semanalmente
- o Anualmente
- o Cada dos años o menos

3.2. Selecciones las áreas que comprenden estas evaluaciones:

- o Infraestructura
- o Aplicaciones

- Directiva
- Auditoria

Preguntas	Vulnerabilidad	Escala	Respuesta
1	-	0-3	No - No lo sé
2	-	0-4	No - No lo sé
3	-	0-4	No - No lo sé

Protección	Escala	Respuesta
-	0 a 4	Sí
-	0 a 6	Sí
-	0 a 6	Sí

Valores de evaluación de la sección.

Anexo XI: Directiva y procedimientos

1. ¿Realiza la empresa comprobaciones del historial personal como parte del proceso de contratación?

- o Sí
- o No
- o No lo sé

Se debe comprobar el historial personal de aspirantes para identificar asuntos que puedan afectar a la seguridad de su empresa.

En caso de responder Sí:

1.1. Seleccione la opción más adecuada:

- o Se hacen comprobaciones del historial personal de cada aspirante.
- o Se hacen comprobaciones del historial personal sólo de aspirantes a puestos críticos o confidenciales.

2. ¿Hay un proceso formal para la salida de la empresa de los empleados?

- o Sí
- o No
- o No lo sé

Cuando los empleados dejan la empresa, existe la posibilidad de que lo hagan de forma hostil. Para reducir los riesgos, se debe mantener un proceso formal para los empleados que dejan la empresa.

3. ¿Hay una directiva formal para las relaciones con terceros?

- o Sí
- o No
- o No lo sé

Las relaciones con terceros (socios, clientes o fabricantes) aumentan notablemente el riesgo al que ambas partes se ven expuestos.

Preguntas	Vulnerabilidad	Escala	Respuesta		Protección	Escala	Respuesta
1	-	0-3	No - No lo sé		-	0 a 3	Sí
2	-	0-3	No - No lo sé		-	0-3	Sí
3	-	0-3	No - No lo sé		-	0-3	Sí

Valores de evaluación de la sección.

Anexo XII: Formación y conocimiento

1. ¿Hay un programa de divulgación de las medidas de seguridad en su empresa?

- o Sí
- o No
- o No lo sé

Un programa de divulgación de las medidas de seguridad mantiene a los empleados al corriente de los riesgos y vulnerabilidades presentes. Los empleados que son conscientes de su importancia benefician la seguridad general de la empresa.

En caso de responder Sí:

1.1. ¿Cuál es el porcentaje de empleados que han participado en el programa de divulgación de las medidas de seguridad?

- o Menos del 25%
- o Del 25 al 49%
- o Del 50 al 75%
- o Más del 75%

2. ¿Cuáles de los siguientes temas se incluyen en los cursos de formación sobre la seguridad?

- o Directivas y controles de seguridad de la empresa
- o Informes sobre actividades sospechosas
- o Confidencialidad
- o Seguridad del correo electrónico, incluyendo Spam y gestión de adjuntos
- o Seguridad de Internet, incluyendo navegación por la Web y descargas
- o Seguridad informática, incluyendo el uso de cortafuegos particulares y cifrado

- o Ninguno

2.1. ¿Con que frecuencia se realizan estos cursos?

- o Trimestralmente
- o Semestralmente
- o Anualmente
- o Cada dos años o menos

3. ¿Se ofrece a los empleados formación relacionada con el cargo que desempeñan en la empresa?

- o Sí
- o No
- o No lo sé

La formación basada en roles y el aprendizaje continuo garantizan que todos los empleados entiendan qué se espera de ellos.

En caso de responder Sí:

3.1. Seleccione las opciones que correspondan en la siguiente lista:

- o Seguridad de las operaciones
- o Seguridad de la infraestructura
- o Seguridad de las aplicaciones
- o Preparación para incidentes y reacción

Preguntas	Vulnerabilidad	Escala	Respuesta
1	-	0-3	No - No lo sé
2	-	0-3	Ninguno
3	-	0-2	No - No lo sé

Protección	Escala	Respuesta
-	0 a 4	Sí
-	0 a 5	Varios
-	0 a 3	Sí

Valores de evaluación de la sección.

Anexo XIII: Lista de puertos usados por troyanos

puerto 1 (UDP) - Sockets des Troie
puerto 2 Death
puerto 15 B2
puerto 20 Senna Spy FTP server
puerto 21 Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP,
Doly Trojan, Fore, FreddyK, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, RTB 666, Senna Spy FTP server, The Flu, Traitor 21, WebEx,
WinCrash
puerto 22 Adore sshd, Shaft
puerto 23 ADM worm, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server - TTS, Truva Atl
puerto 25 Ajan, Antigen, Barok, BSE, Email Password Sender - EPS, EPS II, Gip, Gris,
Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing
Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth,
Stukach, Tapiras, Terminator, WinPC, WinSpy
puerto 30 Agent 40421
puerto 31 Agent 31, Hackers Paradise, Masters Paradise
puerto 39 SubSARI
puerto 41 Deep Throat, Foreplay
puerto 44 Arctic
puerto 48 DRAT
puerto 50 DRAT
puerto 53 ADM worm, Lion
puerto 58 DMSetup
puerto 59 DMSetup
puerto 69 BackGate
puerto 79 CDK, Firehotcker
puerto 80 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins,
Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB
666, Seeker, WAN Remote, Web Server CT, WebDownloader
puerto 81 RemoConChubo
puerto 99 Hidden
puerto, Mandragore, NCX
puerto 110 ProMail trojan
puerto 113 Invisible Identd Deamon, Kazimas
puerto 119 Happy99

puerto 121 Attack Bot, God Message, JammerKillah
puerto 123 Net Controller
puerto 133 Farnaz
puerto 137 Chode
puerto 137 (UDP) - Msinit, Qaz
puerto 138 Chode
puerto 139 Chode, God Message worm, Msinit, Netlog, Network, Qaz, Sadmind, SMB
Relay
puerto 142 NetTaxi
puerto 146 Infector
puerto 146 (UDP) - Infector
puerto 166 NokNok
puerto 170 A-trojan
puerto 334 Backage
puerto 411 Backage
puerto 420 Breach, Incognito
puerto 421 TCP Wrappers trojan
puerto 455 Fatal Connections
puerto 456 Hackers Paradise
puerto 511 T0rn Rootkit
puerto 513 Grlogin
puerto 514 RPC Backdoor
puerto 515 lpdw0rm, Ramen
puerto 531 Net666, Rasmin
puerto 555 711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0,
Stealth Spy
puerto 600 Sadmind
puerto 605 Secret Service
puerto 661 NokNok
puerto 666 Attack FTP, Back Construction, BLA trojan, Cain & Abel, lpdw0rm, NokNok,
Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)
puerto 667 SniperNet
puerto 668 th3r1pp3rz (= Therippers)
puerto 669 DP trojan
puerto 692 GayOL
puerto 777 AimSpy, Undetected
puerto 808 WinHole
puerto 911 Dark Shadow, Dark Shadow
puerto 999 Chat power, Deep Throat, Foreplay, WinSatan
puerto 1000 Connecter, Der Späher / Der Spaeher, Direct Connection
puerto 1001 Der Späher / Der Spaeher, Le Guardien, Silencer, Theef, WebEx
puerto 1005 Theef
puerto 1008 Lion

puerto 1010 Doly Trojan
puerto 1011 Doly Trojan
puerto 1012 Doly Trojan
puerto 1015 Doly Trojan
puerto 1016 Doly Trojan
puerto 1020 Vampire
puerto 1024 Jade, Latinus, NetSpy, Remote Administration Tool - RAT [no 2]
puerto 1025 Fraggle Rock, md5 Backdoor, NetSpy, Remote Storm
puerto 1025 (UDP) - Remote Storm
puerto 1031 Xanadu
puerto 1035 Multidropper
puerto 1042 BLA trojan
puerto 1042 (UDP) - BLA trojan
puerto 1045 Rasmin
puerto 1049 /sbin/initd
puerto 1050 MiniCommand
puerto 1053 The Thief
puerto 1054 AckCmd
puerto 1080 SubSeven 2.2, WinHole
puerto 1081 WinHole
puerto 1082 WinHole
puerto 1083 WinHole
puerto 1090 Xtreme
puerto 1095 Remote Administration Tool - RAT
puerto 1097 Remote Administration Tool - RAT
puerto 1098 Remote Administration Tool - RAT
puerto 1099 Blood Fest Evolution, Remote Administration Tool - RAT
puerto 1104 (UDP) - RexxRave
puerto 1150 Orion
puerto 1151 Orion
puerto 1170 Psyber Stream Server - PSS, Streaming Audio Server, Voice
puerto 1174 DaCryptic
puerto 1180 Unin68
puerto 1200 (UDP) - NoBackO
puerto 1201 (UDP) - NoBackO
puerto 1207 SoftWAR
puerto 1208 Infector
puerto 1212 Kaos
puerto 1234 SubSeven Java client, Ultors Trojan
puerto 1243 BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles
puerto 1245 VooDoo Doll
puerto 1255 Scarab
puerto 1256 Project nEXT, RexxRave
puerto 1269 Matrix
puerto 1272 The Matrix
puerto 1313 NETrojan

puerto 1337 Shadyshell
puerto 1338 Millennium Worm
puerto 1349 Bo dll
puerto 1386 Dagger
puerto 1394 GoFriller
puerto 1441 Remote Storm
puerto 1492 FTP99CMP
puerto 1524 Trinoo
puerto 1568 Remote Hack
puerto 1600 Direct Connection, Shivka-Burka
puerto 1703 Exploiter
puerto 1777 Scarab
puerto 1807 SpySender
puerto 1826 Glacier
puerto 1966 Fake FTP
puerto 1967 For Your Eyes Only - FYEO, WM FTP Server
puerto 1969 OpC BO
puerto 1981 Bowl, Shockrave
puerto 1991 PitFall
puerto 1999 Back Door, SubSeven, TransScout
puerto 2000 Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000,
Senna Spy Trojan Generator
puerto 2001 Der Späher / Der Spaeher, Trojan Cow
puerto 2023 Ripper Pro
puerto 2080 WinHole
puerto 2115 Bugs
puerto 2130 (UDP) - Mini Backlash
puerto 2140 The Invasor
puerto 2140 (UDP) - Deep Throat, Foreplay
puerto 2155 Illusion Mailer
puerto 2255 Nirvana
puerto 2283 Hvl RAT
puerto 2300 Xplorer
puerto 2311 Studio 54
puerto 2330 IRC Contact
puerto 2331 IRC Contact
puerto 2332 IRC Contact
puerto 2333 IRC Contact
puerto 2334 IRC Contact
puerto 2335 IRC Contact
puerto 2336 IRC Contact
puerto 2337 IRC Contact
puerto 2338 IRC Contact
puerto 2339 IRC Contact, Voice Spy
puerto 2339 (UDP) - Voice Spy

puerto 2345 Doly Trojan
puerto 2400 puertod
puerto 2555 Lion, T0rn Rootkit
puerto 2565 Striker trojan
puerto 2583 WinCrash
puerto 2589 Dagger
puerto 2600 Digital RootBeer
puerto 2702 Black Diver
puerto 2716 The Prayer
puerto 2773 SubSeven, SubSeven 2.1 Gold
puerto 2774 SubSeven, SubSeven 2.1 Gold
puerto 2801 Phineas Phucker
puerto 2929 Konik
puerto 2989 (UDP) - Remote Administration Tool - RAT
puerto 3000 InetSpy, Remote Shut
puerto 3024 WinCrash
puerto 3031 Microspy
puerto 3128 Reverse WWW Tunnel Backdoor, RingZero
puerto 3129 Masters Paradise
puerto 3131 SubSARI
puerto 3150 The Invasor
puerto 3150 (UDP) - Deep Throat, Foreplay, Mini Backlash
puerto 3456 Terror trojan
puerto 3459 Eclipse 2000, Sanctuary
puerto 3700 puertoal of Doom
puerto 3777 PsychWard
puerto 3791 Total Solar Eclypse
puerto 3801 Total Solar Eclypse
puerto 4000 Connect-Back Backdoor, SkyDance
puerto 4092 WinCrash
puerto 4201 War trojan
puerto 4242 Virtual Hacking Machine - VHM
puerto 4321 BoBo
puerto 4444 CrackDown, Prosiak, Swift Remote
puerto 4488 Event Horizon
puerto 4523 Celine
puerto 4545 Internal Revise
puerto 4567 File Nail
puerto 4590 ICQ Trojan
puerto 4653 Cero
puerto 4666 Mneah
puerto 4950 ICQ Trogen (Lm)
puerto 5000 Back Door Setup, BioNet Lite, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des
Troie
puerto 5001 Back Door Setup, Sockets des Troie

puerto 5002 cd00r, Linux Rootkit IV (4), Shaft
puerto 5005 Aladino
puerto 5010 Solo
puerto 5011 One of the Last Trojans - OOTLT, One of the Last Trojans - OOTLT, modified
puerto 5025 WM Remote KeyLogger
puerto 5031 Net Metropolitan
puerto 5032 Net Metropolitan
puerto 5321 Firehotcker
puerto 5333 Backage, NetDemon
puerto 5343 WC Remote Administration Tool - wCrat
puerto 5400 Back Construction, Blade Runner
puerto 5401 Back Construction, Blade Runner, Mneah
puerto 5402 Back Construction, Blade Runner, Mneah
puerto 5512 Illusion Mailer
puerto 5534 The Flu
puerto 5550 Xtcp
puerto 5555 ServeMe
puerto 5556 BO Facil
puerto 5557 BO Facil
puerto 5569 Robo-Hack
puerto 5637 PC Crasher
puerto 5638 PC Crasher
puerto 5742 WinCrash
puerto 5760 puertomap Remote Root Linux Exploit
puerto 5802 Y3K RAT
puerto 5873 SubSeven 2.2
puerto 5880 Y3K RAT
puerto 5882 Y3K RAT
puerto 5882 (UDP) - Y3K RAT
puerto 5888 Y3K RAT
puerto 5888 (UDP) - Y3K RAT
puerto 5889 Y3K RAT
puerto 6000 The Thing
puerto 6006 Bad Blood
puerto 6272 Secret Service
puerto 6400 The Thing
puerto 6661 TEMan, Weia-Meia
puerto 6666 Dark Connection Inside, NetBus worm
puerto 6667 Dark FTP, EGO, Maniac rootkit, Moses, ScheduleAgent, SubSeven, Subseven
2.1.4 DefCon 8, The Thing (modified), Trinity, WinSatan
puerto 6669 Host Control, Vampire
puerto 6670 BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame
puerto 6711 BackDoor-G, SubSARI, SubSeven, VP Killer
puerto 6712 Funny trojan, SubSeven

puerto 6713 SubSeven
puerto 6723 Mstream
puerto 6767 UandMe
puerto 6771 Deep Throat, Foreplay
puerto 6776 2000 Cracks, BackDoor-G, SubSeven, VP Killer
puerto 6838 (UDP) - Mstream
puerto 6883 Delta Source DarkStar (??)
puerto 6912 Shit Heep
puerto 6939 Indoctrination
puerto 6969 2000 Cracks, Danton, GateCrasher, IRC 3, Net Controller, Priority
puerto 6970 GateCrasher
puerto 7000 Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1
Gold
puerto 7001 Freak88, Freak2k, NetSnooper Gold
puerto 7158 Lohoboyshik
puerto 7215 SubSeven, SubSeven 2.1 Gold
puerto 7300 NetMonitor
puerto 7301 NetMonitor
puerto 7306 NetMonitor
puerto 7307 NetMonitor, Remote Process Monitor
puerto 7308 NetMonitor, X Spy
puerto 7424 Host Control
puerto 7424 (UDP) - Host Control
puerto 7597 Qaz
puerto 7626 Binghe, Glacier, Hyne
puerto 7718 Glacier
puerto 7777 God Message, The Thing (modified), Tini
puerto 7789 Back Door Setup, ICKiller, Mozilla
puerto 7826 Oblivion
puerto 7891 The ReVeNgEr
puerto 7983 Mstream
puerto 8080 Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW Tunnel
Backdoor, RingZero
puerto 8685 Unin68
puerto 8787 Back Orifice 2000
puerto 8812 FraggleRock Lite
puerto 8988 BacHack
puerto 8989 Rcon, Recon, Xcon
puerto 9000 Netministrator
puerto 9325 (UDP) - Mstream
puerto 9400 InCommand
puerto 9870 Remote Computer Control Center
puerto 9872 puertoal of Doom
puerto 9873 puertoal of Doom

puerto 9874 puertoal of Doom
puerto 9875 puertoal of Doom
puerto 9876 Cyber Attacker, Rux
puerto 9878 TransScout
puerto 9989 Ini-Killer
puerto 9999 The Prayer
puerto 10000 OpwinTRojan
puerto 10005 OpwinTRojan
puerto 10008 Cheese worm, Lion
puerto 10067 (UDP) - puertoal of Doom
puerto 10085 Syphillis
puerto 10086 Syphillis
puerto 10100 Control Total, GiFt trojan
puerto 10101 BrainSpy, Silencer
puerto 10167 (UDP) - puertoal of Doom
puerto 10520 Acid Shivers
puerto 10528 Host Control
puerto 10607 Coma
puerto 10666 (UDP) - Ambush
puerto 11000 Senna Spy Trojan Generator
puerto 11050 Host Control
puerto 11051 Host Control
puerto 11223 Progenic trojan, Secret Agent
puerto 11831 Latinus
puerto 12076 Gjamer
puerto 12223 Hack´99 KeyLogger
puerto 12310 PreCursor
puerto 12345 Adore sshd, Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates,
ValvNet, Whack Job, X-bill
puerto 12346 Fat Bitch trojan, GabanBus, NetBus, X-bill
puerto 12348 BioNet
puerto 12349 BioNet, Webhead
puerto 12361 Whack-a-mole
puerto 12362 Whack-a-mole
puerto 12363 Whack-a-mole
puerto 12623 (UDP) - DUN Control
puerto 12624 ButtMan
puerto 12631 Whack Job
puerto 12754 Mstream
puerto 13000 Senna Spy Trojan Generator, Senna Spy Trojan Generator
puerto 13010 BitchController, Hacker Brasil - HBR
puerto 13013 PsychWard
puerto 13014 PsychWard
puerto 13223 Hack´99 KeyLogger

puerto 13473 Chupacabra
puerto 14500 PC Invader
puerto 14501 PC Invader
puerto 14502 PC Invader
puerto 14503 PC Invader
puerto 15000 NetDemon
puerto 15092 Host Control
puerto 15104 Mstream
puerto 15382 SubZero
puerto 15858 CDK
puerto 16484 Mosucker
puerto 16660 Stacheldraht
puerto 16772 ICQ Revenge
puerto 16959 SubSeven, Subseven 2.1.4 DefCon 8
puerto 16969 Priority
puerto 17166 Mosaic
puerto 17300 Kuang2 the virus
puerto 17449 Kid Terror
puerto 17499 CrazzyNet
puerto 17500 CrazzyNet
puerto 17569 Infector
puerto 17593 AudioDoor
puerto 17777 Nephron
puerto 18667 Knark
puerto 18753 (UDP) - Shaft
puerto 19864 ICQ Revenge
puerto 20000 Millenium
puerto 20001 Insect, Millenium, Millenium (Lm)
puerto 20002 AcidkoR
puerto 20005 Mosucker
puerto 20023 VP Killer
puerto 20034 NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
puerto 20203 Chupacabra
puerto 20331 BLA trojan
puerto 20432 Shaft
puerto 20433 (UDP) - Shaft
puerto 21544 GirlFriend, Kid Terror, Matrix
puerto 21554 Exploiter, FreddyK, Kid Terror, Schwindler, Winsp00fer
puerto 21579 Breach
puerto 21957 Latinus
puerto 22222 Donald Dick, Prosiak, Ruler, RUX The TIc.K
puerto 23005 NetTrash, Olive, Oxon
puerto 23006 NetTrash
puerto 23023 Logged
puerto 23032 Amanda
puerto 23321 Konik

puerto 23432 Asylum
puerto 23456 Evil FTP, Ugly FTP, Whack Job
puerto 23476 Donald Dick
puerto 23476 (UDP) - Donald Dick
puerto 23477 Donald Dick
puerto 23777 InetSpy
puerto 24000 Infector
puerto 24289 Latinus
puerto 25123 Goy\'Z TroJan
puerto 25555 FreddyK
puerto 25685 MoonPie
puerto 25686 MoonPie
puerto 25982 MoonPie
puerto 26274 (UDP) - Delta Source
puerto 26681 Voice Spy
puerto 27160 MoonPie
puerto 27374 Bad Blood, EGO, Fake SubSeven, Lion, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven 2.2, SubSeven Muie, The Saint,
Ttfloader, Webhead
puerto 27444 (UDP) - Trinoo
puerto 27573 SubSeven
puerto 27665 Trinoo
puerto 28431 Hack´a´Tack
puerto 28678 Exploiter
puerto 29104 NetTrojan
puerto 29292 BackGate
puerto 29369 ovasOn
puerto 29559 Latinus
puerto 29891 The Unexplained
puerto 30000 Infector
puerto 30001 ErrOr32
puerto 30003 Lamers Death
puerto 30005 Backdoor JZ
puerto 30029 AOL trojan
puerto 30100 NetSphere
puerto 30101 NetSphere
puerto 30102 NetSphere
puerto 30103 NetSphere
puerto 30103 (UDP) - NetSphere
puerto 30133 NetSphere
puerto 30303 Sockets des Troie
puerto 30700 Mantis
puerto 30947 Intruse
puerto 30999 Kuang2
puerto 31221 Knark

puerto 31335 Trinoo
puerto 31336 Bo Whack, Butt Funnel
puerto 31337 ADM worm, Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back
Orifice russian, Baron Night, Beeone, bindshell, BO client, BO Facil, BO spy, BO2, cron /
crontab, Freak88, Freak2k, Gummo, icmp_pipe.c, Linux Rootkit IV (4), Sm4ck, Sockdmini
puerto 31337 (UDP) - Back Orifice, Deep BO
puerto 31338 Back Orifice, Butt Funnel, NetSpy (DK)
puerto 31338 (UDP) - Deep BO, NetSpy (DK)
puerto 31339 NetSpy (DK), NetSpy (DK)
puerto 31557 Xanadu
puerto 31666 BOWhack
puerto 31745 BuschTrommel
puerto 31785 Hack´a´Tack
puerto 31787 Hack´a´Tack
puerto 31788 Hack´a´Tack
puerto 31789 (UDP) - Hack´a´Tack
puerto 31790 Hack´a´Tack
puerto 31791 (UDP) - Hack´a´Tack
puerto 31792 Hack´a´Tack
puerto 32001 Donald Dick
puerto 32100 Peanut Brittle, Project nEXT
puerto 32418 Acid Battery
puerto 32791 Acropolis
puerto 33270 Trinity
puerto 33333 Blakharaz, Prosiak
puerto 33567 Lion, T0rn Rootkit
puerto 33568 Lion, T0rn Rootkit
puerto 33577 Son of PsychWard
puerto 33777 Son of PsychWard
puerto 33911 Spirit 2000, Spirit 2001
puerto 34324 Big Gluck, TN
puerto 34444 Donald Dick
puerto 34555 (UDP) - Trinoo (for Windows)
puerto 35555 (UDP) - Trinoo (for Windows)
puerto 37237 Mantis
puerto 37266 The Killer Trojan
puerto 37651 Yet Another Trojan - YAT
puerto 38741 CyberSpy
puerto 39507 Busters
puerto 40412 The Spy
puerto 40421 Agent 40421, Masters Paradise
puerto 40422 Masters Paradise
puerto 40423 Masters Paradise

puerto 40425 Masters Paradise
puerto 40426 Masters Paradise
puerto 41337 Storm
puerto 41666 Remote Boot Tool - RBT, Remote Boot Tool - RBT
puerto 44444 Prosiak
puerto 44575 Exploiter
puerto 44767 (UDP) - School Bus
puerto 45559 Maniac rootkit
puerto 45673 Acropolis
puerto 47017 T0rn Rootkit
puerto 47262 (UDP) - Delta Source
puerto 48004 Fraggle Rock
puerto 48006 Fraggle Rock
puerto 49000 Fraggle Rock
puerto 49301 OnLine KeyLogger
puerto 50000 SubSARI
puerto 50130 Enterprise
puerto 50505 Sockets des Troie
puerto 50766 Fore, Schwindler
puerto 51966 Cafeini
puerto 52317 Acid Battery 2000
puerto 53001 Remote Windows Shutdown - RWS
puerto 54283 SubSeven, SubSeven 2.1 Gold
puerto 54320 Back Orifice 2000
puerto 54321 Back Orifice 2000, School Bus
puerto 55165 File Manager trojan, File Manager trojan, WM Trojan Generator
puerto 55166 WM Trojan Generator
puerto 57341 NetRaider
puerto 58339 Butt Funnel
puerto 60000 Deep Throat, Foreplay, Sockets des Troie
puerto 60001 Trinity
puerto 60008 Lion, T0rn Rootkit
puerto 60068 Xzip 6000068
puerto 60411 Connection
puerto 61348 Bunker-Hill
puerto 61466 TeleCommando
puerto 61603 Bunker-Hill
puerto 63485 Bunker-Hill
puerto 64101 Taskman
puerto 65000 Devil, Sockets des Troie, Stacheldraht
puerto 65390 Eclypse
puerto 65421 Jade
puerto 65432 The Traitor (= th3tr41t0r)
puerto 65432 (UDP) - The Traitor (= th3tr41t0r)
puerto 65530 Windows Mite
puerto 65534 /sbin/initd