UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

Tema:

"SEGURIDAD DE ACCESO AL SERVICIO DE INTERNET Y LOS ATAQUES CIBERNÉTICOS EN EL HOTEL CASINO EMPERADOR DE LA CIUDAD DE AMBATO "

TESIS DE GRADO

Previa a la obtención del Título de Magister en Redes y Telecomunicaciones

Autor: Ing. Santiago José Gavilanes Vásquez

Director: Ing. M. Sc. Franklin Mayorga

Ambato – Ecuador

2011

Al Consejo de Posgrado de la UTA.

El comité de defensa de la Tesis de Grado. "**SEGURIDAD DE ACCESO AL SERVICIO DE INTERNET Y LOS ATAQUES CIBERNÉTICOS EN EL HOTEL CASINO EMPERADOR DE LA CIUDAD DE AMBATO**", presentada por: Ing. Santiago José Gavilanes Vásquez y conformada por: Ing. M.Sc David Guevara, Ing. M.Sc. Hernando Buenaño e Ing. M.Sc. Eddie Galarza, Miembros del Tribunal de Defensa, Ing. M.Sc. Franklin Mayorga, Director de Tesis de Grado y presidido por: Ing. M.Sc. Oswaldo Paredes O,. Presidente del Tribunal de Defensa; Ing. M.Sc. Luis Anda Torres, Director del CEPOS – UTA, una vez escuchada la defensa oral y revisada la Tesis de Grado escrita en la cual se ha constatado el cumplimiento de las observaciones realizadas por el Tribunal de Defensa de la Tesis, remite la presente Tesis para uso y custodia en las bibliotecas de la UTA.

Ing. M.Sc. Oswaldo Paredes O.
Presidente del Tribunal de Defensa

Ing. M.Sc. Luis Anda Torres
DIRECTOR CEPOS

Ing. M.Sc. Franklin Mayorga
Director de Tesis

Ing. M.Sc. David Guevara
Miembro del Tribunal

Ing. M.Sc. Hernando Buenaño
Miembro del Tribunal

Ing. M.Sc. Eddie Galarza
Miembro del Tribunal

AUTORIA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y criticas emitidas en el trabajo de investigación con el tema "**SEGURIDAD DE ACCESO AL SERVICIO DE INTERNET Y LOS ATAQUES CIBERNÉTICOS EN EL HOTEL CASINO EMPERADOR DE LA CIUDAD DE AMBATO**", nos corresponde exclusivamente a Ing. Santiago José Gavilanes Vásquez Autor e Ing. M.Sc. Franklin Mayorga, Director de la Tesis de Grado; y el patrimonio intelectual de la misma a la Universidad Técnica de Ambato.

---	---
Ing. Santiago José Gavilanes Vásquez	Ing. M.Sc. Franklin Mayorga
Autor	Director de Tesis

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de esta tesis o parte de ella un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos en línea patrimoniales de mi tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Ing. Santiago José Gavilanes Vásquez

DEDICATORIA

Este trabajo que lo he realizado se lo dedico a mis padres quienes me han sabido guiar con sus consejos sus palabras que me han hecho la persona que soy.

A mis hermanos que me han apoyado y han estado en todo momento junto a mí.

A mi esposa que ha sabido comprender mis horas de trabajo y darme su aliento.

A mi hijo Santiago Matías por ser la luz de la fuerza y por quien he logrado realizar este trabajo

Ing. Santiago Gavilanes Vásquez

AGRADECIMIENTO

Agradezco ante todo a Dios por la vida, por darme la fuerza necesaria para salir adelante.

A mis padres quienes con sus palabras y apoyo han sabido llevarme a culminar con mis estudios.

A mi esposa quien me ha dado todo su apoyo incondicional para terminar este trabajo, y en especial a mi hijo Santiago Matías quien mi fuerza para toda la vida.

A la UNIVERSIDAD TÉCNICA DE AMBATO, FACULTAD DE INGENIERÍA EN SISTEMAS, ya que en esta institución he logrado realizarme como profesional con sus conocimientos.

A todos quienes estuvieron durante mi carrera universitaria al Tutor Ingeniero Franklin Mayorga, por su trabajo y tiempo que dedicó para guiar este trabajo.

Ing. Santiago Gavilanes Vásquez

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

ÍNDICE DE CUADROS

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE ESTUDIOS DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES (II Edición)

"SEGURIDAD DE ACCESO AL SERVICIO DE INTERNET Y LOS ATAQUES CIBERNÉTICOS EN EL HOTEL CASINO EMPERADOR DE LA CIUDAD DE AMBATO"

Autor: Gavilanes Vásquez Santiago José
Tutor: Ing. Franklin Mayorga, M. Sc.

RESUMEN

La investigación sobre "**SEGURIDAD DE ACCESO AL SERVICIO DE INTERNET Y LOS ATAQUES CIBERNÉTICOS EN EL HOTEL CASINO EMPERADOR DE LA CIUDAD DE AMBATO**", tiene como objetivo general reflexionar sobre el estado actual y futuro posible de Seguridad Informática, que en realidad dentro de la empresa Emperador Hotel Casino se maneja de una manera muy relegada y que no se le da la importancia necesaria. También se intentará brindar un completo plan de estrategias y metodologías, que si bien no brindan la solución total, podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática dentro de la empresa.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta. Es por esto que a la empresa Emperador Hotel Casino se ha planteado la prevención de los daños y pérdidas que puede ocasionar el mal manejo de la información (datos).

INTRODUCCIÓN

La importancia del tema de Seguridad en el acceso a Internet dentro de Emperador Hotel Casino es de suma valía para brindar una atención al cliente excelente, y garantizar que los recursos informáticos de los mismos estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, y prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

El CAPÍTULO I, EL PROBLEMA contiene:

El planteamiento del problema de investigación con la contextualización tanto macro, meso y micro contextualización en las cuales se está dando a conocer al problema de manera general, particular y local.

De igual manera se trata de la relación Causa – Efecto con su análisis crítico.

La prognosis donde nos indica en un futuro si no se da una solución al problema.

La formulación del problema en sí, donde se realiza la pregunta al tema.

Las Interrogantes de la investigación tanto para las variables como para la propuesta.

La delimitación de la investigación en Campo, Área, Aspecto, Espacial y Temporal.

Las unidades de observación en que se enmarcará el problema.

La justificación donde se observa la importancia del problema, la factibilidad, el interés, beneficiarios de la investigación.

Los objetivos en que se enmarca el problema y el tema de investigación.

El CAPÍTULO II MARCO TEÓRICO contiene:

Los antecedentes de la investigación relacionados a las variables de investigación del tema.

La fundamentación teórica y legal que encierra al tema de investigación.

La constelación de Ideas, tanto de la variable independiente como la variable dependiente.

La hipótesis o pregunta directriz del problema.

El señalamiento de las variables Independiente y Dependiente.

El CAPÍTULO III METODOLOGÍA contiene:

El enfoque con su modalidad de investigación, los niveles o tipos de investigación del problema.

La población y muestra referente al lugar donde se realiza la investigación.

La operacionalización de variables Independiente y Dependiente, indicando las descripciones, dimensiones, ítems y técnicas e instrumentos a utilizarse.

El plan para la recolección de la información con el respectivo plan para procesar dicha información que se obtendrá.

El análisis e interpretación de los resultados cómo se realizará.

El CAPÍTULO IV MARCO ADMINISTRATIVO contiene:

El Marco Administrativo, donde están los recursos de la investigación. Estos recursos son: Humanos, materiales, económicos.

El cronograma de actividades de la investigación.

El CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES contiene:

las conclusiones del análisis realizado a la actualidad de la empresa con respecto al tema de seguridad.

Las propuesta recomendada para la mejora del estudio realizado en la empresa.

El CAPÍTULO VI LA PROPUESTA contiene:

Los datos informativos de la empresa.

Los antecedentes de la propuesta relacionados con el tema propuesto.

Justificación, objetivos de la propuesta del estudio realizado.

Factibilidades técnicas y económicas de la propuesta.

La propuesta para la mejora de la situación actual de la empresa.

Conclusiones y Recomendaciones de la propuesta

Las conclusiones de la propuesta realizada a la empresa respecto del tema.

Las recomendaciones de la propuesta para la empresa.

Finalmente se encuentra la Bibliografía consultada y los respectivos Anexos.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

Contextualización

Contextualización

El desarrollo tecnológico: Internet, comunicaciones móviles, banda ancha, satélites, microondas, está produciendo cambios significativos en la estructura económica y social, y en el conjunto de las relaciones sociales.

La información se ha convertido en el eje promotor de cambios sociales, económicos y culturales. El auge de las telecomunicaciones ha producido una transformación de las tecnologías de la información y de la comunicación, cuyo impacto ha afectado a todos los sectores de la economía y de la sociedad.

A nadie sorprende estar informado minuto a minuto, comunicarse con gente del otro lado del planeta, ver el video de una canción o trabajar en equipo sin estar en un mismo sitio.

Las empresas a nivel mundial de término medio, actualmente, tienen debido a su seguridad, un incidente al mes. Las grandes empresas, tienen aproximadamente uno cada semana.

Tres cuartas partes de las operaciones que informan de intrusiones en sus sistemas, han sido estimadas como las peores causas en incidencias de seguridad (incluso peor que infecciones por virus…)

Datos proporcionados por **DTI/PWC Information security breaches survey 2004** el 61% de las compañías necesita más de un día para recuperarse de sus peores fallos de sistema. Una cuarta parte de las empresas tienen fallos en sus sistemas de manera accidental. El robo de información y los actos de sabotajes, suelen cometerse de manera interna. Además, más de 1/3 de los fraudes financieros recientes fueron parcialmente causados por empleados.

Mientras que **National hi-tech crime unit survey 2003** el 42% de las compañías fueron víctimas de fraude en 2006. Una de cada tres compañías, admiten haber sido víctimas de daños intencionados en sus sistemas de información en los últimos 12 meses.

En Latinoamérica, hubo un incremento de 135% en el número de fraudes en línea y 80% de los casos de fraude del 2008 fueron mediante phishing.

Por este último método de fraude, han sido víctimas muchas personas en Ecuador, como el último caso reciente de un correo electrónico que llegó en muchas empresas de parte de servicios@pichincha.com. Debemos notar que el protocolo SMTP, el más usado para enviar correos electrónicos, permite especificar como dirección de origen a una dirección email de cualquier dominio, seguramente fue lo que se hizo en este caso.

Juan José Mena, Gerente de Programas de Adopción de Microsoft Ecuador, **el Phishing es uno de los delitos informáticos que más se dan en el país**. Los sabotajes desde dentro de la empresa, son mucho más difíciles de controlar, porque persona sabe toda la seguridad del sistema y puede violentarlo fácilmente, dice el especialista de Microsoft.

En el Ecuador después del phishing, se han registrado casos de manipulación de programas llamados caballos de troya, realizado por personas con conocimientos técnicos y son muy difíciles de descubrir. Los caballos de troya modifican los programas existentes en el sistema o inserta nuevos programas o procesos de forma encubierta para realizar acciones no autorizadas. Según Microsoft los delitos que le siguen son los ya conocidos virus informáticos.

Desde el 2007 según la Escuela Superior Politécnica del Litoral (ESPOL), se han reportado 51 casos que lastimosamente se los reporta como "otras denuncias". También en casos de compra en línea de páginas web locales se han reportado casos de fraude, donde los perjudicados envían el dinero y a cambio no reciben nada.

Hay ciertos castigos por delitos informáticos en el país como por ejemplo, si es información de seguridad nacional la multa seria entre $1000 a $1500 ó de 1 a 3 años de prisión; de 3 a 6 años de prisión por divulgación y utilización de manera fraudulenta de la información protegida, así como secretos industriales, con una multa de $2000 a $10000; de 6 a 9 años si la divulgación o utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización ilegítima de la información, la multa es de $2000 a $10000.

El problema central de la empresa Emperador Hotel Casino es la falta de una conexión inalámbrica dentro de sus instalaciones, la cual facilitará la comunicación mediante el servicio de internet de todos los clientes que pertenecen a la empresa. El servicio de internet inalámbrico ayudará a mejorar la atención al cliente debido a que actualmente se cuenta solo con conexión con cable dentro de cada habitación.

Con el servicio de internet mejorado se brindará una mejor cobertura y sin el molestoso uso de cables, con lo cual se expone a todos los clientes el gran servicio y el mejoramiento permanente de los servicios para su mejor estadía.

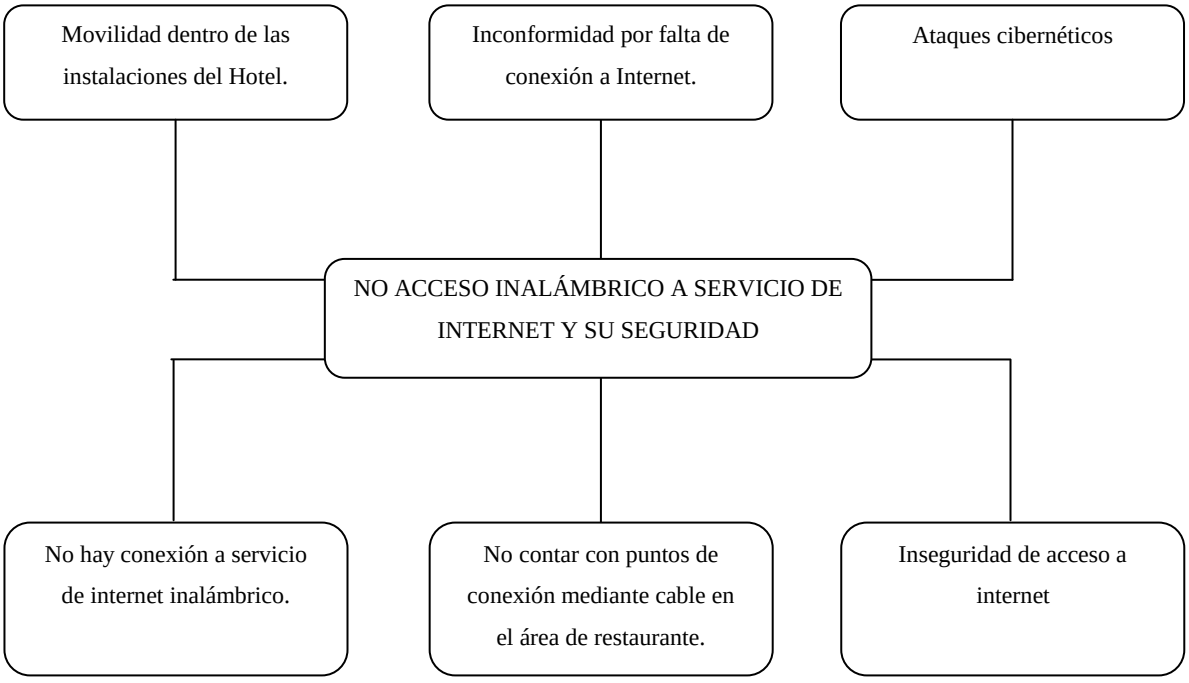
De igual manera al brindar el servicio de internet se debe brindar una seguridad en el acceso a dicho servicio tanto para los clientes como para la empresa Emperador Hotel Casino, para evitar cualquier tipo de ataque cibernético.

El porcentaje de ocupación diario es del 79.36%, lo que representa 50 habitaciones ocupadas. De las habitaciones ocupadas un 60% utilizan el servicio de conexión a internet (cableado).

Las horas de mayor conectividad son en la noche a partir de las 20h00, con un 60%, un 25% en la mañana y 25% a medio día.

Árbol de Problemas

EFECTOS



CAUSAS

Gráfico No. 1 Relación Causa – Efecto

Análisis Crítico

El acceso al servicio de Internet de huéspedes en Emperador Hotel Casino se lo realiza actualmente mediante cable y sin ninguna seguridad en el ingreso de usuarios a la red, es decir, el acceso a la red de Emperador Hotel Casino no tiene ninguna configuración de seguridad para el acceso a la misma y para el huésped es molestoso el conectarse estáticamente (mediante cable), sin poder movilizarse dentro del hotel.

De mantener este proceso actual, el malestar de los huéspedes les motivaría a buscar otras alternativas de hospedaje, para lo cual se ha visto la necesidad realizar un análisis técnico en el cual consta el problema del servicio de internet con conexión mediante cable y el problema de seguridad al acceder al servidor de Emperador Hotel Casino; con este análisis se diseñará una propuesta para una red inalámbrica con servicio de internet para el edificio de Emperador Hotel Casino con su respectiva seguridad de acceso a este.

Por el tema de seguridad se podrían dar ciertos ataques al servidor de internet de Emperador Hotel Casino, con lo cual se presentarían diferentes problemas como:

- Riesgo de daños o pérdida de información.
- Dificultad en el acceso a la red, por diferentes configuraciones de red.
- Lentitud en el servicio de internet.
- Ataques al servidor de internet.
- Daños a usuarios de red, perjudicando el servicio.

El acceso a esta red para poder obtener el servicio de internet debe ser mediante el ingreso de un usuario con su respectivo password, para así poder llevar el control de acceso y tener la red libre de ataques en especial al servidor de internet.

Prognosis

El no contar a futuro con una red inalámbrica en Emperador Hotel Casino traería problemas para obtener resultados en el mejoramiento de servicio al cliente de todos quienes realizan su visita a las instalaciones de la empresa. La falta de una red inalámbrica, deterioraría la calidad de servicio hacia los clientes que frecuentan las instalaciones de Emperador Hotel Casino, los clientes que más suelen visitar las instalaciones siempre están necesitados de movilidad, desplazamiento y flexibilidad para conectarse a internet.

La inexistencia de una red inalámbrica con seguridad daría serios inconvenientes en el servicio para eventos que se realizan dentro de las instalaciones de Emperador Hotel Casino afectando directamente a videoconferencias, compartir recursos (impresoras, archivos), internet.

La problemática de no contar con una red inalámbrica con seguridad atraería los ataques cibernéticos tanto a clientes que frecuentarían el acceso a internet, como el mismo servidor de internet de Emperador Hotel Casino.

Formulación del Problema

¿Cómo influye la seguridad de acceso a internet en los ataques cibernéticos en Emperador Hotel Casino, de la ciudad de Ambato?

Interrogantes de la Investigación

- ¿Cuál es el nivel de seguridad de acceso a internet que tiene Emperador Hotel Casino?
- ¿Qué ataques cibernéticos han ocurrido en Emperador Hotel Casino?
- ¿Existen alternativas para solucionar el problema de conexión de internet y su seguridad?

Delimitación de la Investigación

Área de estudio:	Ingeniería
ÁREA:	Sistemas
CAMPO:	Sistemas
ESPACIO:	Empresa hotelera EMPERADOR HOTEL CASINO
TIEMPO:	Primer trimestre del año 2010.

Delimitación espacial

La investigación se realizará en la empresa hotelera Emperador Hotel Casino, ubicada en la Av. Cevallos y Lalama esquina, del cantón Ambato provincia de Tungurahua.

Delimitación Temporal

El análisis se llevará a cabo en un periodo de tres meses del año 2010.

Unidades de observación

- Gerencia General
- Gerencia Hotel
- Jefe de Recepción
- Departamento de Sistemas
- Clientes (huéspedes, particulares)

Justificación

El presente proyecto se justifica por el interés que tiene la empresa hotelera Emperador Hotel Casino mediante el Departamento de Sistemas en mejorar el servicio al cliente brindándole un acceso a Internet con mayor comodidad, movilidad y flexibilidad.

Hoy en día las empresas hoteleras necesitan un flujo de clientes constante para que les permita hacerles frente a la intensa competencia a las que están sometidas en un ambiente de globalización para enrumbar la entidad al logro de sus objetivos.

La magnitud del servicio al cliente es incalculable, ya que aquellas empresas que cuentan con la mayor cantidad y calidad, podrán mejorar la captación de clientes.
Las empresas hoteleras en la actualidad se encuentran vulnerables debido al cambio que manifiestan los mercados y los competidores, pues la competitividad es cada vez mayor, y en algunos casos los resultados son desfavorables, ante esta situación las empresas hoteleras modernas han incorporado a su estructura el mejoramiento de servicios que brindan a sus clientes, para actuar ante los retos que impone el mercado.

Objetivos

Objetivo General

Establecer la seguridad de acceso a Internet para evitar ataques cibernéticos en Emperador Hotel Casino de la ciudad de Ambato.

Objetivos Específicos:

- Determinar el nivel de seguridad de acceso a Internet en Emperador Hotel Casino.
- Cuantificar los ataques cibernéticos que se presentan en Emperador Hotel Casino.
- Proponer una alternativa de solución al problema de falta de acceso inalámbrico a servicio de Internet y seguridad en Emperador Hotel Casino.

CAPITULO II

MARCO TEÓRICO

Antecedentes de Investigación

Para realizar esta investigación se tomará como referencia monografías, tesis, linkografía, que tengan relación con el presente tema, además de la documentación proporcionada por el Departamento de Sistemas y Departamento de Recepción de la empresa. (Porcentajes de ocupación, encuestas de servicio; Departamento de Recepción).

Fundamentaciones

Fundamentación Filosófica

Este trabajo se orienta mediante un enfoque dialéctico, puestos que no se inclina ni al enfoque materialista ni al idealista.

No.	PARADIGMAS ASPECTOS	CRITICO PROPOSITIVO
1	Finalidad de la Investigación	Comprensión Identificación de Potencialidades Acción social emancipadora
2	Visión de la realidad	Existen múltiples realidades socialmente construidas
3	Relación sujeto-objeto del conocimiento	Interacción transformadora

Cuadro No. 1: Paradigmas Filosóficos

Cuadro No. 1. (cont.)

4	Papel de los valores	Investigación comprometida e influida por valores
5	Generalización científica	Explicaciones contextualizadas
6	Metodología	Hermenéutica - dialéctica
7	Diseño de Investigación	Participativo Abierto, flexible, nunca acabado
8	Énfasis en el análisis	Cuantitativo

La fundamentación filosófica se encuentra enmarcada dentro del paradigma crítico pro positivo.

Debido que se fundamenta en la realidad, es decir, accede a los cambios con la intención de perfeccionar los procesos de una dinámica orientada al cambio. Es factible establecer métodos, técnicas y procedimientos que sean aptos de proveer información adecuada y oportuna para ser mejores.

Fundamentación teórica

Internet

Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

El acceso a Internet

Lógicamente el primer paso para entrar en Internet es disponer de **acceso a la red**. Internet es una red de ordenadores y como tal nuestra empresa deberá conectar los

ordenadores a esta red cuando queramos acceder a ella. Y si lo que deseamos es que terceros accedan a nuestra empresa deberemos tener al menos un ordenador permanentemente conectado a Internet.

Los **proveedores de acceso y de servicios de Internet proporcionan cuentas de conexión**, ya sean conectándose bajo demanda o permaneciendo conectada la red de forma permanente.

En función del uso que queramos que nuestra empresa haga de Internet una conexión por modem es suficiente. Si deseamos o necesitamos hacer un uso intensivo de Internet deberemos contratar una conexión permanente de calidad suficiente (p.e. RDSI o por cable).

Servidor

Un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Proxy

Es un servicio que brinda una computadora, ya sea cliente o servidor (como se desee implementar) con el fin de interponerse entre nosotros y la computadora a la que deseemos conectarnos, mandar información o visitar, a su vez se puede establecer que sirve como pasarela para llegar a un lugar. En la actualidad un proxy no solo puede servir como pasarela, sino que puede ser un buen firewall que se interpone entre nosotros y puede tomar una decisión (dependiendo su configuración) para poder hacernos llegar al destino o no, y lo mismo viceversa.

Existen dos tipos de proxys, los proxys que se especializan en recibir y contestar peticiones del tipo web y del tipo información, que sirven para transportar información de un sitio a otro. Esto con sus respectivas limitaciones que vendría

conformando una forma de filtro para saber qué información podrá pasar por alto y cual no.

A diferencia de un navegador normal, los proxys utilizan un puerto adicional (distinto al 80, puerto de Internet), por donde se manejarán para pasar información y determinan la forma en que se contestará, claro está, dependiendo el tipo de servicio que se proporcione por el proxy.

Un Proxy es una buena barrera de protección a nivel website (enviar páginas web) y nivel acceso a recursos compartidos de forma anónima o utilizando una sola dirección IP como salida.

Proxy web

Los proxy web son aplicaciones que proporcionan servicio de filtraje de sitios web, son utilizados para poder filtrar cierto contenido permitido por la configuración que se le haya dado al servidor proxy web. El filtro actúa conforme a un conjunto de cadenas de caracteres que deseemos omitir, en dado caso nos regula el tipo de páginas que se podrán visualizar y se delimita al usuario el acceso a sitios web restringidos, o bien, que el proxy web tenga configurado apto para el usuario.

Un proxy web tiene un uso mayor bajo instituciones educativas donde se proporciona acceso a internet de forma "libre", de esta forma se controla el acceso a las páginas los alumnos entran, poniendo reglas donde no se permitan contenidos del tipo pornográfico, hacking, contenido no educativo o cualquier cosa que genere tráfico inútil en la red.

La configuración de un proxy no es solo para delimitar contenido dentro de una consulta a sitios web, sino también genera registros de acceso a sitios donde es casi imposible obtener información sobre sus contenidos, es decir que es imposible realizar las comparaciones de los filtros/reglas establecidas

previamente. En base a ese registro el administrador puede visualizar las páginas con mayor acceso por los usuarios y poder tomar una decisión determinante conforme al contenido que se muestra en dicho sitio web con mayor acceso.

El funcionamiento de un proxy web es el siguiente:

1. El usuario pide al servidor una consulta de visualización de página web.
2. El servidor realiza la consulta al sitio web y espera que se le devuelva como respuesta dicha página.
3. El servidor pasa por un filtro el contenido de la página que se le dio como respuesta y toma una decisión.
4. Si el contenido fue aceptado por el servidor, la página es visualizada. En caso contrario se muestra el mensaje que se configure, este puede ser: "Página no encontrada" o "Página censurada".

Como forma dinámica, el servidor proxy web también resguarda las cookies sobre consultas a páginas web ya realizadas por otros usuarios de la red, en caso que otro usuario consulte el mismo web que otro, el servidor proxy web no perderá tiempo ni recursos de la red para enviar una petición de pagina web, sino que de forma automática le envía al usuario el contenido del sitio web o en su defecto la censuración de dicha pagina. Este método es muy recomendable para evitar saturación o uso inútil de la red cuando los usuarios desean realizar peticiones o consultas a sitios web iguales.

Por el lado de la privacidad y seguridad, un proxy web no solo sirve tanto para filtrar, delimitar, sino que a su vez puede estar configurado de dos maneras:

a) Anónimo. El servidor proxy web enviará peticiones de páginas web y ocultará la dirección IP de la máquina cliente que realizó la consulta al servidor proxy y este a su vez al sitio web. Este método resguarda la identidad (dirección IP) del cliente.
b) No anónimo. El servidor proxy web enviará la petición de la página web y

cuando el sitio web desee obtener información de la máquina que lo está consultando, el servidor proxy web contestará con los datos de la dirección del cliente que realizó la petición original. Este método tiene la desventaja de no resguardar la privacidad del cliente.

Tanto el modo anónimo y no anónimo, proporcionan un servicio rápido y confiable cuando el Servidor proxy web tiene con anterioridad el contenido de dicho web solicitado. El gráfico 2 muestra un mejor ejemplo.

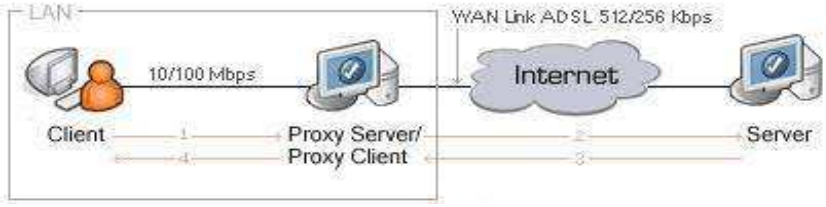


Gráfico 2: Ilustración de Proxy Web.

Proxy Server

Los proxy server son de forma parecida al proxy Web, solo que el proxy Web se enfoca al servicio de página web, los proxy server no solo pueden alimentar el servicio de páginas web, sino que también sirven para proporcionar más recursos a los que se deseen acceder o conectar otro cliente de la red, de esta forma poder realizar una respuesta más rápida a un recurso ya solicitado con anterioridad.

Los proxy server son intermediario entre el cliente e Internet, y sirven para cuando dentro de la red solo se cuenta con una dirección a Internet para salir, y todas las aplicaciones o recursos que requiere obtener están en una computadora fuera de la compañía o bien dentro de ella, el servidor proxy puede alimentar las peticiones y permitir acceso a Internet a los equipos con una sola conexión

Las ventajas de un servidor proxy es que puede limitar los accesos a Internet a los clientes deseados y solo dar acceso a los que se configuren aptos para este servicio, así mismo se puede denegar la ejecución de aplicaciones que requieren

conectar a otros servidores, ejemplo claro es: MSN Messenger, un proxy server puede denegar el acceso hacia Internet a aplicaciones previamente establecidas.

El ahorro de trabajo de carga en los clientes disminuye, ya que se puede utilizar como almacenador de datos, los cuales van a ser llamados por la aplicación directamente al proxy server. Esto sin ocupar recursos del cliente y dejando más recursos para trabajar con otras aplicaciones.

Así como el proxy server realice las tareas más pesadas, esto puede ser contrario a lo que se desea obtener, ya que el exceso de trabajo realizado, o bien la carga de peticiones en la red y procesamiento de datos pueden disminuir el rendimiento del mismo proxy server. El gráfico 3 ilustra la explicación.

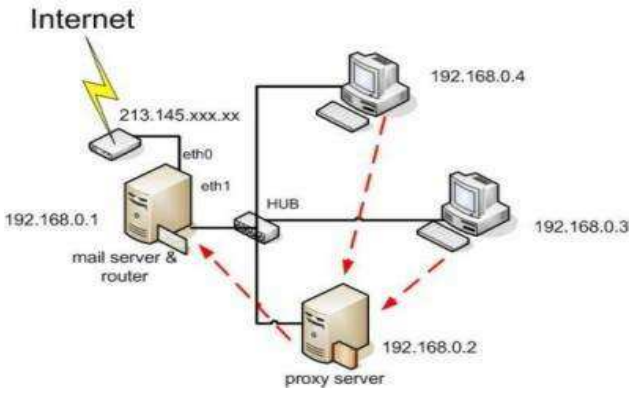


Gráfico 3: Proxy Server con servicio variado.

Routers y enrutamiento

El router es un dispositivo de hardware utilizado para la comunicación entre: routers y/o hosts. A diferencia de los otros dispositivos de hardware para redes el router posee las siguientes características:

- ✓ Entrada WAN para el servicio de Internet y posteriormente los equipos conectados serán capaces de acceder a dicho servicio, esto también dependiendo de la configuración que tenga el router.
- ✓ Entrada LAN, consiste en un número específico de puertos Ethernet

para la conexión de los clientes.

- ✓ Panel de configuración del router, el administrador podrá configurar o limitar los servicios a como sea necesario.
- ✓ Firewall incluido, la mayoría de los routers poseen su propio firewall en donde se puede configurar equipos de forma particular o bien zonas desmilitarizadas (DMZ).
- ✓ Posee una tabla de enrutamiento, mostrando los equipos que se encuentran activos o pasivos en la red.
- ✓ Log de conexiones y desconexiones como estadísticas para un mayor conocimiento sobre equipos que están trabajando o acceden al router de una u otra forma.
- ✓ Configuraciones de administrador para implementar puentes de red hacia otros puntos.

En el gráfico 4 se puede apreciar un router para un mejor conocimiento.

Gráfico 4: Descripción de Router D-Link.

El enrutamiento es la forma en que se transportará un paquete de un nodo a otro dentro o fuera de la red. La tarea principal es tomar el paquete a enrutar, encapsularlo dentro del router utilizando el protocolo de ruteo que se requiera y

realizar el envío del paquete al equipo o bien al router siguiente.

El fin de la comunicación entre routers es para actualizar sus tablas de direcciones según los equipos que se tenga en cada LAN, de este modo utilizando algún protocolo de enrutamiento se realizan los envíos de paquetes de forma más directa, tratando de evitar contratiempos o peticiones de búsqueda en otros puntos de la red.

Existen dos tipos de enrutamiento para lograr acabo la actualización de tablas de ruteo entre routers, estos son:

1. Ruteo estático. El administrador debe actualizar su propia lista de direcciones cada vez que la topología de la red o los equipos conectados al routers cambien, así mismo el modo estático especifica que los equipos se conectarán mediante una dirección IP estática, la cual debe ser establecida a su vez por el administrador. Esto resulta muy difícil si la red fuese muy amplia y estuviera en crecimiento constante, pero es una buena técnica para preservar la seguridad y saber el conocimiento exacto de equipos conectados y que se pueden conectar a la red, en base a esto poder realizar análisis de fallos en busca de problemas dentro de la red.

2. Ruteo dinámico. El administrador configura el router para que actualice su tabla de enrutamiento de forma automática, de este modo los equipos pueden obtener su dirección IP de forma automática (DHCP) sin problema alguno. Este método es muy eficaz y evita contratiempos en caso que la red estuviese en crecimiento constante, pero reduce el rendimiento de la red ya que el router realizará trabajo extra al realizar actualizaciones constantemente.

Una vez especificada la forma de enrutamiento se continúa con la configuración del tipo de protocolo para el ruteo de paquetes en la red. Los tipos de protocolos para el enrutamiento son:

- ✓ **RIP ::** Protocolo de Ruteamiento por Vector Distancia. Determina la dirección (vector) y la distancia a cualquier enlace de la red.

- ✓ **IGRP ::** Protocolo de Ruteamiento de Gateway Interior. Protocolo de enrutamiento patentado por Cisco.

- ✓ **OSPF ::** Protocolo de Ruteamiento de Estado del Enlace. Obtención de la ruta más corta, recreando la topología de la red e implementando un algoritmo para la obtención de la ruta más corta.

- ✓ **EIGRP ::** Protocolo de Ruteamiento de Gateway Interior Mejorado. Combina aspectos de RIP y OSPF para determinar el envío del paquete, también patentado por Cisco.

En el gráfico 5 se ilustra un ejemplo.

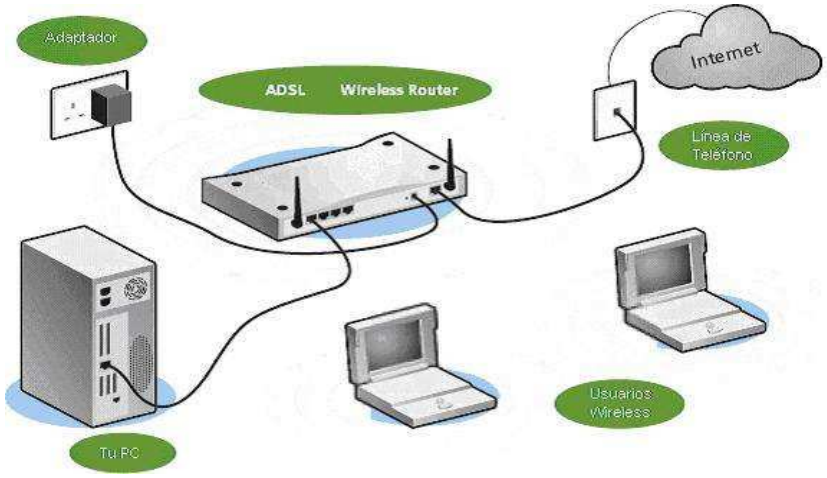


Gráfico 5: Ilustración de una red con utilización de Router.

NAT Y PAT

La NAT (Network Adress Traduction) que significa traducción de direcciones de red, permite el enmascaramiento de las direcciones IP bajo una única dirección IP, que sería la dirección asignada por el proveedor de servicio de Internet (ISP,

Proveedor del Servicio de Internet). Esto es de gran utilidad ya que permite salir a Internet con una única IP pública y tener la IP de la red Internet segura.

A continuación un ejemplo de 2 computadoras realizando una búsqueda en Google en la Cuadro 2:

IP Interna	Puerto Origen	IP Pública	Consultando a:	Datos
PC1 – 192.168.0.100	1010	200.107.40.193	google.com	????
PC1 – 192.168.0.101	1011	200.107.40.193	google.com	????

Cuadro 2. Búsqueda en Google

En el ejemplo se visualiza que tanto el equipo PC1 y PC2 realizan una misma consulta a google.com, enviando su consulta por el puerto 1010 y 1011 respectivamente, el servidor de Google recibe dos consultas de una misma dirección IP (200.107.40.193), y revisando la tabla NAT visualiza que son consultas realizadas por distintos puertos, el servidor de google.com contesta a la petición por el puerto donde se origino actualmente la consulta y de este modo varios equipos pueden realizar consultas al mismo servidor sin que este se confunda.

PAT (Port Adress Traduction) que significa traducción de direcciones de puerto, este se utiliza cuando más de un equipo realiza una consulta al mismo servidor, brinda la traducción del puerto a otro (cambiando el puerto de recepción), envía la consulta por un puerto y espera respuesta por otro puerto especificado en la tabla NAT, de esta forma se sigue preservando la dirección Interna del equipo, se realiza su petición y tanto el servidor como el router podrán dirigir los paquetes de un sitio a otro.

A continuación un ejemplo de implementación de PAT, cuando ambos equipos realizan consultas a un mismo servidor utilizando un mismo puerto.

IP Interna	Puerto Origen	PAT	IP Pública	Consultando a:	Datos
PC1 – 192.168.0.100	1010	1010	200.107.40.193	google.com	????
PC1 – 192.168.0.101	1010	1011	200.107.40.193	google.com	????

Cuadro 3. Implementación PAT

Al realizar la consulta y generar el paquete, el router realiza una revisión de la tabla NAT y se toma con la generación de dos paquetes que tienen un mismo puerto de origen y que van a una misma dirección IP (google.com), es aquí donde el router implementa PAT sobre la NAT, para traducir el puerto a un nuevo puerto, esto lo realiza modificando el paquete directamente y cambiando su puerta de origen a una nueva que encuentre disponible, este suceso se registra en su tabla NAT y envía la consulta.

Seguridad informática

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Historia y evolución de la seguridad informática

Los problemas de seguridad surgen desde antes de la interconexión de computadoras en los años 70’s y 80’s; estos problemas se remontan a los inicios del desarrollo de las máquinas de tiempo compartido, en donde se presentaban riesgos de acceso no autorizado y modificación de información. Previo a estos desarrollos, se hablaba de seguridad desde los inicios de la Segunda Guerra Mundial, donde surgieron los problemas de comunicación segura entre las diferentes tropas en misión; para solucionar estos problemas se empezó a hablar del cifrado de mensajes.

Aunque la seguridad computacional, realmente tuvo un auge importante cuando se conectaron los computadores entre sí para compartir información, poco a poco se conectaban mayor cantidad de equipos llegando a un crecimiento exponencial, que presentaban cada vez mayor riesgo para asegurar la información.

A continuación se describen algunos de los hechos históricos que han marcado los inicios y evolución de la seguridad informática:

A finales de los años 50 los computadores trabajaban con registros especiales para definir particiones en memoria para el uso de programas separados y asegurar que un programa en ejecución no pueda acceder a particiones de otro programa. La memoria virtual ofrece mecanismos que permiten proteger la información como si estuviese es su propia partición de memoria; las particiones y el concepto de memoria virtual proveen una de las primeras medidas de protección de seguridad en ambientes multi-usuarios.

A principios de los años 60, los sistemas de tiempo compartido proveían almacenamiento de información a usuarios individuales. Este sistema fue seguro usando control de acceso, que permitía al dueño de la información, especificar y autorizar accesos a otros diferentes usuarios. La primera característica de la seguridad fue la protección de contraseñas de usuarios, en donde los sistemas de autenticación codificaban la imagen de éstas.

En 1968 el sistema Multics del MIT, presentó algunas características de seguridad y privacidad, donde se prestó mucha atención a identificar un pequeño kernel en el sistema operativo, que garantizara que todas las políticas de seguridad del sistema fueran permitidas.

En 1969, vino la aparición de ARPANET (Advanced Research Project Agency Network) comenzando con cuatro nodos, hasta convertirse en lo que es hoy en día Internet. Este continuo aumento de interconexiones, incrementó el riesgo de acceso a usuarios externos no autorizados y asimismo, el conocimiento sobre

temas de seguridad a los administradores y propietarios de las redes.

El Unix-Unix System Mail (UUCP) en 1975 permitía a usuarios Unix ejecutar comandos en un sistema Unix secundario. Este permitía que, correos electrónicos y archivos fuesen transferidos automáticamente entre sistemas, lo que también permitía a los atacantes borrar o sobre escribir los archivos de configuración. Como no había una administración central del UUCP en la red, el ARPANET hizo un acercamiento al control de los problemas de seguridad que no se aplicaban. En los siguientes años se empezó a hablar sobre criptografía con llave pública y firmas digitales, debido a la necesidad de permitir comunicación confidencial entre dos usuarios. Esto ha generado que la criptografía sea un tema importante en el desarrollo de la seguridad informática.

En 1978 (Morris y Thompson) se realizó un estudio que demostraba que adivinar contraseñas a partir de datos personales de los usuarios, como son el nombre, teléfono, fecha de nacimiento, era más eficiente que decodificar las imágenes de dichas contraseñas. Estos fueron los primeros pasos de la ingeniería social, dentro del área de seguridad informática, y en donde evolucionan así mismo, los principios de la misma, y en específico, la confidencialidad.

En el mismo año nace una nueva preocupación de la seguridad informática, que consiste en la protección de los pagos electrónicos a través de la red que comenzaron a hacerse disponibles a los clientes. Este tipo de transacciones se tradujo en la necesidad de un alto nivel de seguridad, evolucionando así los conceptos de confidencialidad e integridad.

El crecimiento exponencial de la red, comenzó a requerir un DNS (Directory Name Server) dinámico, que actualizara la base de datos de asociación de nombres y direcciones. Estos nuevos servidores se convierten en otro blanco para los atacantes y suplantadores. Los virus informáticos tienen un crecimiento notable y se convierten en una seria amenaza para los administradores de seguridad informática y para los usuarios.

En 1988, se destaca el primer ataque a gran escala, a través de gusanos cibernéticos, que podrían llegar a infectar en horas un porcentaje significativo de la red. Este hecho permite reconocer las vulnerabilidades que se tienen en la red.

La seguridad encuentra otro interés profundo en los años previos a 1993, donde los atacantes utilizan métodos de sniffing (rastreo) para detectar contraseñas, y spoofing (suplantación) o usan los mismos computadores con identificadores falsos para transmitir sus propios paquetes al ganar accesos al sistema.

A raíz de dicho crecimiento de las redes, se comenzaron a presentar abusos computacionales causados por los mismos usuarios. Estos abusos se pueden clasificar en: robo de recursos computacionales, interrupción de servicio, divulgación no autorizada de información y modificación no autorizada de información. A partir de estos abusos, y a partir de la evolución de los principios de la seguridad informática a través del tiempo, hoy en día se tiene un modelo actual basado en dichos principios de confidencialidad, integridad y disponibilidad, que buscan proteger la información, recursos y personas que hacen uso de esta, tratando así de evitar el continuo crecimiento a dichos abusos. Dichos principios han ido evolucionando a través del tiempo, lo que no significa que hayan surgido solo hasta esta época.

Se pueden definir además seis clases de abusos técnicos por los que debe preocuparse la seguridad informática: Errores humanos, abuso de usuarios autorizados, exploración directa, exploración con software especializado, penetración directa, mecanismos de subversión de seguridad.

En el caso de errores humanos, son simples errores cometidos por los usuarios que pueden llegar a representar grandes daños al sistema. El abuso de usuarios autorizados, se refiere a los abusos que hacen los usuarios al entregarles demasiada confianza o privilegios sobre algún sistema. La exploración directa, se presenta cuando el usuario ingresa teniendo autorización, pero sin ser previsto por los operadores del sistema. Por su parte, la exploración con software

especializado, consiste en exploraciones en donde se hace uso de herramientas especializadas para acceder a recursos no autorizados o generar irregularidades en los sistemas. Algunos de estos software empleados son: los troyanos que son ocultados en aplicaciones comunes y comerciales, los virus que tienen la capacidad de reproducirse, las bombas de tiempo, entre otros. Ahora bien, en la penetración directa, a diferencia de la exploración directa, no se tiene autorización, pero los intrusos encuentran alguna falla o vulnerabilidad, y generan algún tipo de código malicioso para explotarla y obtener el control del sistema. Por último en los mecanismos de subversión de seguridad, se ataca el control interno para entrar sin autorización a un sistema, sin ser detectado.

Hoy en día, y con el paso del tiempo, los avances tecnológicos y la investigación, la seguridad informática ha venido estructurándose de manera tal que se ha convertido en un arte y ciencia, con principios fundamentales y una importante cantidad de teoría en todos sus aspectos.

Con esta historia, como base literaria de la investigación, se busca entonces, comprender la evolución de los objetivos y principios de la seguridad informática vigentes en los modelos actuales, para aplicarlos y tenerlos como base para el desarrollo de la guía metodológica.

Conceptos y modelo actual de la seguridad informática

La Seguridad Informática ha sido uno de los temas más mencionados en la literatura en la última década, debido a su dinamismo y constantes cambios e innovaciones. Todo sistema es desarrollado y cambiado varias veces a lo largo de su ciclo de vida, debido a nuevas funcionalidades que son adicionadas, políticas, mejoras, etc. Todos estos cambios y nuevas funcionalidades alteran los requerimientos de seguridad de los sistemas, y obligan a una reevaluación de éstos, para lograr una revaloración de las nuevas vulnerabilidades y debilidades del nuevo sistema o sistema modificado, y así implementar soluciones ante estos nuevos requerimientos.

Junto a estos grandes cambios que actualmente atañen a todas las organizaciones, han venido surgiendo cada vez más retos, que se convierten no sólo en un problema tecnológico sino también en un problema cultural de dichas organizaciones; y entre dichos desafíos se encuentra la seguridad informática, o también caracterizada como, Seguridad de Tecnología de Información (Seguridad de TI), punto a discutir en la presente sección.

Objetivo de la Seguridad Informática

Los continuos desafíos de la seguridad informática que han venido surgiendo, han llevado a esta área a definir metas y propósitos, los cuales han sido resumidos en su objetivo principal, y que permite hacer un acercamiento al cumplimiento de los nuevos y cambiantes retos. Es así como la Seguridad Informática busca dar apoyo a los objetivos y misión de las organizaciones, a través de la protección de sus principales recursos y activos: la información, la tecnología que la soporta (hardware y software) y las personas que la utilizan y/o conocen, a través de la selección y aplicación de protecciones adecuadas, manteniendo así, el debido cuidado de sus recursos físicos, financieros, reputación, y otros activos tangibles e intangibles.

Para el cumplimiento de dicho objetivo, la Seguridad Informática ha definido tres principios básicos (confidencialidad, integridad y disponibilidad) y 4 servicios (autenticación, autorización, no repudio y auditabilidad), los cuales serán detallados en secciones posteriores.

Desafortunadamente, la Seguridad Informática algunas veces ha sido vista, no sólo como una fuente de gastos y grandes inversiones [WILS03], sino como un obstáculo para la misión de la organización, debido a la imposición de reglas, procedimientos y protecciones mal seleccionadas, que llegan a ser molestos para los usuarios, administradores, y para los mismos sistemas y su respectiva administración.

Sin embargo, al procurar una buena administración de la Seguridad Informática, y hacer una adecuada selección de procedimientos, reglas y protecciones, puestas en su debido lugar, se dará apoyo a la organización al cumplimiento de su misión.

Principios de la Seguridad Informática

Al ser la protección de los activos, uno de los objetivos principales de la seguridad informática, esto significa mantenerlos seguros frente a las diversas amenazas a las que se enfrentan y que pueden afectar su funcionalidad de diferentes maneras: corrupción, acceso indebido e incluso hurto y eliminación, la Seguridad Informática se basa en la preservación de unos principios básicos, los cuales son enumerados y definidos por diferentes autores, con algunas variantes y algunas constantes. Cada uno de dichos principios tiene un propósito específico dentro del marco del objetivo de la seguridad informática. Para el desarrollo de esta investigación, se definen los siguientes principios básicos:

Confidencialidad

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos.

La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, es decir en los sistemas y dispositivos en los que reside dentro la red, como durante su procesamiento y tránsito, hasta llegar a su destino final.

Integridad

La integridad tiene como propósito principal, garantizar que la información no sea modificada o alterada en su contenido por sujetos no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos. Debido a esto, la integridad como principio de la Seguridad Informática, se ha definido en dos partes: integridad de los datos e integridad de los sistemas.

La integridad de los datos, se refiere a que la información y los programas solo deben ser modificados de manera autorizada por las personas indicadas para ello. Estas alteraciones pueden darse por inserciones, sustituciones o eliminaciones de contenido de la información.

Por su parte, la integridad de los sistemas, hace referencia a que todo sistema debe poder cumplir su función a cabalidad, sin ninguna violación o modificación del mismo, en su estructura física y/o lógica, sin perder necesariamente su disponibilidad.

Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Al referirse a los sistemas que soportan la información, se trata de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información.

Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes.

Se han presentado varias interpretaciones y discusiones alrededor de los principios de integridad y confidencialidad; dichas discusiones radican en la pertinencia de dichos principios a los sistemas que soportan la información. Algunos autores argumentan que la confidencialidad y la integridad conciernen únicamente a la información, mientras que la disponibilidad atañe a la información y a los sistemas que la soportan.

Mientras que otros, plantean la integridad y la disponibilidad como principios relativos a dichos sistemas que soportan la información. En la presente investigación se tienen en cuenta los dos principios mencionados anteriormente, como fundamentales para los sistemas que soportan la información, debido a que la violación de la integridad de un sistema, física o lógicamente, no significa necesariamente su pérdida de disponibilidad, aunque de forma contraria, la falta de disponibilidad de un sistema, posiblemente puede estar ligada a una violación previa de su integridad, ya sea en su estructura física o lógica.

En conclusión, disponibilidad, integridad y confidencialidad son principios básicos de la seguridad informática, y su adecuada comprensión es necesaria en esta investigación, para la correcta identificación de problemas y las soluciones apropiadas a ellos a través de la administración de la seguridad, con el objetivo de calcular el retorno a la inversión sobre dichas soluciones.

Servicios de la Seguridad Informática

Para lograr hacer cumplir la preservación y el cumplimiento de los tres principios básicos de la seguridad informática, discutidos anteriormente, se han planteado cuatro servicios principales, que sirven como base para la implementación de una infraestructura de seguridad de TI en una organización.

Autenticación

Este servicio busca asegurar la validez de una identificación proporcionada para

acceder cierta información, proveyendo medios para verificar la identidad de un sujeto, básicamente, de tres formas: por algo que el sujeto es, por algo que el sujeto tiene o por algo que el sujeto conoce.

Autorización

El servicio de autorización permite la especificación y continua administración de las acciones permitidas por ciertos sujetos, para el acceso, modificación o inserción de información de un sistema, principalmente, mediante permisos de acceso sobre los mismos.

No repudio

La administración de un sistema de información debe estar en capacidad de asegurar quién o quiénes son los remitentes y destinatarios de cualquier información. Es por esto que este servicio provee los medios y mecanismos para poder identificar quien ha llevado a cabo una o varias acciones en un sistema, para que los usuarios no puedan negar las responsabilidades de las acciones que han llevado a cabo.

Auditabilidad

Este servicio proporciona los mecanismos para la detección y recuperación ante posibles fallas o incidentes de seguridad, mediante el registro de todos los eventos y acciones hechas en un sistema.

Definición de Seguridad Informática

Luego de comprender los objetivos principales y los principios básicos de la seguridad informática, ésta se puede definir como, la definición y posterior implementación de protecciones, políticas y procedimientos, en búsqueda de la preservación de la integridad, disponibilidad y confidencialidad de la información,

los recursos que la soportan (hardware, software, firmware, dispositivos de comunicación) y los individuos que la utilizan o conocen.

Para llegar a cumplir los principios de la seguridad informática y lograr un buen funcionamiento de sus servicios, se debe tener una buena base de administración de los recursos, tanto tecnológicos como humanos, así como la información y los procesos que la seguridad busca proteger, tratando de llevar un manejo eficiente y eficaz de dichos recursos. En el siguiente capítulo, se presentarán los conceptos generales de la administración de la seguridad informática, y cómo ésta apoya los procesos de seguridad informática en una organización.

Administración de la seguridad informática

Diariamente se escucha en varios medios (periódicos, televisión, Internet, foros de discusión, reportes de fabricantes de productos y proveedores de servicios, etc.) acerca de incidentes de seguridad informática, como ataques de virus que causan pérdidas y daños que pueden llegar a representar grandes sumas de dinero para una organización, ataques remotos de hackers a instituciones financieras, ataques a los sitios Web de grandes y prestigiosas empresas y corporaciones, etc. Este tipo de incidentes son los que hacen cada vez más interesante la seguridad informática, pero así mismo significa tareas y responsabilidades diarias de esta área para prevenir ataques como los antes mencionados. Es por esto que la administración de la seguridad informática es uno de los temas más importantes en la estructura de seguridad informática de una organización.

Administrar la Seguridad Informática de una organización, es un trabajo fundamental para conservar confiables, los sistemas de la misma. La tarea de administración, comprende la administración de riesgos, definición, creación e implementación de políticas de seguridad, procedimientos, estándares, guías, clasificación de información, organización de la estructura de seguridad de la compañía, y la educación de los individuos de la organización, entre otras.

Como se mencionó en la sección anterior, la clave de un programa de seguridad informática, es la protección de los activos más importantes de la compañía. Estos activos pueden ser identificados mediante los análisis de riesgos, además de la identificación de las vulnerabilidades y amenazas que pueden llegar a afectar dichos activos, y estimar los costos y daños que tendría para la compañía, la materialización de una o más de dichas amenazas. Como resultado de los análisis de riesgos se puede lograr tener un presupuesto de las inversiones necesarias para la protección de dichos activos, contra los riesgos anteriormente identificados, no solo en cosas materiales, sino también en implementación de políticas, educación del personal, desarrollo de guías o estándares, etc.

El administrador no es un simple observador de un sistema y de sus operaciones posteriores a su instalación. Esta labor también incluye tareas previas de la instalación del sistema, tales como validar y estructurar las políticas de seguridad para el mismo, aunque esto no quiere decir que esta administración pertenece solo al área técnica, también tiene tareas administrativas como son la creación de políticas, hacer que se cumplan y actualizarlas cuando sea necesario.

La administración de seguridad debe tener en cuenta que el desarrollo y crecimiento de un sistema, las redes, etc., producen cambios constantes en las políticas de seguridad, en la protección de bienes y las amenazas establecidas, lo cual requiere también de una debida gestión y administración.

Una de las formas más utilizadas para hacer administración de la seguridad informática, se basa en la utilización de estándares. El crecimiento de las necesidades de gestión de la seguridad informática en las organizaciones, ha motivado la creación de estándares locales e internacionales para la administración de tecnología de información, y en particular la seguridad de dicha información, y todo lo que a ésta concierne.

La historia de los estándares se remonta a los inicios del siglo XX, con los primeros usos que se dieron a la electricidad; se comenzaron a desarrollar

entonces aplicaciones eléctricas bajo los primero estándares establecidos por la International Electronic Committee (IEC). Más adelante con el paso del tiempo, fue surgiendo la necesidad de nuevos y mejores estándares en más y más áreas del conocimiento, y así nació la International Organisation of Standarisation (ISO).

Pero no sólo existen estándares reconocidos internacionalmente, sino también han surgido estándares locales o nacionales, referentes a la administración de seguridad informática. La razón principal de la creación de estos estándares locales, radica en la casuística y especificidad que pueden llegar a tener las mejores prácticas en el área, en un país o región determinada.

Uno de los factores positivos de la existencia actual de los estándares, es la cantidad que hay de los mismos, ya que esto permite a una organización particular, acoplarse o acomodarse a uno de estos estándares, según sus características y necesidades, o en una situación determinada. Adicionalmente, otro punto a favor de las organizaciones gracias a los estándares, no sólo es el ahorro de recursos, tanto de dinero, como de personas y tiempo, en desarrollar estándares propios, sino que pueden utilizar estándares que han sido demostrados a partir de las mejores prácticas en el área, que para el caso de esta investigación, son las mejores prácticas en administración de la seguridad informática.

En dicha área, la administración de seguridad informática, existen varios estándares, nacionales e internacionales, que están orientados a ser una guía para las organizaciones en la formación y mantenimiento de la infraestructura de seguridad informática de las empresas. A continuación se listan algunos de los estándares más importantes que existen en el área:

- ✓ ISO/IEC 13335-1:2004 : Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
- ✓ ISO/IEC TR 13335-3:1998 : Information technology -- Guidelines for the

management of IT Security -- Part 3: Techniques for the management of IT Security

- ✓ ISO/IEC TR 13335-4:2000 : Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
- ✓ ISO/IEC TR 13335-5:2001 : Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
- ✓ ISO/IEC 17799:2005 : Information technology -- Security techniques -- Code of practice for information security management
- ✓ British Standard 7799 – BS7799
- ✓ Estándares publicados por NIST (National Institute of Standards and Technology)
- ✓ COBIT Security Baseline
- ✓ ISF Standard of Good Practice

Para lograr los objetivos de la administración de la seguridad informática, ésta se vale de controles que se utilizan para hacer cumplir las directivas que esta área ha fijado para la organización. Dichos controles se clasifican en: controles administrativos, controles técnicos y controles físicos. Los controles administrativos, hacen referencia al desarrollo y publicación de políticas, estándares, procedimientos, investigación del personal, entrenamiento y el cambio de los procedimientos de control.

Los controles técnicos, se refieren a los mecanismos de control de acceso, administración de recursos y contraseñas para su acceso, métodos de autenticación y autorización, dispositivos de seguridad, y la configuración de la infraestructura técnica de seguridad de la organización.

Los controles físicos corresponden a los controles físicos de acceso a diferentes locaciones de la organización, bloqueo de sistemas, monitoreo de los lugares críticos de almacenamiento y manejo de información, etc.

Dentro de la administración de la seguridad de la información, se deberían tener en cuenta las inversiones requeridas para el desarrollo de los procedimientos, políticas, estándares, etc., anteriormente mencionados, y para que dichas inversiones lleguen a retornar los beneficios o ganancias esperadas, se debería también conocer la forma de estimar las ganancias o posibles pérdidas de dichas inversiones. En la sección que se presenta a continuación, se expondrán algunas ideas y acercamientos planteados por diferentes autores acerca del cálculo del retorno de las inversiones en seguridad informática.

Red inalámbrica WLAN

Es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

Seguridad Inalámbrica

La seguridad inalámbrica es un punto importante que merece la atención debida, teniendo en cuenta que la utilización de equipos portátiles crea la necesidad de establecer un método de comunicación entre la red local (LAN) y la red inalámbrica, ya sea por cuestiones de trabajo, de diversión o personal.

Para la estructuración o implantación de una red inalámbrica es necesario considerar un concentrador para ser el punto de acceso (AP) y la implementación de un método de seguridad para tener un canal seguro en la comunicación, posteriormente un método de encriptación para proteger la información que viajará por el canal y así evitar miradas indiscretas a la información, equipos y posibles intentos de intrusión a las redes que se tengan interconectadas.

La seguridad inalámbrica se basa principalmente en los métodos de encriptación de la información utilizando algoritmos para resguardar los datos. Estos algoritmos son implementados por el método de seguridad utilizado (en este documento se describe el método de encriptación TKIP). Algunos algoritmos son:

- ✓ TKIP (Temporal Key Integrity Protocol). Genera claves temporales para evitar intrusiones mediante re-envío de mensajes y anida un código de integridad del mensaje para proteger la información y determinar su fidelidad.
- ✓ CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol).
- ✓ WRAP (Wireless Robust Authenticated Protocol).

Los métodos de seguridad para afianzar el canal son los encargados de asegurar la conexión entre el punto de acceso (AP) y el cliente conectado, de esta forma se previene de usuarios indeseados o que no estén dentro de la red inalámbrica, se mantiene una sincronización segura, los datos son confidenciales y están fuera del alcance de los intrusos y en caso que la red inalámbrica esté conectada a la red local, se mantiene la seguridad entre ambas redes. Los métodos de seguridad son:

- ✓ WEP (Wires Equivalent Privacy).

- ✓ WPA (Wi-Fi Privacy Access). Es una mejor de WEP, estableciendo un vector inicial de 48 bits, incorporación de encriptación por algoritmo TKIP. Pero WEP se puede implementar en dos modalidades que son:

    - ✓WPA-PSK (Wi-Fi Privacy Access-Pre-Shared Key). Estableciendo una Clave como método de acceso, pero siguiendo con los mismos procesos de encriptación de WPA. Este método es para facilitar el método de implementación de WPA.
    - ✓WPA-RADIUS (Wi-Fi Privacy Access – RADIUS). Este método es más complicado de implementar ya que requiere de un servidor

RADIUS el cual establecerá claves de acceso entre los AP y sus usuarios, de esta forma se tendrá una red inalámbrica aún más protegida, segura y administrable. Los métodos de encriptación son los establecidos en WPA, más los métodos de claves generadas por el servidor RADIUS y el usuario.

De esta forma combinando los métodos de encriptación que se tienen soportados y la seguridad que se implementara en la red inalámbrica, se tendrá un mejor resguardo de la información, otras redes locales y la tranquilidad que se estará trabajando en una conexión segura donde los datos o cualquier cosa que se transfiera estará asegurada, así que una buena elección y un buen montaje de seguridad en redes inalámbricas serán hincapié para alcanzar una mejor forma de trabajo sin robo de información o pérdida de confianza para desarrollo de proyectos privados.

Puntos de Acceso (AP)

Los Puntos de Acceso (AP-Access Points) son solo uno o varios dispositivos de hardware con capacidad de brindar servicio para redes inalámbricas. Estos dispositivos son concentradores de red como switch, hub o routers que permiten la intercomunicación entre redes, teniendo como principal característica una o un par de antenas que son las que se encargarán de enviar/recibir las ondas en alguno de los canales que posee o se tenga configurado en el concentrador.

Los puntos de acceso aparte de intercomunicar redes inalámbricas, también pueden comunicar la red LAN, ya que los concentradores inalámbricos también poseen entrada Ethernet para formar redes LAN, y así poder tener en constante comunicación ambas redes inalámbricas y LAN.
Existen delimitaciones en las redes inalámbricas, y éstas se basan principalmente en que un punto de acceso tiene un ancho determinado para la comunicación de las redes inalámbricas, de este modo el envío masivo de información o cualquier actividad que ocupe un ancho de banda, disminuirá el rendimiento y en algunos

casos la misma conectividad del punto de acceso con el equipo inalámbrico. Otro de los factores más comunes es la distancia del punto de acceso, este solo puede abarcar una distancia determinada, la cual está especificada o se rige mediante la potencia que posea la antena del concentrador. El gráfico 6 muestra un concentrador inalámbrico.

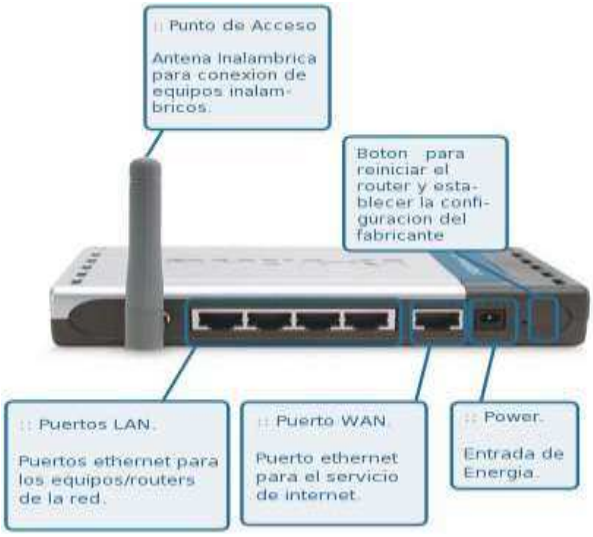


Gráfico 6. Descripción de Router D-Link para inalámbrica.

Protocolo de Aplicaciones Inalámbricas (WAP)

El protocolo de aplicaciones inalámbricas (WAP-Wireless Application Protocol) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo los accesos a Internet desde un teléfono móvil.

La tecnología WAP consiste en un entorno de aplicación y una pila de protocolos para aplicaciones y servicios accesible mediante terminales móviles (por ejemplo los celulares), esto permite que cualquier terminal móvil pueda tener acceso a servicios de manera limitante, ya que la tecnología telefónica ofrece grandes ventajas en sus equipos como serían: almacenamiento de información, pequeña cantidad de RAM para procesamiento, caché interna, todas sus características de manera limitada ya que esto se deriva por el tamaño y peso del equipo. Es por eso

que las tecnologías WAP permiten estandarizar los equipos y servicios para brindar a cualquier celular la mejor de las prestaciones conforme sean las capacidades del mismo equipo telefónico. Observar el gráfico 7.

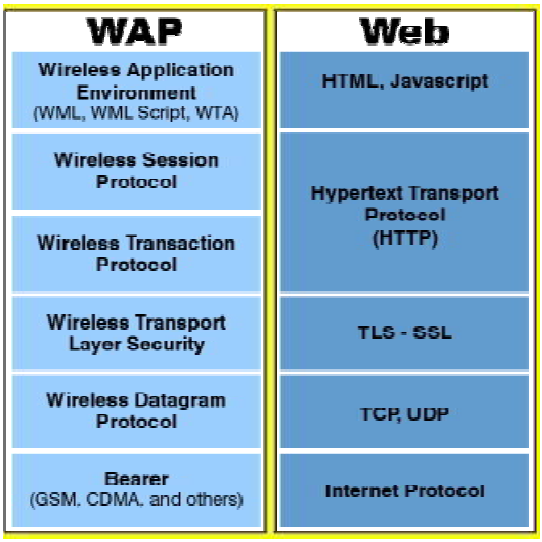


Gráfico 7. Pila de Protocolos WAP y WEB.

WAP en su versión 1 definida en 1999, mostró al mundo su lenguaje en el que se estandarizaba para proporcionar los distintos servicios a tecnologías móviles, éste tuvo como nombre WML (Wireless Markup Lenguage), pero a pesar de esto aún existían puntos débiles a cubrir en vista que el estándar WAP y su lenguaje WML no eran totalmente compatibles con Internet debido al tipo de servicios que puede proporcionar un servidor con una potencia variable contra un equipo móvil con capacidades distintas.

Los avances en la implementación de algoritmos en la pila de WAP han ido avanzando hasta el año 2004 cuando surge WAP 2.0, siendo una reingeniería de WAP versión 1, utilizando XHTML-MP (Mobile Profile) como lenguaje de presentación de contenidos, incorpora mejoras al soporte de gráficos y en cuanto a los protocolos usados en la capa de transporte se utiliza TCP y en la aplicación HTTP, alcanzando a cubrir la mayoría de los protocolos usados en Internet. El gráfico 8 ilustra la explicación.

Gráfico 8. Servicios a tecnologías móviles mediante internet.

Aislamiento equivalente de redes inalámbricas (WEP)

WEP como sus siglas dicen Wireless Equivalent Privacy (Aislamiento Equivalente de Redes Inalámbricas) es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite.

WEP es un método de cifrado de la información utilizando cifrado a nivel 2, se encuentra basado en el algoritmo de cifrado RC4 el cual implementa claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 124 bits (104 bits más 20 bits del vector de iniciación IV). Su principal funcionamiento consiste en dos pasos cifrar las tramas antes de ser enviadas al punto de acceso (AP) apoyándose en el algoritmo RC4 y posteriormente en el algoritmo de chequeo de integridad del mensaje para comprobación de tramas al ser recibidas.

El funcionamiento del algoritmo RC4 se apoya en el flujo de las semillas (seed), donde dicha semilla es un número aleatorio generado para cifrar los mensajes realizando operaciones XOR, el único inconveniente que posee este tipo de cifrado o algoritmo, es que se debe tener una semilla (número aleatorio) distinta para cada mensaje a cifrar, cabe mencionar que el paquete entero es cifrado con la

clave WEP. Observar el gráfico 9 como ejemplo.

Gráfico 9. Proceso de cifrado WEP.

Actualmente el cifrado WEP es uno de los más utilizados en redes inalámbricas como protección a nuestra red, pero la realidad es que el cifrado WEP es uno de los más fáciles de crackear o saltar, ya que utiliza la misma clave para cifrar todos los mensajes, por lo tanto cualquier router con cifrado WEP puede ser atentado y poder gozar de los servicios que proporcione la red, por ejemplo: Internet. El proceso de audición de una red inalámbrica con cifrado WEP se realiza utilizando la aplicación aircrack. De forma general el modo más básico para hacerse de una clave WEP es realizando dos pasos que son: Sniffing de Packetes y utilizar algún WEP-Cracker, es decir se deben capturar algunos paquetes de la red inalámbrica (no es necesario estar conectado o tener un IP), posteriormente se procede a desempaquetar la información para intentar sacar la clave WEP, entre más grande sea la clave WEP, mayor deben de ser los paquetes interceptados. Observar gráfico 10.

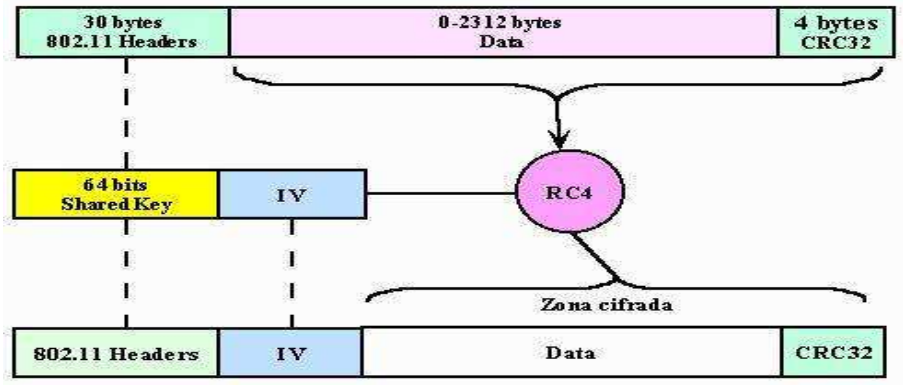


Gráfico 10. Panel de Configuración de Métodos de Cifrado para redes inalámbricas.

Acceso Protegido A Wi-Fi (WPA).

WPA que significa Wi-Fi Protected Access (Acceso Protegido a Wi-Fi) es un sistema para proteger las redes inalámbricas creado para corregir las deficiencias del sistema previo (WEP) e implementa la mayoría del estándar IEEE 802.11i. Evidentemente la evolución o mejora del cifrado WEP es WPA basándose en métodos de autentificación y cifrado nuevo, el cual congela los puntos débiles que poseía WEP respecto a su vector de inicialización (VI) el cual podría ser retomado en las tramas para obtención de la clave WEP por fuerza bruta, de modo que WPA es el reforzamiento de WEP con sus distintas desventajas.

Para utilización del WPA como método de seguridad en nuestra red inalámbrica debe tener en cuenta que la mayoría de los equipos antiguos o mejor dicho, con las primeras tarjetas inalámbricas del mercado, no soportan este tipo de cifrado, también que a la fecha siguen en existencia estas tarjetas que no brindan soporte a WPA, la prueba principal está en el precio de los productos.

WPA incorpora un reforzamiento en generación de claves de 128 bits y un vector inicial de 48 bits, inicialmente WPA se diseñó como un sistema de protección de redes inalámbricas protegido mediante autentificación forzosa, para esto se utilizó el protocolo RADIUS, brindando así un usuario y clave para cada equipo que se

conecte al punto de acceso (AP). Posteriormente se incorpora un método menos complicado y más factible para implementar WPA en oficinas y casa, para esto se dio uso de una clave pre-compartida (PSK, Pre-Shared Key) continuando en ambas modalidades de configuración la utilización del algoritmo RC4 para el cifrado de la información.

A continuación una pequeña lista de las mejoras de WPA:

- ✓ Implementación de un código de integridad del mensaje (MIC).

- ✓ Evita el ataque de repetición (replay attack), ya que incluye un contador de tramas.

- ✓ En base al mayor tamaño de las claves, implementación de MIC y el contador de tramas, resulta más difícil la intrusión a la red inalámbrica.

- ✓ Al detectar dos intentos de ataques durante un minuto, las redes WPA se desconectan durante 60 segundos. El gráfico 11 ilustra la explicación.

Gráfico 11. Panel de Configuración de Métodos de Cifrado WPA para redes inalámbricas.

Actualmente WPA ha pasado a evolucionar como WPA2 adoptando por completo el estándar IEEE 802.11i pero aún no se extiende como soporte incluido en todos los dispositivos de hardware, sus respectivos fabricantes aún están en implementación del mismo.

Protocolo Dominante Temporal de la Integridad (TKIP)

TKIP o Protocolo Dominante Temporal de la Integridad (Temporal Key Integrity Protocol), también conocido como hashing de clave WEP WPA, basado para brindar una mejor protección al protocolo WEP el cual puede ser quebrado de una manera fácil, con el algoritmo que utiliza TKIP para encriptación de los datos se puede tener una red segura y sin la necesidad de cambiar de hardware para soportar otros protocolos.

El funcionamiento de TKIP se basa en generar una clave temporal (hashing), esta misma clave es compartida entre los equipos de la red inalámbrica y los puntos de acceso (AP), posteriormente TKIP utiliza el hashing y la MAC del cliente para combinarlos, así mismo le agrega la clave del vector de inicialización de 16 octetos generado y con esto cifra los datos, esta clave se reemplazara después de cada 10,000 paquetes. Una de las cuestiones similares a WEP, es que TKIP utiliza RC4 para cifrar el mensaje.

Con los métodos mencionados TKIP proporciona una mejor forma de brindar seguridad a las redes inalámbricas utilizando claves distintas después de un determinado número de paquetes, así mismo evita el reemplazo del hardware (solo el firmware) para trabajar con este protocolo. Observar el gráfico 12.

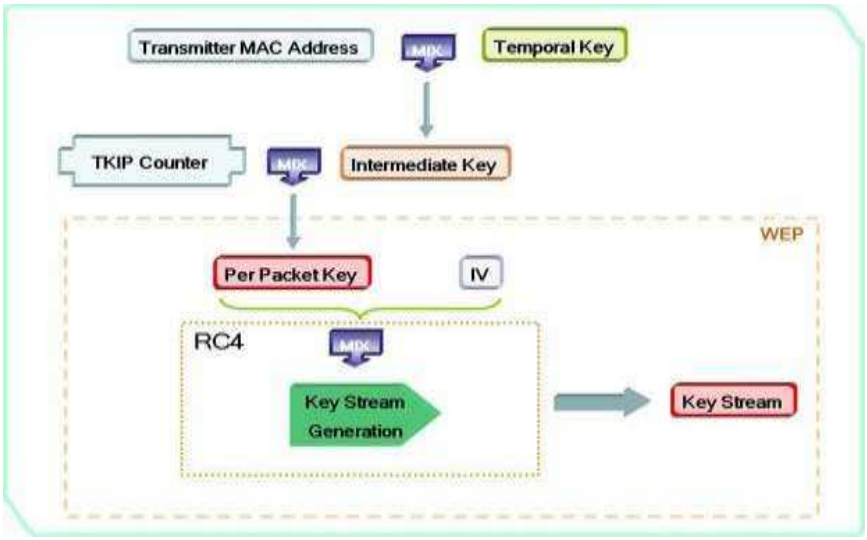


Gráfico 12. Estructura de Encriptación del Protocolo TKIP.

Código de Integridad del Mensaje (MIC)

MIC como su siglas lo indica es Código de la Integridad del Mensaje (Message Integrity Code), y está fuertemente implementado o enlazado con el protocolo TKIP ya que viene a formar un complemento para reforzar la encriptación del mensaje y así brindar una clave más fuerte y más difícil de quebrar. Con esto se obtiene una mayor seguridad en redes inalámbricas mediante la utilización de MIC.

El algoritmo MIC también es conocido como algoritmo Michael, el cual se implementa sobre redes inalámbricas para determinar la fidelidad del mensaje, siguiendo el método de encriptación TKIP, este mismo genera la clave MIC y se la anida al paquete.

Fundamentación Legal

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El objetivo de este trabajo es analizar, Las conductas delictivas que pueden generar el gran avance tecnológico, sobre todo en el campo de la informática" desde tres de puntos de vista: normativo, delincuencia y prevención

Concepto de Delito Informático

Argibay Molina señala respecto de "Los delitos Económicos" que, los delitos de esta naturaleza en el derecho penal no existen, existen derechos patrimoniales, como uno de tantos grupos de conductas clasificadas, tomando como pauta el bien jurídico protegido, pero ello no quiere decir que tales delitos sean Económicos.

Si hacemos una analogía entre "delitos informáticos" y "delitos económicos" concluiríamos que, solo son delitos los tipificados en nuestro ordenamiento jurídico; y como ninguno de ellos lo está, tanto la informática como lo económico son solo "factores criminógenos"

Legislación Nacional

Nuestra legislación regula Comercial y penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos.

La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual.

La ley Penal 11723 de "La propiedad Científica, literaria y artística" ha modificado los artículos 71, 72, 72 bis, 73 y 74.

El artículo 71 tipifica como conducta ilícita a "el que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley"

El Art. 72 considera casos especiales de defraudación:
a. El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derecho-habientes.

b. El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto.

c. El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el titulo de la misma o alterando dolosamente su texto.

El Art. 72 bis
a. El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;

b. El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;

c. El que reproduzca copias no autorizadas por encargo de terceros mediante un precio.

d. El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con el productor legítimo;

e. El que importe las copias ilegales con miras a distribución al público.

El decreto 165/94 (B.O. del 8/2/94) incluyó al software dentro de la Ley de Propiedad Intelectual 11723.

También dentro del Código Penal encontraremos sanciones respecto de los delitos contra el honor (109 a 117); Instigación a cometer delito (209), instigación al suicidio (83); estafas (172), además de los de defraudación, falsificación, tráfico de menores, narcotráfico, etc., todas conductas que pueden ser cometidas utilizando como medio la tecnología electrónica

Legislación Internacional

Tratados Internacionales

En este sentido habrá que recurrir a aquellos tratados internacionales, que nuestro país es parte y que, en virtud del artículo 75 inc. 22 de la Constitución Nacional reformada en 1994, tienen rango constitucional.

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político- jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes.

En este sentido Argentina es parte del acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio, que en su artículo 10 relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

En el Artículo 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que, "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias"

El convenio de Berna fue ratificado en nuestro país por la Ley 22195 el 17/3/80
La convención sobre la Propiedad Intelectual de Estocolmo, fue ratificada por la ley 22.195 del 8/7/1990.

La Convención para la Protección y Producción de Phonogramas de 1971, fue ratificada por la ley 19.963 el 23/11/1972.

La Convención Relativa a la Distribución de Programas y Señales, fue ratificada por la ley 24425 el 23/12/1994.

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación.

Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.
En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de ésta sección.

En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad"

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante a partir del 8/10/1980

En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:

- ✓ Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas
- ✓ Blanqueo de capitales, contrabando y narcotráfico
- ✓ Hacia una policía Europea en la persecución del delito Cibernético.
- ✓ Internet: a la búsqueda de un entorno seguro.
- ✓ Marco legal y Deontológico de la Informática.

Organizador Lógico de Variables

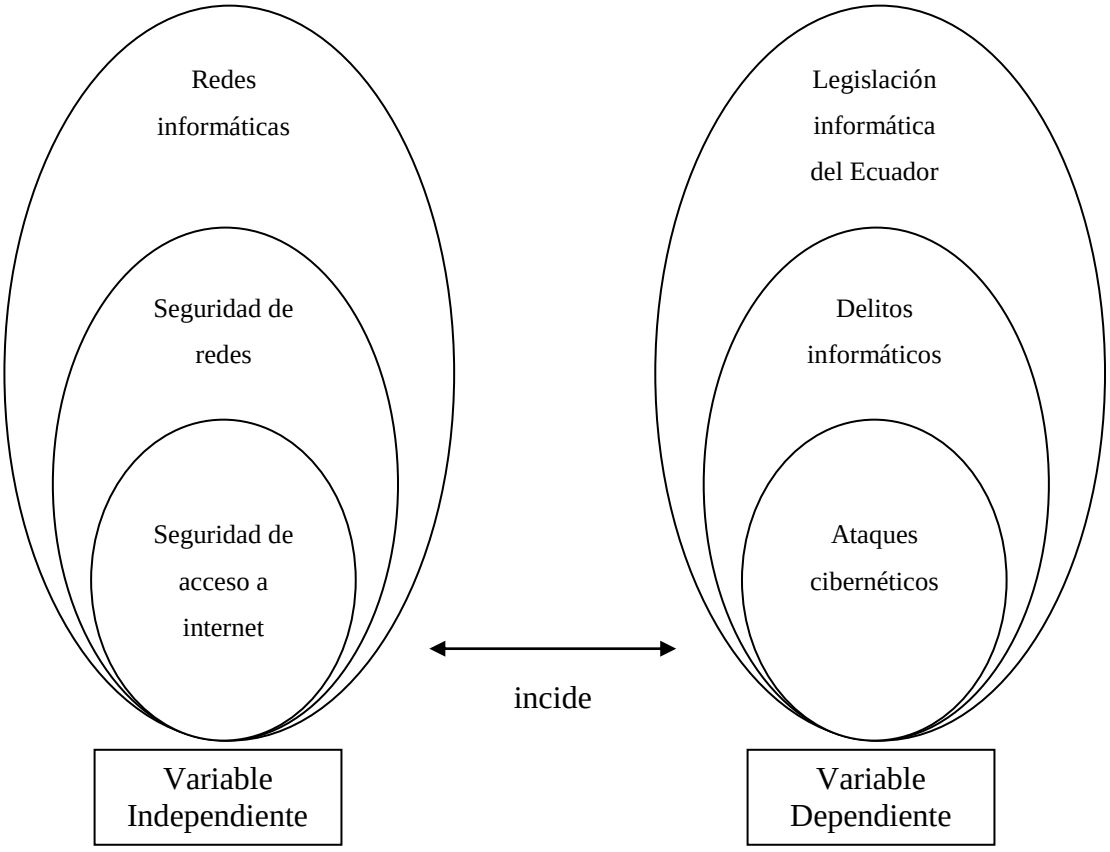


Gráfico No. 13: Inclusiones Conceptuales

Constelación de Ideas, Variable Independiente

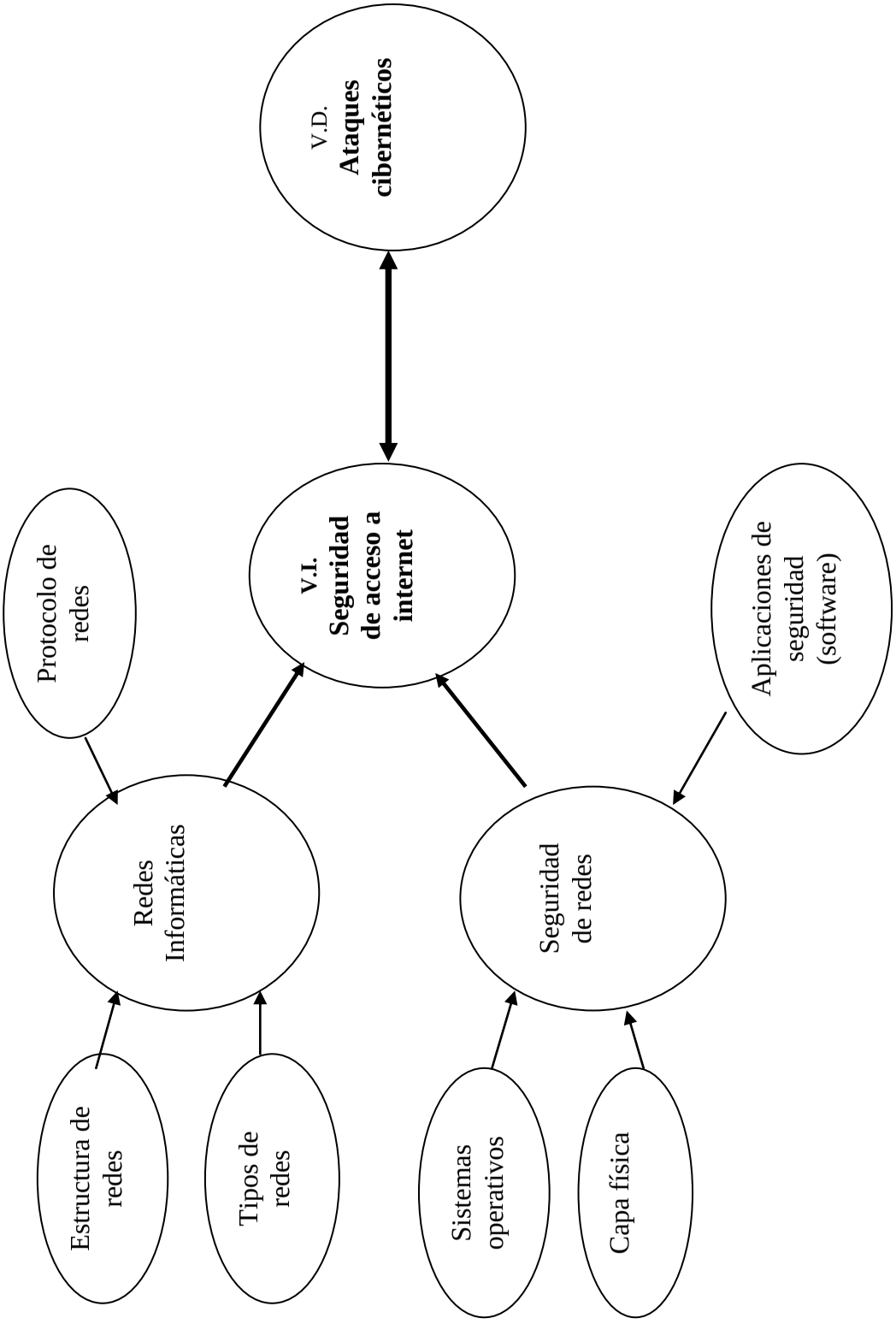


Gráfico No. 14: Constelación de Ideas de la Variable Independiente

Constelación de Ideas, Variable Dependiente

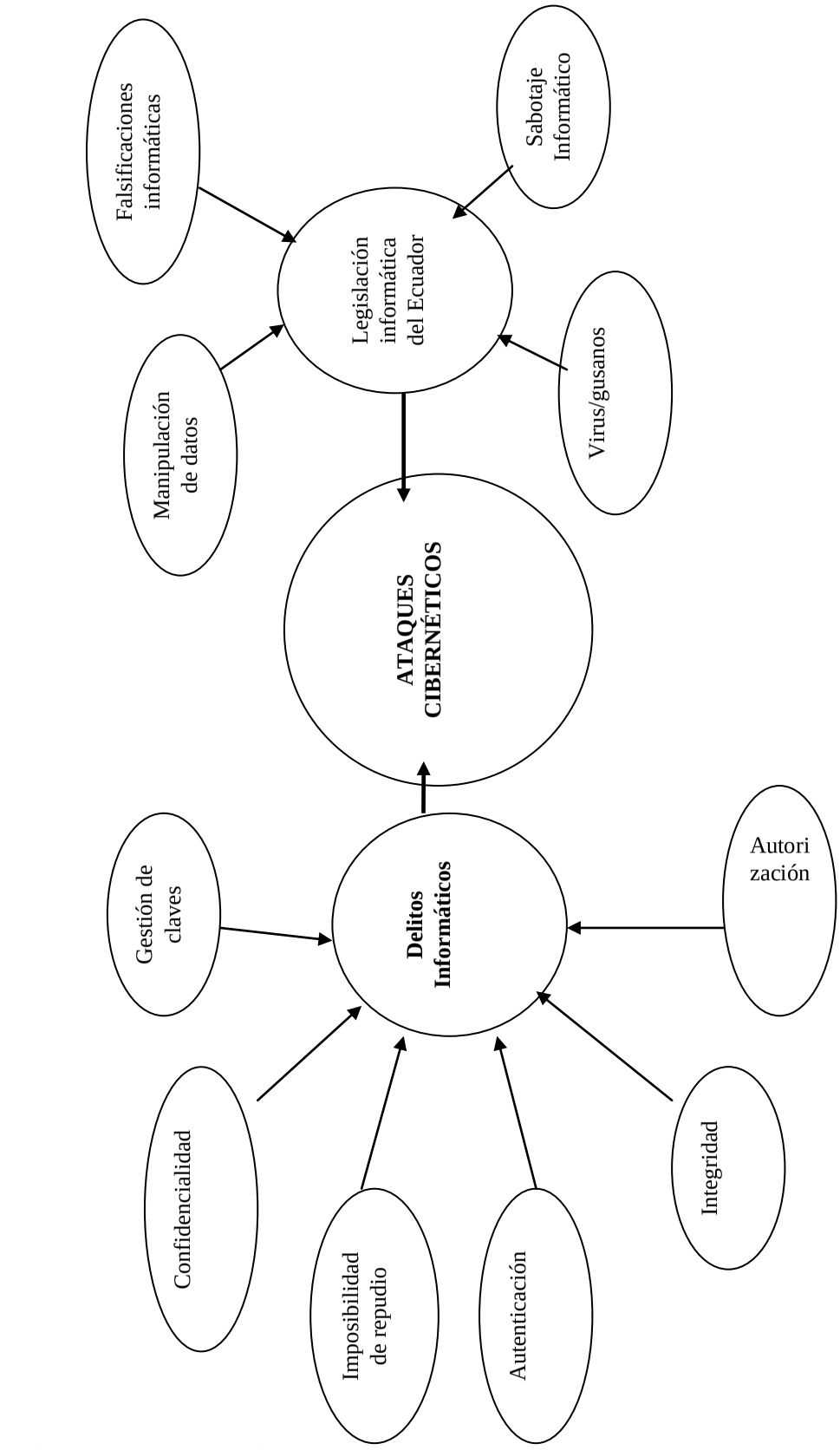


Gráfico No. 15: Constelación de Ideas de la Variable Dependiente

Hipótesis

La seguridad de acceso a Internet incide en los Ataques cibernéticos en Emperador Hotel Casino de la ciudad de Ambato.

Señalamiento de Variables

Variable Independiente: Seguridad de Acceso a Internet

Variable Dependiente: Ataques Cibernéticos

CAPITULO III

METODOLOGÍA

Enfoque

Al ya tener delimitado el problema, establecido los objetivos y las respectivas variables, es necesario seleccionar los métodos y técnicas a emplearse. Esta selección dependerá del área científica que se va investigar, del tema y de la hipótesis planteada. La investigación predominante es cualitativa ya que esta tiene cualidades de normativas, explicativa y realista

Modalidad de Investigación

Bibliográfica –documental

Se realizó este método de investigación Bibliográfica – documental debido a que se utiliza diferentes tipos de documentos como son encuestas, reportes, resultados, los cuales se han basado a linkografías, revistas.

Debido a que se caracteriza de la siguiente manera:

- Por la utilización de documentos; recolecta, selecciona, analiza y presenta resultados coherentes.

- Utiliza los procedimientos lógicos y mentales de toda investigación; análisis, síntesis, deducción, inducción, etc.

- Realiza un proceso de abstracción científica, generalizando sobre la base de lo fundamental.

- Realiza una recopilación adecuada de datos que permiten redescubrir hechos, sugerir problemas, orientar hacia otras fuentes de investigación, orientar formas para elaborar instrumentos de investigación, elaborar hipótesis, etc.

- Puede considerarse como parte fundamental de un proceso de investigación científica, mucho más amplio y acabado.
- Es una investigación que se realiza en forma ordenada y con objetivos precisos, con la finalidad de ser base a la construcción de conocimientos.
- Se basa en la utilización de diferentes técnicas de: localización y fijación de datos, análisis de documentos y de contenidos.

De campo

Se presenta mediante la manipulación de una variable externa no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o por qué causas se produce una situación o acontecimiento particular (Investigación Pura).
Este tipo de investigación se la utilizará para realizar un estudio del acceso a Internet y su seguridad en la empresa Emperador Hotel Casino de la ciudad de Ambato, con el fin de obtener la información necesaria para proponer una solución al problema del acceso a Internet inalámbrico y su seguridad.

Proyecto factible

Esta investigación se la puede ubicar como un proyecto factible, ya que el planteamiento del problema, la fundamentación teórica y procedimiento metodológico, permite dar una solución práctica, viable y que se encuentra enmarcada en plazos fijos al problema.

Niveles o Tipos

Exploratorio

Es de nivel exploratorio ya que no existen estudios o investigaciones anteriores dentro de la empresa Emperador Hotel Casino sobre la problemática del acceso a Internet y su seguridad.

Descriptivo

De nivel descriptivo debido a que formula una hipótesis y se enuncia los supuestos de acuerdo a la hipótesis con los procesos adoptados. Por la selección y elaboración de técnicas para la recolección de datos, como son encuestas, reportes y entrevistas.

Correlacional

Nivel correlacional para establecer comparaciones entre las problemáticas que aquejan a Emperador Hotel Casino con el acceso a Internet y su seguridad para brindar un buen servicio a todos los clientes que frecuentan sus instalaciones.

Población y Muestra

Población

	Cantidad	Porcentaje
Habitaciones total	63	100%*
Habitaciones ocupadas	50	79.36%*
Habitaciones utilizan Internet (de 50 ocupadas)	30	60%*
Clientes no hospedados**	15	
Personal administrativo	4	

Cuadro No. 4 Población

* Datos recogidos de porcentaje de ocupación de Recepción de Emperador Hotel Casino y del Departamento de Sistemas.

** Áreas de Restaurante, Spa, Eventos.

La población será de 45, entre huéspedes y clientes que frecuentan otras áreas de Emperador Hotel Casino.

Muestra

TIPO DE CLIENTE	CANTIDAD
Huésped	30
Cliente otras áreas	15
Personal Administrativo	4

Cuadro No. 5 Muestra

Se toma el mismo número de población en la muestra debido al número reducido de elementos.

Operacionalización de Variables

Variable Independiente: Seguridad de acceso a internet

TÉCNICAS INSTRUMENTOS	ÍTEMS BÁSICOS	INDICADORES	DIMENSIONES	CONCEPTUALIZACIÓN
Cuestionario estructurado a los clientes que frecuentan Emperador Hotel Casino.	¿Qué seguridad se tiene por parte de las personas que tienen acceso a Internet?	Eliminación de información Uso no autorizado de servicios Revelación no autorizada de la información Alteración o destrucción de la información.	✓ Seguridad Sistemas Operativos	La seguridad de acceso a internet se conceptúa como: el conjunto de medidas que los internautas deben tomar para navegar con ciertas garantías por la Red, mantener a salvo su privacidad y la integridad de sus PCs.
Cuestionario estructurado al personal que labora en Emperador Hotel Casino.	¿Con qué seguridad se cuenta para los equipos físicos de la conexión de la red?	Destrucción de firewall (hardware). Alteración de tarjetas de red. Interferencia de equipos de red. Acceso no autorizado a cuarto de servidores.	✓ Seguridad en capa física	
Entrevista focalizada al personal que manipula los PC's en Emperador Hotel Casino.	¿Qué seguridad hay en el usuario para instalar o desinstalar programas?	Eliminación de antivirus. Desactivar firewall (software.) Instalación de programas maliciosos.	✓ Aplicaciones de seguridad	

Cuadro No. 6: Seguridad de acceso a Internet.

Cuadro No. 7: Ataque cibernético

TÉCNICAS INSTRUMENTOS	ÍTEMS BÁSICOS	INDICADORES	DIMENSIONES	CONCEPTUALIZACIÓN
Entrevista focalizada al personal que manipula los PC's en Emperador Hotel Casino. Reporte estadístico de clientes que acceden al servicio de internet.	¿Qué ataques cibernéticos han causado la destrucción de equipos? ¿Qué ataques cibernéticos han ocasionado pérdida de información?	Daño de información. Destrucción de equipos (hardware). Regar líquido en PC's Infección de virus Sustracción de información. Eliminación de información. Manipulación de programas Falsificación de información. Alteración de información	✓ Sabotaje informático. ✓ Manipulación de datos	Ataque cibernético se conceptúa como: Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Variable Dependiente: Ataque cibernético

Técnicas e Instrumentos

Para el desarrollo de la investigación se utilizarán las siguientes técnicas e instrumentos de recolección de información de acuerdo al tipo de investigación elegida:

TIPO DE INVESTIGACIÓN	TÉCNICAS DE INVESTIGACIÓN	INSTRUMENTOS DE INVESTIGACIÓN
Documental	Análisis de documentos	Datos estadísticos, libros, textos, publicaciones, revistas, internet.
De campo	Encuestas Entrevistas	Cuestionarios

Cuadro No.8 Técnicas e instrumentos

Plan para Recolección de la Información

La recolección de la información la realizaremos en las áreas de Restaurante, Spa, Habitaciones y salones de eventos de Emperador Hotel Casino, para recoger la opinión acerca del acceso a internet dentro de las instalaciones de la empresa.

Se realizarán encuestas a funcionarios como son Gerente General, Gerente de Hotel, Jefe de Recepción, las preguntas serán diseñadas por el autor, con el afán de identificar y conseguir información útil para el desarrollo y aplicación de la propuesta.

Plan para el Procesamiento de la Información

Se llevará el procesamiento estadístico de los datos e información recolectada, para los gráficos se realizará en Microsoft Excel, y se mostrará los datos con sus respectivos porcentajes.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Encuesta dirigida a: Huéspedes de Emperador Hotel Casino

Pregunta 1

1. Usted visita Emperador Hotel Casino por:

OPCIONES	FRECUENCIA	PORCENTAJE
Placer	8	18%
Negocios	15	33%
Trabajo	22	49%
TOTAL	**45**	**100%**

Cuadro 9. Pregunta 1

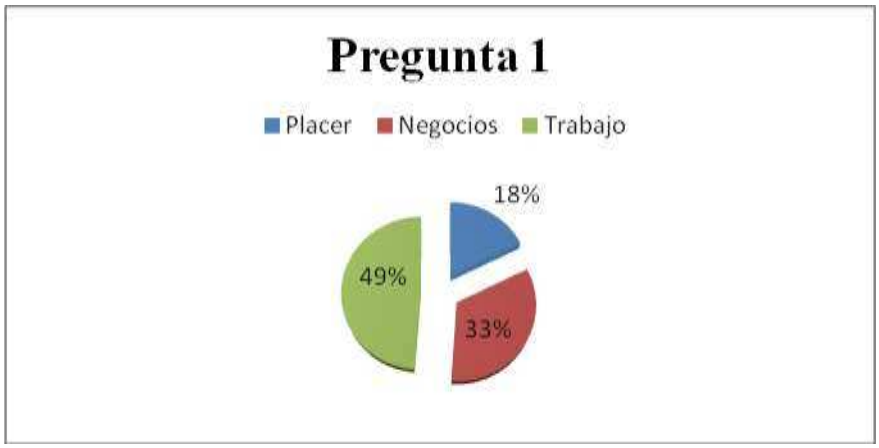


Gráfico 16. Pregunta 1.

La empresa Emperador Hotel Casino es visitada en un 49% por clientes y su trabajo; un 33% visita por negocios; y, un 18% visita la empresa por placer.

Pregunta 2

2. ¿Qué área de Emperador Hotel Casino es la que más frecuenta durante su estadía?

OPCIONES	FRECUENCIA	PORCENTAJE
Restaurante	17	38%
SPA	5	11%
Salones de eventos	6	13%
Casino	3	7%
Discoteca	3	7%
Habitación	11	24%
TOTAL	**45**	**100%**

Cuadro 10. Pregunta 2

Gráfico 17. Pregunta 2

El área que más se frecuenta por parte de los clientes es Restaurante con un 38%; Habitaciones con un 24%; salones de eventos en un 13%; SPA con 11%; y, Casino y Discoteca con un 7%.

Pregunta 3

3. ¿Qué tipo de conexión utiliza para acceder a Internet en su trabajo y/o domicilio?

OPCIONES	FRECUENCIA	PORCENTAJE
Conexión mediante cable	12	27%
Conexión Inalámbrica	33	73%
TOTAL	**45**	**100%**

Cuadro 11. Pregunta 3

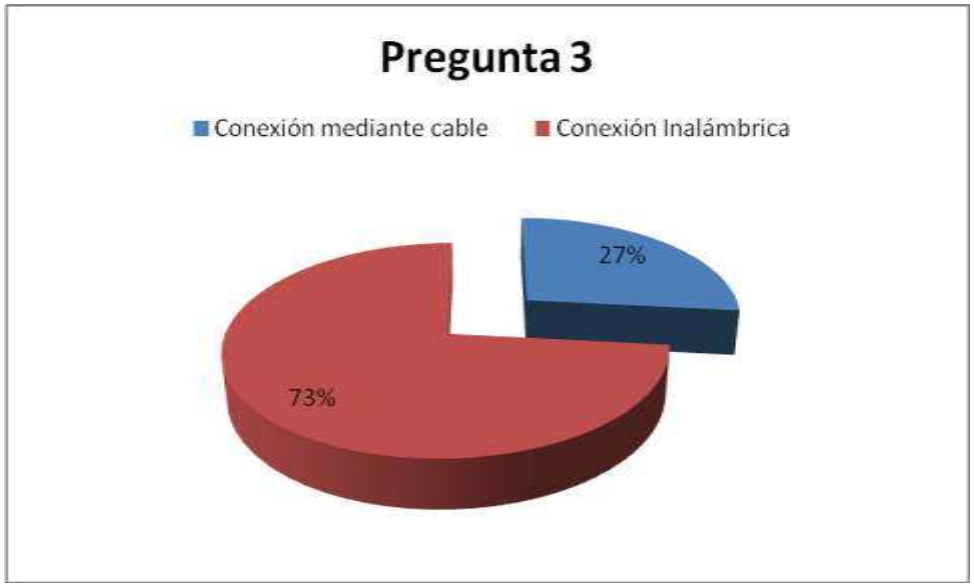


Gráfico 18. Pregunta 3

El tipo de conexión utilizado por los clientes en un 73% es la conexión con cable; mientras que un 27% realiza su conexión inalámbricamente.

Pregunta 4

4. Usted, ¿utiliza alguna aplicación específica al momento de acceder a Internet y conectarse con su empresa?

OPCIONES	FRECUENCIA	PORCENTAJE
SI	14	31%
NO	31	69%
TOTAL	**45**	**100%**

Cuadro 12. Pregunta 4

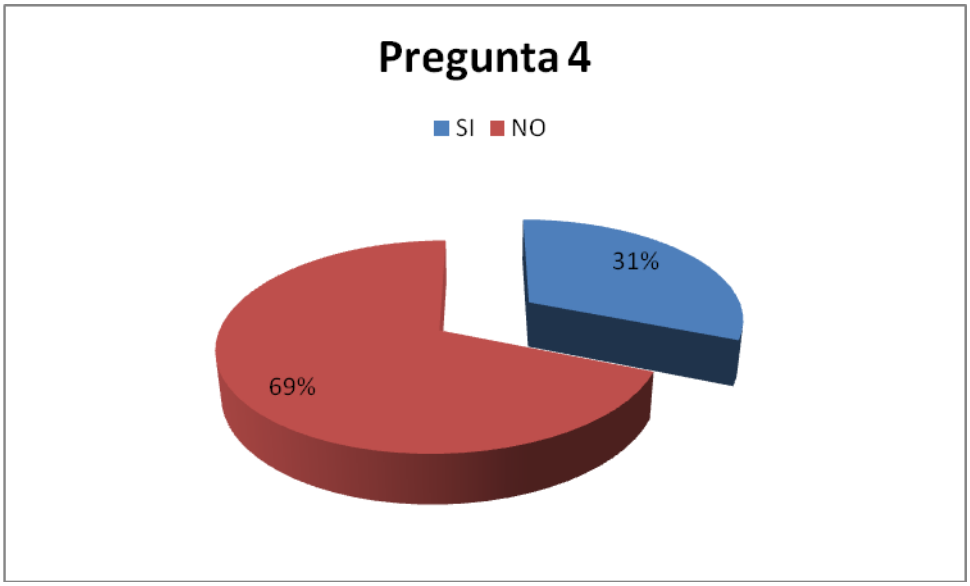


Gráfico 19. Pregunta 4

Los clientes en un 69% no utilizan alguna aplicación para acceder a internet y conectarse a su empresa; mientras que un 31% utiliza alguna aplicación.

Se realiza la prueba de CHI Cuadrado, se tomó en cuenta la Pregunta Nº 1 para lo que:

Placer 8; Negocios 15; Trabajo 22.

Se toma estos valores para tomar en cuenta un valor esperado de 25 (uso de alguna aplicación por motivo de conexión al trabajo) para la respuesta **SI** y de 20

(no necesita ninguna aplicación ya que solo necesita navegar en Internet revisando correos personales) para la respuesta **NO.**

Para esto:

Valores observados

SI	14
NO	31
TOTAL	45

Valores esperados

SI	25
NO	20
TOTAL	45

Se aplica la fórmula de Chi cuadrado con un valor de grado de libertad de 1 y significatividad de 0.05 se obtiene el valor de 10,89; lo que indica que hay diferencia entre las dos respuestas lo que quiere decir que hay diferencia entre las personas que utilizan alguna aplicación específica para conexión a internet y las personas que no utilizan ninguna aplicación específica para poder navegar.

Pregunta 5

5. Para tener acceso a Internet usted prefiere que sea:

OPCIONES	FRECUENCIA	PORCENTAJE
Sin restricciones	28	62%
Con contraseña	17	38%
TOTAL	**45**	**100%**

Cuadro 13. Pregunta 5.

Gráfico 20. Pregunta 5.

La preferencia de acceso a Internet por parte de los clientes en un 62% es que no tenga restricciones; mientras que un 38% tiene preferencia por acceso mediante contraseñas.

Se realiza la prueba de CHI Cuadrado, se tomó en cuenta la Pregunta Nº 1 para lo que:

Placer 8; Negocios 15; Trabajo 22.

Se toma simplemente a los del grupo Negocios y trabajo, quienes deben tener muy en cuenta la seguridad de su información.

Se toma estos valores para tomar en cuenta un valor esperado de 8 (ningún uso de contraseña para ingresar a internet) para la respuesta **SIN RESTRICCIONES** y

de 37 (con contraseña para conexión a Internet) para la respuesta **CON CONTRASEÑA.**

Para esto:

Valores observados

Sin contraseña	28
Con contraseña	17
TOTAL	45

Valores esperados

Sin contraseña	8
Con contraseña	37
TOTAL	45

Se aplica la fórmula de Chi cuadrado con un valor de grado de libertad de 1 y significatividad de 0.05 se obtiene el valor de 60,81; lo que indica que esta pregunta es un indicativo que se debe aplicar medidas de seguridad dentro de la red inalámbrica de Emperador Hotel Casino, y así brindar buen servicio con el agregado de una seguridad para los clientes; debido a la diferencia entre 60,81 y 3.84 que es la referencia para que sea aplicable.

Pregunta 6

6. ¿Con qué frecuencia usted se conecta a Internet?

OPCIONES	FRECUENCIA	PORCENTAJE
A diario	38	84%
Una vez por semana	6	13%
Una vez al mes	1	2%
TOTAL	**45**	**100%**

Cuadro 14. Pregunta 6

Gráfico 21. Pregunta 6.

La frecuencia con la que los clientes se conectan a Internet a diario es de un 84%; los que se conectan una vez por semana son el 13%; y, un 2% se conecta una vez al mes.

Pregunta 7

7. ¿Al navegar por Internet usted está seguro que sus datos son enviados y recibidos con seguridad, sin que sean manipulados o vistos por otros?

OPCIONES	FRECUENCIA	PORCENTAJE
SI	11	24%
NO	34	76%
TOTAL	**45**	**100%**

Cuadro 15. Pregunta 7

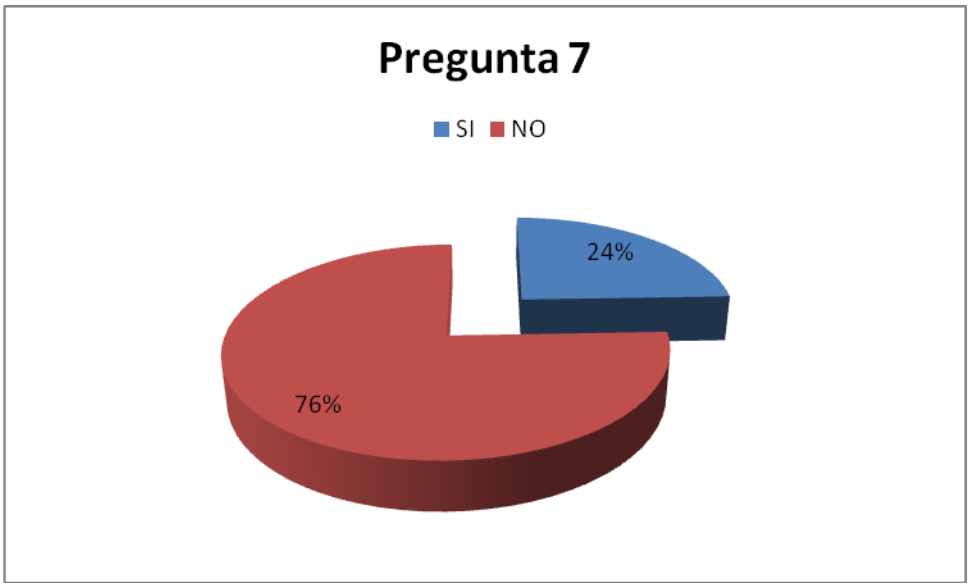


Gráfico 22. Pregunta 7

Los clientes en un 76% no tienen la seguridad de la privacidad de su información; y, el 24% de clientes indica que si se siente seguro de la información que envía no es manipulado o vista por otros.

Pregunta 8

8. ¿Ha sido víctima de ataques cibernéticos con su información?

OPCIONES	FRECUENCIA	PORCENTAJE
SI	8	18%
NO	37	82%
TOTAL	**45**	**100%**

Cuadro 16. Pregunta 8

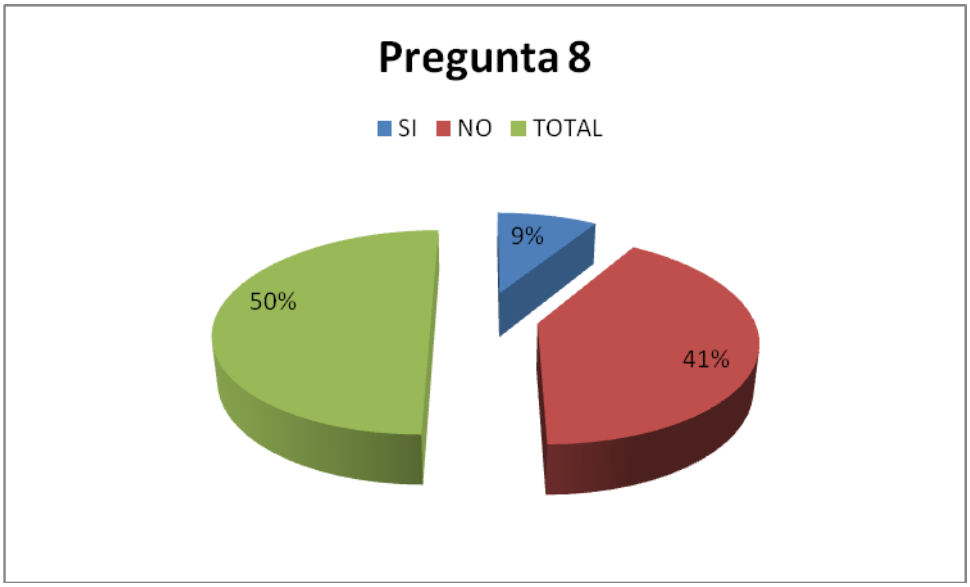


Gráfico 23. Pregunta 8.

En un 82% los clientes indican que no han sido víctimas de un ataque cibernético; y, un 18% se siente perjudicado por los ataques cibernéticos.

Pregunta 9

9. ¿Su computador personal ha sido infectado por algún virus informático por razones desconocidas?

OPCIONES	FRECUENCIA	PORCENTAJE
SI	41	91%
NO	4	9%
TOTAL	**45**	**100%**

Cuadro 17. Pregunta 9

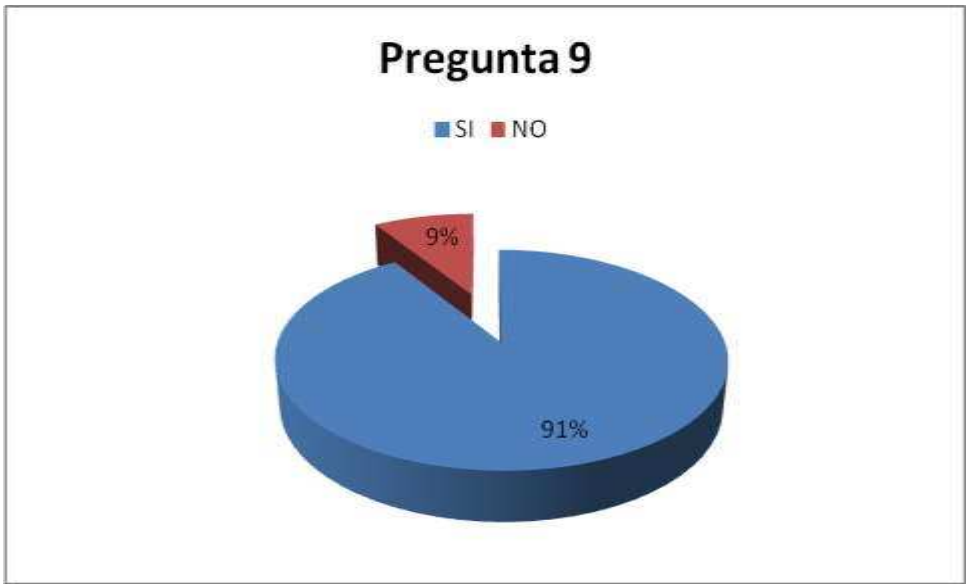


Gráfico 24. Pregunta 9

Los clientes en un 91% indican que han sido infectados por algún virus informático; y, un 9% indica que no ha sido infectado por algún virus informático.

Se realiza la prueba de CHI Cuadrado

Se toma los siguientes valores esperados: 15 (ha sido objeto de algún virus en su computador) para la respuesta **SI** y de 30 (no ha sido infectado por algún virus) para la respuesta **NO.** Estos valores tomando en cuenta que es a lo que se espera llegar.

Para esto:

Valores observados

SI	41
NO	4
TOTAL	45

Valores esperados

SI	15
NO	30
TOTAL	45

Se aplica la fórmula de Chi cuadrado con un valor de grado de libertad de 1 y significatividad de 0.05 se obtiene el valor de 67,6.

Pregunta 10

10. Al conectarse a Internet, ¿cree Usted que otras personas pueden ingresar a su información?

OPCIONES	FRECUENCIA	PORCENTAJE
SI	12	27%
NO	33	73%
TOTAL	**45**	**100%**

Cuadro 18. Pregunta 10

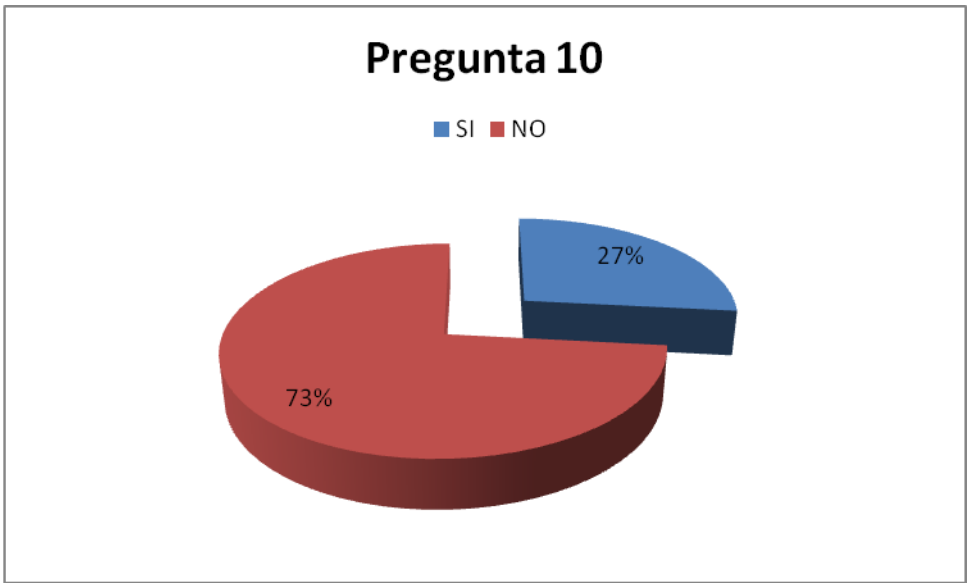


Gráfico 25. Pregunta 10.

Los clientes en un 73% indica que otras personas no pueden ingresar a la información que manejan; y, un 27% responde que si cree que otras personas pueden ingresar a la información que manejan.

Verificación de la hipótesis

Para verificar la hipótesis planteada, se realizó el análisis de las preguntas 4, 5 y 9; obteniéndose los siguientes resultados:

En la pregunta 4 referente a si los usuarios utilizan alguna aplicación específica para conectarse a su lugar de trabajo mediante Internet, en un 69% de las respuestas indicaron que NO lo que puede ocasionar que sean susceptibles a algún ataque cibernético, o de virus.

En la pregunta 5 el 62% de los encuestados prefiere una conexión SIN RESTRICCIONES, lo que en la práctica para evitar algún intruso no es recomendable motivo por el cual se debe dar solución colocando contraseña para el acceso a internet.

En la pregunta 9 un 91% de los clientes respondió afirmativamente al ataque de virus, esto es, que ha sido infectada su computadora (portátil, desktop) con algún tipo de virus (troyano, spyware, malware, etc.)

Con estos resultados tomados de las preguntas relacionadas al tema de la hipótesis de la seguridad informática dentro de las instalaciones de Emperador Hotel Casino se ve que es necesario realizar la propuesta para mejorar la Seguridad de la red de Emperador Hotel Casino para brindar un buen servicio y de calidad a los usuarios que la utilizan.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- ✓ La empresa Emperador Hotel Casino en la mayoría de sus clientes que la visita es por motivos de trabajo, negocio y en un bajo porcentaje por placer; por lo que la mayoría de clientes necesitan de conexión a Internet para poder realizar su trabajo normalmente.

- ✓ Dentro de las áreas con que más frecuencia es visitada por parte de los clientes se encuentran Restaurante y Habitaciones por lo que son en estos lugares donde los clientes necesitan tener conexión a Internet.

- ✓ Los clientes de Emperador Hotel Casino no tienen la seguridad necesaria para poder realizar la conexión a Internet, pues han sido atacados por virus informáticos.

- ✓ El desconocimiento por parte de los clientes de los diferentes ataques cibernéticos que existen les hace propensos a que su información sea manipulada, o que se pierda.

Recomendaciones

- ✓ Brindar acceso a Internet a los clientes de la empresa Emperador Hotel Casino para dar mejor servicio y así puedan realizar su trabajo de una manera eficiente.

- ✓ Colocar acceso a Internet inalámbrico en partes estratégicas de la empresa Emperador Hotel Casino para que los clientes tengan comodidad y acceso en los lugares frecuentan mayormente.

- ✓ Dar seguridad en el acceso a Internet a los clientes que visitan Emperador Hotel Casino, para poder disminuir ataques cibernéticos a su información.

CAPITULO VI

LA PROPUESTA

Datos Informativos

Empresa:	Emperador Hotel Casino
Gerente:	Alfonso Pérez
Actividad:	Hotelera – Casino
Inicio actividad:	Marzo 2006
Ciudad:	Ambato
Dirección:	Av. Cevallos y Lalama
Nº Habitaciones:	63
Nº Pisos:	7 pisos
Pisos de habit.:	4 pisos
Servicios presta:	Hospedaje, casino, restaurante, discoteca, SPA, eventos y banquetes.

Antecedentes de la Propuesta

EMPERADOR HOTEL CASINO inició sus actividades en marzo del año 2006, se encuentra ubicado en el cantón Ambato, de la provincia de Tungurahua, en la Av. Cevallos y Lalama.

EMPERADOR HOTEL CASINO es una empresa especializada en el servicio de hospedaje. La empresa se dedica a dar servicios adicionales en diferentes áreas dentro de sus instalaciones como son: Restaurante, Eventos y Banquetes, SPA, Casino, Discoteca. En sus respectivas áreas se pretende dar el servicio de internet inalámbrico el mismo que contará con la respectiva seguridad informática para el

bienestar de los clientes que visitan dichas instalaciones, pues con la seguridad implanta se realizará un análisis en tres momentos antes, durante y después que se sufra algún ataque cibernético.

Misión

Brindar un servicio de excelencia a la comunidad, dentro de un ambiente de comodidad, esparcimiento, seguridad y tranquilidad. Buscamos posicionarnos en el mercado con reconocimiento nacional e internacional, en un periodo de cinco años con el compromiso de superación constante de todos quienes forman parte de la empresa.

Visión

Ser una compañía líder de los mercados Hotelero y Turístico, comprometidos con nuestros valores, la innovación y la excelencia, enfocados en la satisfacción de sus clientes, alcanzando las expectativas de su personal y accionistas.

Justificación

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la empresa y especialmente de los clientes de dicha empresa. Vale la pena implementar una política de seguridad si los recursos y la información que la empresa y sus clientes tienen en sus redes merecen protegerse. La mayoría de las empresas tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del mismo modo que otros bienes valiosos como la propiedad corporativa y los edificios de oficinas.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de firewall antes de que se haya identificado un problema particular de seguridad de red.

Quizá una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de inter redes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.

Si actualmente los usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso.

También debe tomar en cuenta que la política de seguridad que debe usar es tal, que no disminuir la capacidad de su organización-cliente. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo cual la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

Dado estos puntos de seguridad informática relación organización-cliente se realiza el estudio y análisis de políticas de seguridad para evitar ataques cibernéticos, ya que con la instalación de la red inalámbrica esta estará más vulnerable a dichos ataques; es por esto y por el servicio a los clientes de resguardar su información por el análisis y propuesta.

Objetivos

Objetivo General

Entregar un servicio de internet confiable y seguro para su acceso de los clientes de Emperador Hotel Casino.

Objetivos Específicos

- Brindar Seguridad en el ingreso a internet para todos los clientes de Emperador Hotel Casino.
- Ofrecer acceso a internet en cualquier lugar de Emperador Hotel Casino, para así dar una comodidad y servicio excelente a los clientes.
- Evitar ataques cibernéticos mediante seguridad en el servidor.

Factibilidad

Es pertinente realizar un estudio de factibilidad para determinar la infraestructura tecnológica y la capacidad técnica que implica la implantación del sistema en cuestión, así como los costos, beneficios y el grado de aceptación que la propuesta genera en la empresa.

Este análisis permitió determinar las posibilidades de implementar el sistema propuesto y su puesta en marcha, los aspectos tomados en cuenta para este estudio fueron clasificados en tres áreas, las cuales se describen a continuación:

Factibilidad Técnica

La Factibilidad Técnica consistió en realizar una evaluación de la tecnología existente en la organización, este estudio estuvo destinado a recolectar información sobre los componentes técnicos que posee la organización y la posibilidad de hacer uso de los mismos en el desarrollo e implementación del sistema propuesto y de ser necesario, los requerimientos tecnológicos que deben ser adquiridos para el desarrollo y puesta en marcha del sistema en cuestión.

Se evaluó bajo dos enfoques: **Hardware y Software**.

Hardware

En cuanto a Hardware, específicamente el servidor para el servicio de Internet propuesto, este debe cubrir con los siguientes requerimientos mínimos:

Procesador Pentium 4 3.0Ghz.
Tarjeta Madre.
512 MB de Memoria RAM
Disco Duro de 120 GB.
Unidad de CD-ROM
Tarjetas de Red.
Tarjeta de Vídeo.
Monitor SVGA.
Teclado.
Mouse.
Unidad de Protección UPS

HARDWARE			
Recursos	Número	Descripción	Estado
Computadores	1	SERVER HP PAVILION HD 80 Gb Memoria 3.0 GHz	Optimo
Computadores	2	Pentium Core 2 Duo HD 160 Gb Memoria 1 GHz	Optimo

Cuadro 19. Elementos técnicos de Hardware

Evaluando el hardware existente y tomando en cuenta la configuración mínima necesaria, la empresa no requirió realizar inversión inicial para la adquisición de nuevos equipos para servidores, ni tampoco para repotenciar o actualizar los equipos existentes, ya que los mismos satisfacen los requerimientos establecidos

tanto para el desarrollo y puesta en funcionamiento del proyecto propuesto, además hay que agregar que estos componentes se encuentran en el mercado actualmente a unos precios bajos.

Lo que la empresa requiere realizar una inversión es la adquisición de los equipos para la red inalámbrica los cuales son:

HARDWARE –Equipos Inalámbricos			
Recursos	Número	Descripción	Estado
Router	1	TRENDNET TEW 632brp	Nuevo
Puntos de acceso (AP) – Access point	12	TRENDNET TEW 430apb	Nuevos

Cuadro 20. Hardware equipos inalámbricos

Software

En cuanto al software, la empresa cuenta con todos las aplicaciones que se necesita para el desarrollo del proyecto y funcionamiento del sistema, lo cual no amerita inversión alguna para la adquisición de los mismos. Para el uso general de las estaciones en actividades diversas se debe poseer las herramientas de escritorio y los navegadores que existen en el mercado actualmente.

SOFTWARE			
Recursos	**Número**	**Descripción**	**Estado**
Windows XP	12	Profesional	Optima
Windows 2003 Server Small Business	1	Servidor	Óptimo

Cuadro 21. Elementos técnicos de Software

Personal Técnico

Personal Técnico			
Recursos	Número	Descripción	Estado
Administrador de sistemas	1	Administrador	---------

Cuadro 22. Elementos técnicos (Personal técnico)

Como resultado de este estudio técnico se determina que en los actuales momentos la empresa posee la infraestructura tecnológica (Hardware (servidores), Software, Personal técnico) para el desarrollo del proyecto propuesto.

Factibilidad Económica

A continuación se presenta un estudio que dio como resultado la factibilidad económica del proyecto propuesto. Se determinaron los recursos para desarrollar, implantar, y mantener en operación el proyecto, haciendo una evaluación donde se puso de manifiesto el equilibrio existente entre los costos intrínsecos y los beneficios que se derivaron de éste, lo cual permitió observar de una manera más precisa las bondades del proyecto propuesto.

Análisis Costos-Beneficios

Este análisis permitió hacer una comparación entre la relación costos del sistema actual, y los costos que tendría un nuevo sistema, conociendo de antemano los beneficios que la ciencia de la Informática ofrece.

Como se mencionó anteriormente en el estudio de factibilidad técnica, la empresa contaba con las herramientas necesarias para la puesta en marcha del proyecto, por lo cual el desarrollo de la propuesta.

A continuación se presenta un resumen de los costos intrínsecos del proyecto

propuesto y una lista de los costos que conlleva implantar el mismo, y los costos de operación. Luego a través de un análisis de valor se determinaron los beneficios que no necesariamente para el nuevo sistema son monetarios o cuantificables.

El resumen del análisis costos - beneficios se definieron a través de una comparación de los costos implícitos, tanto del sistema actual como del propuesto y su relación con los beneficios expresados en forma tangible.

Costos del Sistema Actual:

Costos Generales

Los gastos generales se encuentran representados o enmarcados por todos aquellos gastos en accesorios y el material de oficina de uso diario, necesarios para realizar los procesos, tales como bolígrafos, papel para notas, cintas para impresoras, papel para embalaje, marcadores y otros. Cuadro 23.

Gastos Generales	Costo aproximado	Consumo mensual	Costo Total
Material de oficina	$ 25.00	1	$ 25.00
Papel impresiones	$ 5.00	5	$ 5.00
Cartuchos impresoras	$ 25.00	2	$ 50.00
Cartuchos respaldo	$ 25.00	2	$ 50.00
CD’s	$ 1.00	10	$ 10.00
Reportes red	$ 3.00	5	$ 15.00
		TOTAL	$ 155.00

Cuadro 23. Costos Generales - Actual.

Costo de Personal

En este tipo de gasto, incluye los generados por el recurso humano, bajo cuya

responsabilidad directa está la operación y funcionamiento del sistema y que se muestra en el siguiente cuadro:

Recurso Humano	Salario Mensual
Administrador de Sistemas	$ 500.00
TOTAL	$ 500.00

Cuadro 24. Costo de Personal – Actual

Costos de enlace a Internet

En la actualidad se cuenta con la conexión de ADSL con la empresa CNT S.A.; a continuación se describe los costos:

Enlace	Costo Mensual	Costo Total
ADSL 512 Kbps	$ 100.00	$ 100.00

Cuadro 25. Enlace a Internet - Actual

Costos de Red

En la actualidad se cuenta con todo el cableado estructurado instalado en toda la edificación de la empresa, en lo que se requiere un egreso económico es en el cambio de cables de conexión Patch Core, por tal motivo se tiene el siguiente costo de red:

Enlace	Costo Mensual	Costo Total
Cable UTP cat. 5e (arreglos) cableado	$ 25.00	$ 100.00

Cuadro 26. Costo de Red - Actual

Costos del proyecto propuesto

El servicio de acceso a Internet inalámbrico, involucra los siguientes costos:

Costos Generales

Al lograr optimizar los procesos, agilizando el flujo y manejo de la información de los clientes que navegan en la red con sus actividades y control de ancho banda, no es necesario la ejecución de múltiples actividades y tareas para alcanzar los resultados esperados, planteando que impresiones de reportes de red, respaldo en CD's , costo cartuchos y material de oficina en general ya no serán necesarios repetitivamente. (Ver Cuadro 27).

Gastos Generales	Costo aproximado	Consumo mensual	Costo Total
Material de oficina	$ 25.00	1	$ 25.00
Papel impresiones	$ 5.00	1	$ 5.00
Cartuchos impresoras	$ 25.00	1	$ 25.00
Cartuchos respaldo	$ 25.00	1	$ 25.00
CD's	$ 1.00	5	$ 5.00
Reportes red	$ 3.00	2	$ 6.00
		TOTAL	$ 91.00

Cuadro 27. Costos Generales de Proyecto Propuesto

Costos de Hardware y Software.

Hardware

Debido a la inexistencia de equipos inalámbricos se requiere los siguientes:

Equipo	Cantidad	Costo Unitario	Costo Total
Router TEW 632brp	1	$ 100.00	$ 100.00
Access Point TEW 430apb	12	$ 65.00	$ 780.00
		TOTAL	$ 880.00

Cuadro 28. Costos de Hardware – Proyecto Propuesto

Software

La empresa como ya cuenta con los recursos necesarios respecto al software no es requerido ningún tipo de inversión en este aspecto.

Costo de Personal

El proyecto propuesto no incluyó variaciones en cuanto al personal bajo cuya responsabilidad está la operación y/o funcionamiento del sistema.

Recurso Humano	Salario Mensual
Administrador de Sistemas	$ 500.00
TOTAL	$ 500.00

Cuadro 29. Costo de Personal – Proyecto Propuesto

Costos enlace a Internet

El costo de enlace a Internet se verá incrementado por ofrecer mayor velocidad y con esto mejor servicio a los clientes. A continuación se describe los costos:

Enlace	Costo Mensual	Costo Total
ADSL 1 Mbps	$ 150.00	$ 150.00

Cuadro 30. Enlace a Internet – Proyecto Propuesto

Costos de Red

En el proyecto propuesto, el costo será una sola vez, debido a que se dejará de lado los patch core, por tal motivo se tiene el siguiente costo de red:

Enlace	Costo Único	Costo Total
Cable UTP cat. 5e cableado AP's	$ 200.00	$ 200.00

Cuadro 31. Costo de Red – Proyecto Propuesto

Imprevistos

Se tomará como referencia el 5% del costo total del proyecto para imprevistos.

Costo Total del Proyecto Propuesto

Con los costos anteriormente descritos el costo del proyecto propuesto será de:

Subtotal Costo Proyecto Propuesto→		$1821.00
Imprevistos (5%)	→	$ 91.05
COSTO PROYECTO PROPUESTO →		**$ 1912.05**

Análisis Costo – Beneficio

En la actualidad se tiene mayor gasto en material de oficina y especialmente en costos de red, al ejecutar el proyecto propuesto se tendrá un beneficio en el egreso económico de costo de red debido a que ya no se tendrá que estar reponiendo o cambiando los patch core; mientras que en los materiales de oficina de igual manera se tendrá disminución en costos por la mejora con el proyecto propuesto.

El mayor beneficio se verá en la satisfacción de los clientes al poder contar con un servicio de acceso al Internet con seguridad, velocidad y sobre todo con acceso en cualquier lugar del edificio de la empresa Emperador Hotel Casino.

Análisis de Riesgos

El concepto de riesgo está presente en la totalidad de las actividades que realiza el ser humano, por lo que antes de implementar cualquier mecanismo de seguridad (software, hardware, política, etc.) en las Tecnologías de la Información, es necesario conocer la prioridad de aplicación y que tip de medida puedo aplicar. El análisis de riesgos es el primer paso de la seguridad informática.

Un riesgo es un evento, el cual es incierto y tiene un impacto negativo. Análisis de riesgo es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. Las metodologías de análisis de riesgos existentes describen sus etapas en forma teórica, se presentan pocos ejemplos o es necesario una herramienta para realizarlo, cuyo costo normalmente es elevado. Por lo anterior es necesario establecer una metodología cualitativa práctica para realizar un análisis de riesgos a la áreas de TI, estableciendo el cómo puede ejecutarse el análisis.

La gestión de los riesgos

El principal objetivo de la administración de riesgos, como primera ley de la naturaleza, es garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radican en la ausencia de objetivos claros.

La administración de riesgos es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

Los objetivos de la administración de riesgos están formalizados en una *"política corporativa de administración de riesgos"*, la cual describe las políticas y medidas tomadas para su consecución. Idealmente los objetivos y las políticas de administración de riesgos deben ser producto de las decisiones de la Alta Dirección de la compañía.

La administración de riesgos se ha considerado como un área funcional especial de la organización, por lo cual se han ido formalizando sus principios y técnicas.

El factor más importante para determinar cuáles riesgos requieren alguna acción específica es el máximo potencial de pérdida, algunas pérdidas pueden ser potencialmente devastadoras literalmente fuera del alcance de la organización

mientras tanto otras envuelven menores consecuencias financieras, si el máximo potencial de pérdida de una amenaza es grande, la perdida sería inmanejable, por lo que el riesgo requiere de un tratamiento especial.

Los Riesgos Informáticos

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

Viendo la necesidad en el entorno empresarial de este tipo de herramientas y teniendo en cuenta que, una de las principales causas de los problemas dentro del entorno informático, es la inadecuada administración de riesgos informáticos, esta información sirve de apoyo para una adecuada gestión de la administración de riesgos, basándose en los siguientes aspectos:

La evaluación de los riesgos inherentes a los procesos informáticos.

- ✓ La evaluación de las amenazas ó causas de los riesgos.
- ✓ Los controles utilizados para minimizar las amenazas a riesgos.
- ✓ La asignación de responsables a los procesos informáticos.
- ✓ La evaluación de los elementos del análisis de riesgos.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

- ✓ Personas tanto internas como externas de la organización.
- ✓ Desastres naturales.
- ✓ Por servicios, suministros y trabajos no confiables e imperfectos.
- ✓ Por la incompetencia y las deficiencias cotidianas.
- ✓ Por el abuso en el manejo de los sistemas informáticos.

- ✓ Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

Todos estos aspectos hacen que sea necesario replantear la seguridad con que cuenta hasta ahora la organización, aunque también hay algunas entidades que están haciendo un trabajo prominente en asegurar sus sistemas informáticos.

Es fundamental que los directivos de las organizaciones que no se han ocupado lo suficiente en implementar un estricto sistema de seguridad se preocupen en:

- ✓ Reconocer la necesidad de establecer normas de seguridad para los datos, políticas, normas y directrices.
- ✓ Comprender que el papel que desempeñan en la organización, está relacionado con la seguridad del ciclo de vida del sistema de información.
- ✓ Establecer una planificación formalizada para la seguridad informática.
- ✓ Gestionar los medios necesarios para administrar correctamente la función de la seguridad informática.

Riesgos relacionados con la Informática

En efecto, las principales áreas en que habitualmente ha incursionado la seguridad en los centros de cómputos han sido:

- ✓ Seguridad física.
- ✓ Control de accesos.
- ✓ Protección de los datos.
- ✓ Seguridad en las redes.

Por tanto se ha estado descuidando otros aspectos intrínsecos de la protección informática y que no dejan de ser importantes para la misma organización, como por ejemplo

- ✓ Organización y división de responsabilidades

- ✓ Cuantificación de riesgos
- ✓ Políticas hacia el personal
- ✓ Medidas de higiene, salubridad y ergonomía
- ✓ Selección y contratación de seguros
- ✓ Aspectos legales y delitos
- ✓ Estándares de ingeniería, programación y operación
- ✓ Función de los auditores tanto internos como externos
- ✓ Seguridad de los sistemas operativos y de red
- ✓ Plan de contingencia

Otra falencia es desconocer las relaciones existentes entre los elementos y factores de la seguridad. El resultado a todo esto es: "una perspectiva limitada de la seguridad informática para la organización".

A los fines de llevar una revisión completa y exhaustiva de este tema, se propone que los especialistas en seguridad informática apliquen un enfoque amplio e integral, que abarque todos los aspectos posibles involucrados en la temática a desarrollar, identificando aquellos concernientes a garantías y resguardos, y, después de haber efectuado un análisis exhaustivo de los mismos, presentarlos en detalle y agrupados convenientemente.

Los principales riesgos informáticos de los negocios son los siguientes:

Riesgos de Integridad: Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

- ✓ Interface del usuario: Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.

- ✓ Procesamiento: Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.

- ✓ Procesamiento de errores: Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (Exceptions) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

- ✓ Interface: Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.

- ✓ Administración de cambios: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuada de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.

- ✓ Información: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos

riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: Errores de programación (buena información es procesada por programas mal construidos), procesamiento de errores (transacciones incorrectamente procesadas) ó administración y procesamiento de errores (Administración pobre del mantenimiento de sistemas).

Riesgos de relación: Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

Riesgos de acceso: Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

- ✓ Procesos de negocio: Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.
- ✓ Aplicación: La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
- ✓ Administración de la información: El mecanismo provee a los usuarios acceso a la información específica del entorno.
- ✓ Entorno de procesamiento: Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

- ✓ Redes: En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
- ✓ Nivel físico: Protección física de dispositivos y un apropiado acceso a ellos. Algunos de los métodos de prevenir el acceso ilegal a los servicios informáticos incluyen:
    - o Claves y contraseñas para permitir el acceso a los equipos.
    - o Uso de cerrojos y llaves.
    - o Fichas ó tarjetas inteligentes.
    - o Dispositivos biométricos (Identificación de huellas dactilares, lectores de huellas de manos, patrones de voz, firma/escritura digital, análisis de pulsaciones y escáner de retina, entre otros).

Riesgos de utilidad: Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- ✓ Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- ✓ Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- ✓ Backups y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos en la infraestructura: Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, etc.). Estos riesgos son generalmente se consideran en el contexto de los siguientes procesos informáticos:

- ✓ Planeación organizacional: Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología

informática en el negocio. Además, verifica si existe una adecuada organización (gente y procesos) asegura que los esfuerzos de la tecnología informática será exitosa.

- ✓ Definición de las aplicaciones: Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos procesos abarcan: la determinación de comprar una aplicación ya existente ó desarrollar soluciones a cliente. Estos procesos también aseguran que cualquier cambio a las aplicaciones (compradas o desarrolladas) sigue un proceso definido que confirma que los puntos críticos de proceso/control son consistentes (Todos los cambios son examinados por usuarios antes de la implementación)

- ✓ Administración de seguridad: Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.

- ✓ Operaciones de red y computacionales: Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado. También aseguran que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.

- ✓ Administración de sistemas de bases de datos: Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición,

correspondan con los requerimientos y reduzcan el potencial de redundancia.

- ✓ Información / Negocio: Los proceso en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.

Riesgos de seguridad general: Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- ✓ Riesgos de choque de eléctrico: Niveles altos de voltaje.
- ✓ Riesgos de incendio: Inflamabilidad de materiales.
- ✓ Riesgos de niveles inadecuados de energía eléctrica.
- ✓ Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- ✓ Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

Seguidamente veremos otros riesgos que afectan a la protección informática puesto que aumentan los puntos de vulnerabilidad de los sistemas.

Concentración de procesamiento de aplicaciones más grandes y de mayor complejidad: Una de las causas más importantes del incremento en los riesgos informáticos probablemente sea el aumento en la cantidad de aplicaciones o usos que se le da a las computadoras y la consecuente concentración de información y tecnología de software para el procesamiento de datos, generalmente la información y programas están concentrados en las manos de pocas personas.

Como consecuencia de ello, se corre el riesgo de sufrir lo que en la jerga de seguridad informática suele denominarse "Amnesia Corporativa" debido a algún desastre ocurrido en las computadoras, y de quedar expuesta a una suspensión prolongada del procesamiento y por ende el mal funcionar de la compañía generándose una situación de caos para la misma y en todos los niveles de la organización.

Dependencia en el personal clave: Además del peligro que encierra algún desastre en los sistemas informáticos, existen otras situaciones potencialmente riesgosas de las cuales la más importante es, quizá, la dependencia hacia individuos clave. La dependencia en individuos clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone a la compañía en manos de relativamente pocas personas, siendo que éstas por lo general son externos a la organización. Este tipo de situaciones ha conducido a situaciones donde las empresas se han visto expuestas al chantaje, la extorsión, mal uso y fraudes en la explotación de los sistemas informáticos.

La amenaza no solo se restringe al abuso del tipo descrito aquí. Este personal especializado con frecuencia posee el conocimiento único y no registrado de las modificaciones o el funcionamiento de las aplicaciones. La supervisión y el control de su trabajo resulta difícil como lo es el conocimiento de lo que si funcionaría sin contar con las habilidades del especialista.

Desaparición de los controles tradicionales: Muchas de las nuevas y extensas aplicaciones omiten las auditorías tradicionales y los controles impresos por razones de volumen. Las aplicaciones contienen verificadores automáticos que aseguran la integridad de la información que se procesa. Este gran cambio en el criterio sobre el control de los empleados y las brechas respecto a la comunicación, crean situaciones de seguridad totalmente diferentes.

Huelgas, terrorismo e inestabilidad social: El nivel actual de riesgo en computación se debe revisar también dentro del contexto de inestabilidad social en muchas partes del mundo. Ha habido ataques físicos a diversas instalaciones, sin embargo algunas veces se trata de la incursión de personal interno y no de agitadores. Este tipo insidioso de riesgo es, en potencia, la fuente de más alto perjuicio para la institución. Este riesgo, solo, genera una amplia posibilidad de nuevas amenazas ante las cuales hay que responder.

Los ataques internos por parte del personal de una institución pueden tomar la forma de huelga; ésta, aunque no sea violenta, puede ser tan perjudicial como el ataque físico. Las huelgas han sucedido en grandes instalaciones que operan en línea en diferentes partes del mundo y por tanto en nuestro país también.

Mayor conciencia de los proveedores: Hasta hace pocos años este tema no constituía motivo de gran preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación acerca de la seguridad. Como resultado, se dispone de un mayor número de publicaciones de alta calidad para los usuarios, lo que permite mejorar la estructura y el enfoque para la seguridad de las computadoras; asimismo, ha intensificado el interés por reducir en forma progresiva el riesgo causado por un desastre en las computadoras.

Matriz para el análisis de Riesgo

La Matriz para el Análisis de Riesgo, es producto del proyecto de Seguimiento al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras" La Matriz, no dará un resultado detallado sobre los riesgos y peligros de cada recurso (elemento de información) de la institución, sino una mirada aproximada y generalizada de estos.

Hay que tomar en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas, es decir terminaríamos con un sinnúmero de grafos de riesgo que deberíamos analizar y clasificar.

Con la Matriz se pretende localizar y visualizar los recursos de la empresa, que están más en peligro de sufrir un daño por algún impacto negativo, para

posteriormente ser capaz de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

Fundamento de la Matriz

La Matriz se basa en el método de Análisis de Riesgo con un grafo de riesgo, usando la formula **Riesgo = Probabilidad de Amenaza x Magnitud de Daño**
La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente

- ✓ 1 = **Insignificante** (incluido Ninguna)
- ✓ 2 = **Baja**
- ✓ 3 = **Mediana**
- ✓ 4 = **Alta**

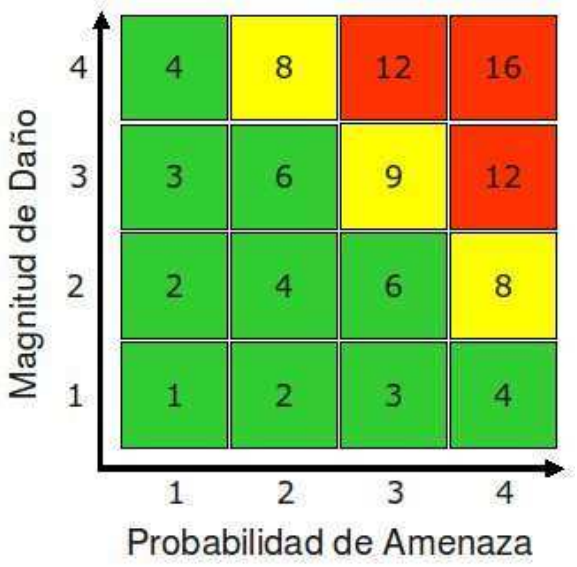


Gráfico 26. Matriz análisis de Riesgo

El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

- ✓ **Bajo Riesgo** = 1 – 6 (verde)
- ✓ **Medio Riesgo** = 8 – 9 (amarillo)
- ✓ **Alto Riesgo** = 12 – 16 (rojo)

Análisis de Riesgo

El análisis de riesgo consta de tres elementos de información:

- ✓ Información de datos e informaciones
- ✓ Información de sistemas e infraestructura
- ✓ Información de personal

Cada uno de estos tres elementos tiene grupos de amenazas, los cuales son tres:

- ✓ Actos originados por la criminalidad común y motivación política
- ✓ Sucesos de origen físico
- ✓ Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales.

Información de Datos e Informaciones

En esta información se observa los resultados luego del análisis **ANEXO 2**.

Los resultados para las amenazas en Información de datos e informaciones:

Actos originados por la criminalidad común y motivación política

En las amenazas Robo/hurto de información electrónica e intrusión a red interna los elementos que tienen mayor riesgo son:

- ✓ Documentos institucionales
- ✓ Finanzas
- ✓ Productos institucionales
- ✓ Bases de datos internas
- ✓ Infraestructura (planes, documentación)
- ✓ Informática (planes, documentación, etc.)
- ✓ Chat externo
- ✓ Llamadas telefónicas externas

En estos elementos el grado de riesgo es de 12 lo que implica una amenaza muy alta de sufrir estos riesgos.

Sucesos de origen físico

Los sucesos de origen físico en los cuales se obtuvo una magnitud de riesgo mediana fueron:
Las amenazas: Inundación/deslave, sismo, polvo, falta de ventilación

- ✓ Documentos institucionales
- ✓ Finanzas
- ✓ Productos institucionales
- ✓ Bases de datos internas
- ✓ Infraestructura (planes, documentación)
- ✓ Informática (planes, documentación, etc.)
- ✓ Chat externo
- ✓ Llamadas telefónicas externas

En los sucesos físicos se toma en cuenta la ubicación de la empresa, la ubicación de oficinas, habitaciones, los desastres naturales latentes (volcán Tungurahua, inundaciones); es por esto que los riesgos en estas amenazas son de nivel **Mediano.**

Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales.

Dentro de las amenazas que tienen mayor riesgo se tiene: Utilización de programas no autorizados, software pirateado; dando como consecuencia los siguientes elementos que están en riesgo:

- ✓ Documentos institucionales
- ✓ Finanzas
- ✓ Productos institucionales
- ✓ Bases de datos internas

- ✓ Infraestructura (planes, documentación)
- ✓ Informática (planes, documentación, etc.)
- ✓ Chat externo
- ✓ Llamadas telefónicas externas

El valor obtenido de 12 da como resultado que estos elementos de la empresa son los que tienen mayor riesgo, y a los que se tiene que dar más importancia al momento de realizar las políticas internas, las seguridades internas y externas.

Sistemas e Infraestructura

En esta información se observa los resultados luego del análisis **ANEXO 3**.

Los resultados para las amenazas en Sistemas e Infraestructura:

Actos originados por la criminalidad común y motivación política

En las amenazas Daños por vandalismo, Fraude/estafa, Robo/hurto (físico), Robo /Hurto de información electrónica, intrusión a red interna, Infiltración, virus-ejecución no autorizado de programas y violación de derechos de autor los elementos que tienen mayor riesgo son:

- ✓ Equipos de red cableada (router, switch, etc.)
- ✓ Equipos de red inalámbrica (router, punto de acceso, etc.)
- ✓ Cortafuego
- ✓ Servidores
- ✓ Memorias portátiles

En este análisis es donde se encuentra el mayor riesgo dentro de la empresa ya que en las amenazas Robo/hurto de información electrónica e intrusión a red interna se tiene el mayor valor que es de 16, es decir probabilidad de amenaza **ALTA**. Mientras que los demás elementos tienen igual una mayor probabilidad de amenaza con un valor de 12 que también da una probabilidad **ALTA**.

Para los elementos siguientes elementos las amenazas Robo/hurto de información electrónica e intrusión a red interna son las que tienen una probabilidad **ALTA** de producirse ya que tienen un valor de 12.

- ✓ Programas de administración (contabilidad, hotelero, RRHH, etc.)
- ✓ Programas de manejo de proyectos
- ✓ Programas de producción de datos
- ✓ PBX (sistema de telefonía convencional)
- ✓ Celulares

Sucesos de origen físico

Los sucesos de origen físico en los cuales se obtuvo una magnitud de riesgo **ALTA** fueron:

Las amenazas: Inundación/deslave, sismo, polvo, falta de ventilación

- ✓ Equipos de red cableada (router, switch, etc.)
- ✓ Equipos de red inalámbrica (router, punto de acceso, etc.)
- ✓ Cortafuego
- ✓ Servidores
- ✓ Memorias portátiles

En los sucesos físicos se toma en cuenta la ubicación de la empresa, la ubicación de oficinas, ubicación de equipos, habitaciones, los desastres naturales latentes (volcán Tungurahua, inundaciones); es por esto que los riesgos en estas amenazas son de nivel **ALTO** al tener un valor de 12**.**

Un análisis de riesgo importante también es con las amenazas Electromagnetismo, sobrecarga eléctrica, falla de corriente (apagones), falla de sistema/disco duro ya que en los siguientes elementos obtuvo una probabilidad de riesgo de valor 8 es decir **MEDIANO** y se deberá tomar muy en cuenta para el análisis.

- ✓ Equipos de red cableada (router, switch, etc.)
- ✓ Equipos de red inalámbrica (router, punto de acceso, etc.)
- ✓ Cortafuego

- ✓ Servidores
- ✓ Memorias portátiles

Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales

Dentro de las amenazas que tienen mayor riesgo con un valor de 16 que dan una probabilidad de riesgo **ALTA** se tiene: Utilización de programas no autorizados, infección de sistemas a través de unidades portables sin escaneo; dando como consecuencia los siguientes elementos que están en riesgo:

- ✓ Equipos de red cableada (router, switch, etc.)
- ✓ Equipos de red inalámbrica (router, punto de acceso, etc.)
- ✓ Cortafuego
- ✓ Servidores
- ✓ Memorias portátiles

Además las amenazas Falta de inducción, capacitación y sensibilización sobre riesgos, mal manejo de sistemas y herramientas, pérdida de datos, manejo inadecuado de datos críticos, unidades portables con información sin cifrado, transmisión no cifrada de datos críticos, manejo inadecuado de contraseñas, compartir contraseñas o permisos a terceros no autorizados, red inalámbrica expuesta al acceso no autorizado dan una probabilidad de riesgo **ALTA** al tener un valor 12 en elementos como:

- ✓ Equipos de red cableada (router, switch, etc.)
- ✓ Equipos de red inalámbrica (router, punto de acceso, etc.)
- ✓ Cortafuego
- ✓ Servidores
- ✓ Memorias portátiles

Otros elementos que dan una probabilidad **ALTA** al obtener valor 12 dentro de las amenazas Utilización de programas no autorizados/software pirateado e infección de sistemas a través de unidades portables sin escaneo son:

- ✓ Programas de administración (contabilidad, hotelero, RRHH, etc.)
- ✓ Programas de manejo de proyectos
- ✓ Programas de producción de datos
- ✓ PBX (sistema de telefonía convencional)
- ✓ Celulares

Los valores obtenidos dan como resultado que estos elementos de la empresa son los que tienen mayor riesgo, y a los que se tiene que dar más importancia al momento de realizar las políticas internas, las seguridades internas y externas.

Personal

En esta información se observa los resultados luego del análisis **ANEXO 4**.

Los resultados para las amenazas en Personal:

Actos originados por la criminalidad común y motivación política

En las amenazas Robo /Hurto de información electrónica, intrusión a red interna, el elemento que tienen mayor riesgo es:

- ✓ Administración

Este elemento tiene un valor de 16 probabilidad de riesgo **ALTA** . Además tiene un valor de 12 que sigue siendo probabilidad de riesgo **ALTA** en los siguientes amenazas: Daños por vandalismo, fraude/estafa, robo/hurto (físico), infiltración, virus/ejecución no autorizado de programas, violación a derechos de autor.

En las amenazas Robo /Hurto de información electrónica, intrusión a red interna, los elementos que tienen mayor riesgo con un valor de 12, es decir una probabilidad ALTA de riesgo son:

- ✓ Junta Directiva
- ✓ Dirección/coordinación
- ✓ Recepción
- ✓ Piloto/conductor
- ✓ Informática/soporte técnico

Sucesos de origen físico

Los sucesos de origen físico en los cuales se obtuvo una magnitud de riesgo **ALTO** fueron:
Las amenazas: Inundación/deslave, sismo, polvo, falta de ventilación

- ✓ Administración

En los sucesos físicos se toma en cuenta la ubicación de la empresa, la ubicación de oficinas, ubicación de equipos, habitaciones, los desastres naturales latentes (volcán Tungurahua, inundaciones); es por esto que los riesgos en estas amenazas son de nivel **ALTO** al tener un valor de 12**.**

Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales

Dentro de las amenazas que tienen mayor riesgo con un valor de 16 que dan una probabilidad de riesgo **ALTA** se tiene: Utilización de programas no autorizados, infección de sistemas a través de unidades portables sin escaneo; estas dos amenazas se encuentran con mayor riesgo en el elemento de:

- ✓ Administración

Además este elemento **ADMINISTRACIÓN** con las amenazas Falta de inducción, mal manejo de sistemas y herramientas, pérdida de datos, manejo

inadecuado de datos críticos, unidades portables con información sin cifrado, transmisión no cifrada de datos críticos, manejo inadecuado de contraseñas, compartir contraseñas o permisos a terceros no autorizados, red inalámbrica expuesta al acceso no autorizado; tiene una probabilidad de riesgo **ALTA** al tener un valor 12.

Otros elementos que dan una probabilidad **ALTA** al obtener valor 12 dentro de las amenazas Utilización de programas no autorizados/software pirateado e infección de sistemas a través de unidades portables sin escaneo son:

- ✓ Junta Directiva
- ✓ Dirección/coordinación
- ✓ Recepción
- ✓ Piloto/conductor
- ✓ Informática/soporte técnico

Los valores obtenidos dan como resultado que estos elementos de la empresa son los que tienen mayor riesgo, y a los que se tiene que dar más importancia al momento de realizar las políticas internas, las seguridades internas y externas.

Análisis de Riesgo Promedio

A continuación en una matriz resumida indica el Análisis de Riesgo Promedio con la Probabilidad de Amenaza y la Magnitud de daño

Análisis de Riesgo promedio				
		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de Daño	Datos e Información	6,2	5,4	5,2
	Sistemas e Infraestructura	7,4	6,4	6,1
	Personal	7,0	6,0	5,8

Gráfico 27. Análisis de Riesgo Promedio

Se observa en el gráfico 27, que la probabilidad de amenaza Criminalidad y Político dentro del elemento Sistemas e Infraestructura tiene un promedio de 7.4 que indica que la probabilidad de Riesgo es **MEDIANA**.

Un punto importante también es la probabilidad de Amenaza en Criminalidad y Político en Magnitud de daño Personal ya que se encuentra en el límite con un valor de 7 acercándose a una probabilidad de Riesgo **MEDIANA**.

Se observa en el gráfico 28, Análisis de Factores de Riesgo que se tiene una magnitud de daño **MEDIANA** para el elemento Sistemas e Infraestructura en las amenazas Criminalidad y Político, Sucesos de Origen crítico y Negligencia Institucional.

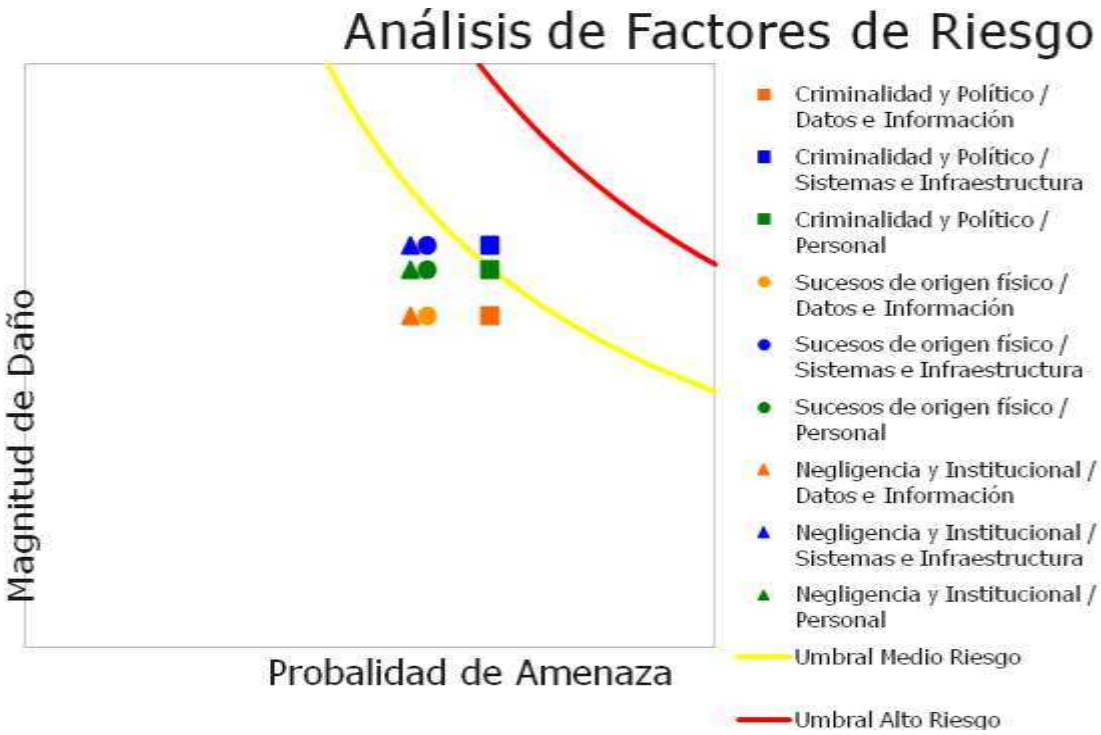


Gráfico 28. Análisis de Factores de Riesgo

Por todo lo expuesto, resulta más que obvio la necesidad de un nuevo modelo de seguridad que cubra tanto los aspectos conocidos o clásicos como aquellos no convencionales, además de que los tratados que se han desarrollado sobre seguridad enfocan su atención únicamente en aquellos aspectos

tradicionales dejando por consiguiente una brecha de vulnerabilidad en la organización al no cubrir por completo los aspectos de protección relacionados a la misma. Podemos entonces aseverar que este accionar trae consigo que la compañía sea vulnerable.

Fundamentación

Metodología

La metodología a utilizar se presenta a continuación:

1. Para la evaluación de la Dirección de Informática se llevarán a cabo las siguientes actividades:
   - ✓ Solicitud de los estándares utilizados y programa de trabajo
   - ✓ Aplicación del cuestionario al personal
   - ✓ Análisis y evaluación de la información
   - ✓ Elaboración del informe

2. Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:
   - ✓ Solicitud del análisis y diseño de los sistemas en desarrollo y en operación
   - ✓ Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)
   - ✓ Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)
   - ✓ Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos
   - ✓ Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado
   - ✓ Entrevista con los usuarios de los sistemas
   - ✓ Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario

- ✓ Análisis objetivo de la estructuración y flujo de los programas
- ✓ Análisis y evaluación de la información recopilada
- ✓ Elaboración del informe

3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:
   - ✓ Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización
   - ✓ Solicitud de contratos de compra y mantenimientos de equipo y sistemas
   - ✓ Solicitud de contratos y convenios de respaldo
   - ✓ Solicitud de contratos de Seguros
   - ✓ Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad Visita técnica de comprobación de seguridad física y lógica de la instalaciones de la Dirección de Informática
   - ✓ Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado
   - ✓ Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación

Políticas de seguridad de la empresa

La seguridad de la red es un proceso o acción para prevenir el uso desautorizado de su computadora y no sufrir invasión a la privacidad teniendo en cuenta los peligros que los usuarios pueden tener si no están bien informados.

La seguridad de la red es una característica prominente de la red asegurando responsabilidad, confidencialidad, integridad y sobretodo protección contra muchas amenazas externas e internas tales como problemas basados en email de la seguridad de red ,virus, spam, los gusanos ,los troyanos y intentos de ataques de seguridad, etc.

La información sobre los diversos tipos de prevención debe de estar actualizados de acuerdo para garantizar su funcionamiento. El no tener una buena seguridad en la red implica que un hacker pueda acceder fácilmente a la red interna. Esto habilitaría a un atacante sofisticado, leer y posiblemente filtrar correo y documentos confidenciales; equipos basura, generando información; y más. Por no mencionar que entonces utilice su red y recursos para volverse e iniciar el ataque a otros sitios, que cuando sean descubiertos le apuntarán a usted y a su empresa, no al hacker.

Debemos tener en cuenta que tampoco es muy fiable conformarse con un antivirus ya que a no son capaces de detectar todas las amenazas e infecciones al sistema además son vulnerables desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún, A veces los métodos más óptimos para la seguridad de redes son muy incómodos ya que dejan a los usuarios sin muchos permisos.

Algunas recomendaciones para los usuarios:

- ✓ No revelar su contraseña a nadie
- ✓ Cambiar de contraseñas cada cierto tiempo.
- ✓ Disminuir la cantidad de correos basuras.
- ✓ No responder a cadenas.
- ✓ Mantener las soluciones activadas y actualizadas.
- ✓ Evitar realizar operaciones comerciales en computadoras de uso público.
- ✓ Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.
- ✓ Usar Penetration Testing (método para probar la seguridad en la red)

Documentos existentes

La seguridad en la empresa Emperador Hotel Casino cuenta con documentación de seguridad interna la cual tiene como principal punto la prohibición de utilizar

cualquier tipo de información fuera de la empresa o que se suministre información a terceros ajenos a la institución.

Protecciones generales

Consideraciones de software

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos).

Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.
Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus A.

Las contraseñas:

Un aspecto importante en la seguridad es la mala política en el manejo de contraseñas. Una buena política incluye rotar contraseñas al menos cada mes, utilizar contraseñas con al menos 8 caracteres mezclando alfanuméricos, mayúsculas y minúsculas y otros caracteres ASCII, evitando utilizar datos personales como referencias.

Uso de congeladores:

Este es unos de los métodos más eficaces y uno de los más utilizados ya que no permite la entrada ni salida de ningún virus ni archivo malicioso, aunque a veces suele ser muy incomodo ya que quita algunos permisos al usuario.

Usuarios (identificación)

La política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red. La siguiente es una lista de los aspectos de las responsabilidades de los usuarios:

- ✓ Lineamientos acerca del uso de los recursos de red, tales como que los usuarios estén restringidos.
- ✓ Que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.
- ✓ Está permitido que los usuarios compartan cuentas o permitan a otros usar la suya.
- ✓ Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas.
- ✓ Política de contraseña de usuario: con qué frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hay al respecto.
- ✓ Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema.
- ✓ Consecuencias para los usuarios que divulguen información que pueda estar patentada. Que acciones legales u otros castigos pueden implantarse.
- ✓ Una declaración sobre la privacidad del correo electrónico (Ley de Privacidad en las Comunicaciones Electrónicas)
- ✓ Una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión.
- ✓ Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

Aspectos generales

Firewalls

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Access Control Lists (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

Wrappers

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- ✓ Debido a que la seguridad lógica está concentrada en un solo programa, los Wrappers son fáciles y simples de validar.
- ✓ Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper.

- ✓ Debido a que los Wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- ✓ Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorias de peticiones a dichos servicios, ya sean autorizados o no.

Sistemas Anti-Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo), y el tráfico de datos en ella.

Filtros de seguridad

CyberSitter ofrece a los guardianes la habilidad de controlar el acceso a material inapropiado en la Red. Este material puede incluir esta clase de sitios:

- ✓ Material Sexual para Adultos
- ✓ Actividades ilegales como drogas
- ✓ Violencia Adulta
- ✓ Armas Ilegales/Violencia
- ✓ Odio/Intolerancia

Se puede optar por bloquear el acceso a cierto material específico, o bloquear horarios específicos o días que no deban tener acceso a la Red.

Anti Phishing

Es un filtro de suplantación de identidad incluye varias tecnologías pendientes de patente diseñadas para avisarle o bloquear su equipo frente a sitios web potencialmente malintencionados.

El Filtro de suplantación de identidad (phishing) ofrece una nueva tecnología dinámica para protegerle del fraude en Internet y del riesgo de robo de datos personales. Las estafas conocidas como "phishing" normalmente intentan atraerle para que visite sitios Web falsos donde se puede recopilar su información personal o de tarjeta de crédito para fines delictivos. Esta forma de robo de identidad está aumentando rápidamente en Internet.

1. **Un filtro integrado** en el explorador que examina las direcciones URL y las páginas web visitadas en busca de características asociadas a fraudes en línea conocidos o estafas de suplantación de identidad (phishing), y le avisa si los sitios que visita son sospechosos.

2. **Un servicio en línea** para ayudarle a bloquear su equipo ante las estafas confirmadas con información actualizada sobre los sitios web de suplantación de identidad (phishing) notificados. Los sitios de suplantación de identidad (phishing) suelen aparecer y desaparecer en un plazo de 24 a 48 horas, por lo que resulta esencial disponer de información actualizada para su protección.

3. **Una forma integrada de informar acerca de sitios sospechosos o estafas.** Con el Filtro de suplantación de identidad (phishing), podrá facilitar valiosa información acerca de cualquier sitio web que crea potencialmente fraudulento. Basta con que envíe la información a Microsoft y Microsoft la evalúa. Si dicha información se confirma, el servicio en línea la agrega a la base de datos para proteger a la comunidad de usuarios de Internet Explorer y la Barra de herramientas de Windows Live.

Antivirus

Los antivirus nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos, durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo, desinfectar y prevenir una infección de los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como Heurística, HIPS, etc.

Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demanda (los conocidos scanners, exploradores, etc), y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

Actualmente hay una gran mayoría de antivirus pero no todos se asemejan al pretendido por todos, un antivirus eficaz en todos los sentidos.

Su función:

Muchas veces las personas se preguntan cómo funciona un antivirus debido a que tienen que verificar cada archivo de las computadoras si están infectadas, puede haber una teoría de que un antivirus es creado con una lista de códigos maliciosos en lo que lleva al antivirus a examinar en la base de datos de un archivo, si en la lista de códigos maliciosos hay un código en el que está en un archivo, este será reconocido como un virus informático.

Daños:

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, baja en el rendimiento del equipo, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir replicándose en otras partes del sistema de información. Las redes en la actualidad ayudan a dicha propagación.

Los daños que los virus dan a los sistemas informáticos son:

- ✓ Pérdida de información (evaluable y actuable según el caso)
- ✓ Horas de contención (Técnicos de SI, Horas de paradas productivas, perdida productiva, tiempos de contención o reinstalación, cuantificables según el caso+horas de asesoría externa)
- ✓ Pérdida de imagen (Valor no cuantificable)

También es importante tener en cuenta que existen algunos malware que tienen la capacidad de ocultar carpetas y archivos.

Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar a priori lo que puede costar una intervención. Tenemos que

encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias.

Tipos o clases de antivirus

Por lo tanto, ¿qué tipo de herramientas de seguridad informática existen?: sencillamente, todas las aplicaciones "anti", como ser:

- ✓ Antivirus
- ✓ Cortafuegos
- ✓ Antiespias
- ✓ Antipop-ups
- ✓ Antispam

Acceso a páginas seguras

Como ya se dijo, uno de los más grandes problemas sobre la violación a la privacidad es por causa de la poca importancia que se le da a los spam y a los virus que estos pueden contraer, troyanos, Básicamente existen dos tipos, más comunes, del robo de información.

En primer lugar tenemos a los spam. Estos son avisos publicitarios lo cuales apresen en nuestro computador de forma inautorizada. En su mayoría estos avisos aparecen con más frecuencia cuado se visita lugares, páginas Web, que no nos proporcionan la seguridad adecuada, tales como páginas pornográficas, paginas musicales, etc. Según FERNANDO TRICAS GARCÍA de la Universidad de Zaragoza, los spam no solo son avisos indeseables, sino también pueden llegar a tomar una conducta espía donde la víctima es la persona que accede al spam.

(Los spams) Merecen una mención especial el correo no solicitado, también conocido como spam. Aunque en la mayoría de los casos podemos considerarlo una simple molestia (borrar unos cuantos mensajes que no nos interesan), en

algunos casos puede suponer un compromiso, cuando menos a nuestra intimidad: puede utilizarse, con mensajes especialmente preparados, para averiguar hábitos de lectura de correo, el tipo de conexión que utilizamos y mucha más información.

Por este motivo, es importante no acceder a los spam ya podríamos ser víctimas de robos de nuestras contraseñas o pass Word

No pinchar en las direcciones que nos envían por correo electrónico (se han dado casos de estafa: el truco consiste en que nosotros vemos una dirección en el mensaje, pero cuando pinchamos vamos a otra diferente). Es mejor copiar y pegar, o ir directamente al sitio de nuestro banco (o cualquier otro servicio) y navegar normalmente ahí; en caso de necesidad, copiar y pegar en el navegador, no pinchar).

Por otro lado, no solo podremos encontrar spams al momento de navegar en lugares poco confiables, sino también los famosos Troyanos o caballos de Troya. Es tos son virus, que se instalan en su computador. La principal tarea de este tipo de virus es la de robar información, tales como hábitos con su computador conversaciones por Chat, registro de claves de sistema y/o claves de tarjetas de crédito. Esto para después mandarlo a las personas creadoras de dichos virus. Por esta razón, es muy importante no acceder a páginas poco confiables, no abrir o descargar spams, y mantener actualizado el computador, los antivirus, para que la base de datos del antivirus pueda reconocer a los nuevos Troyanos que puede hacer daño su intimidad.

Normativas de seguridad

A continuación se presentan algunos puntos que es importante tomar en cuenta para disminuir el impacto de un suceso de criminalidad que afecte a las organizaciones:

- No se recomienda usar computadoras portátiles como estaciones de trabajo: lo más seguro sería usar computadoras de escritorio y usar laptops

sólo cuando se necesita ir a algún lugar a hacer una presentación o a trabajar fuera de la oficina. De otra manera, estaríamos llevando en las portátiles demasiada información sensible.

La información debe ir cifrada siempre: Si la información que va en una computadora portátil está cifrada, la pérdida del equipo no implicará el acceso de la información por terceras personas. Esto mismo aplica para las memorias usb y los discos de respaldo.

- ✓ Es necesario tener un adecuado respaldo de contraseñas: en todas las organizaciones hay personas claves que tienen acceso a las contraseñas, sin embargo, no es seguro que una sola maneje todos los datos y no los respalde con otro de los miembros. Si una sola persona maneja mucha información o tiene todas las contraseñas, se convierte en blanco clave para la criminalidad.

- ✓ Cambio de contraseñas: cuando una persona deja de trabajar en la organización deben cambiarse inmediatamente las contraseñas que maneja. Esto supone que existirá además un respaldo de las contraseñas que esta persona usaba y de la nueva contraseña que se genere, para evitar que la persona cierre el acceso a la información e impedir problemas en el futuro. Los respaldos periódicos también previenen la pérdida de información por la salida de miembros del personal.

- ✓ Uso de claves en teléfonos celulares: se recomienda implementar el uso de claves para dificultar (al menos levemente) el robo de los números telefónicos del personal de la organización o de los actores clave de las comunidades y grupos con los que trabajamos.

- ✓ Políticas de contratación del personal: es importante que en nuestras organizaciones conozcamos quiénes son las personas que vamos a contratar. No debemos centrarnos solamente en capacidades profesionales,

también debemos conocer su trayectoria y otros detalles que nos permitan establecer la confianza.

- ✓ Cuando se trabaja en el campo, las personas que salen deben dar todos los detalles del viaje, transporte, hospedaje etcétera para poder monitorear apropiadamente su seguridad.

- ✓ Respaldos: hay que implementar una política de periodicidad fija, que quede claro cuándo se debe respaldar, cómo se resguardarán esos datos y dónde

Amenazas

Abrir archivos desconocidos

Correo Electrónico

Una de las formas más extendidas de propagación de virus y gusanos es a través del correo electrónico. Conviene por tanto filtrar los mensajes entrantes en el perímetro o en los servidores de correo. Siempre, pero especialmente cuando esta precaución resulte imposible, los usuarios deben utilizar con su propio cliente de correo algunas normas básicas de supervivencia.

Nunca abra un archivo adjunto sin escanearlo antes con un antivirus. Conviene instalar un antivirus que disponga de un complemento/plug-in de Outlook Express o que pueda analizar el trafico SMTP/POP/NNTP directamente desde Winsock.

Utilizan todo tipo de método ilegitimo, como aprovecharse de servidores de correo desprotegidos, ordenadores personales de empresas y particulares

infectados con troyanos tipo Back Orifice, sitios Web de envío de postales, cuentas de prueba en proveedores de servicio, etc.

Desde el momento en que se aventura por el ciberespacio, puede recibir correo no solicitado de cualquier empresa, desde su propio proveedor de Internet o de correo Web.

El problema del spam

El spam representa un gran coste para empresas y particulares:

Cuesta Tiempo

Mientras está leyendo las cabeceras y decidiendo si un mensaje es o no spam, se está perdiendo tiempo. Cuanto mayor es el volumen de spam recibido, más tiempo se pierde. Por otro lado, los administradores invierten gran cantidad de horas formándose primero y luchando diariamente contra el spam después.

Suplantación de la identidad

La suplantación de identidad es una forma de robar información personal. Los que hacen este delito se les hace llamar ciberdelincuente.
Los ataques de suplantación de identidad se distribuyen a través de correos electrónicos o falsos anuncios colgados en la Web o las promociones de su vida.

Phishing

Lo que hacen estas personas es enviar mensajes a sus correos electrónicos, con un mensaje similar a los que recibe cotidianamente de los bancos, estas personas envían un mensaje diciendo que tenemos que actualizar urgente los datos de la cuenta bancaria o de lo contrario cerraran la cuenta bancaria, con falsos engaños

para actualizar los datos de la cuenta bancaria ponen al último del mensaje un link, total mente falso, manda a una página similar a la del banco, y hace llenar todos los datos personales, incluyendo el número de cuenta y la contraseña. Y cuando se envía lo que aparece es un mensaje de error o sino que la página está en mantenimiento ó cualquier otra excusa esto lo hacen para despistar pero ya una vez que se envía los datos estos les llegan al ciberdelincuente.

Otra forma que utilizan estos delincuentes son las famosas promociones que se encuentra en cualquier página de la Web, una de las más famosas son la que ha sido ganador de miles de dólares o que ha sido el visitante numero 9999999 y que ha sido ganador de un premio y que si desea cobrar se necesita de una cuenta de ahorros o introducir una tarjeta de crédito para poder cobrar el supuesto premio, lo que hacen estos delincuentes es que se llene otro formulario de preguntas personales pidiendo número de tarjeta y la contraseña, igualmente que el caso anterior la cuenta será vaciada en instantes.

También lo que hace es mandar un mensaje que se ha creado una nueva red social y la cual podría ser unos de los primeros en utilizarlos y en la cual tiene que poner una cuenta de correo electrónico y contraseña supuestamente para agregar a todos su contactos del correo y téngalo por seguro que su cuenta de correo pero hackeada o podría ser mal utilizada como para robar información o ser víctima de sus mensajes que tiene en el correo, por lo general buscan algún correo que tenga algún banco o financiera para poder retirar algún monto de dinero.

Pero esa no son todas las formas hay una que es la que mas esta estafando en este momento y está mandando a la bancarrota a cientos de bancos y casinos en el mundo se trata de la famosas pagina Web clonadas, lo que hacen los ciberdelincuente es crear páginas Web similares a los de los bancos, identidades nacionales , casinos y hasta las paginas en donde se ofrecen novedades , lo que hacen es crear unas páginas similares a las del los bancos o casinos son casi originales y muy difícil de detectar lo que hacen es cambiar una letra del Link

original por otra letra o un punto que alguna cosa extra, para que cualquier persona escribiendo se pueda equivocar ,este es el caso de los bancos.

Y en las páginas de ventas son clonadas para vender el espacio como publicidad para algún SPAM, sino igualmente las paginas originales cuelgan una promoción súper especial ,este es una caso ,un auto deportivo cero kilómetros a un precio de locura y usted por el precio lo decide comprar pero le dicen que tiene que pagar con una tarjeta de crédito y que la entrega será a domicilio totalmente gratis , y usted ilusionado por el súper auto carga su tarjeta a la cuneta del ciberdelincuente y despídase su dinero.

Causas

Las causa se originan por el error humano por abrir esos mensajes de sudosa procedencia o de otro usuario que no conoce hace caso y llena la infamación de sus cuentas mejor averigüen en su banco, o por hacer clic en eso anuncios que le ofrecen la una casa de playa a mitad de precio o el auto que siempre soñó y de los súper premios que supuestamente lo van a hacer millonario.

Consecuencias

Las consecuencias que se puede tener es que perderá los ahorros en unos instantes ó tendrá una deuda de miles de dólares que no compra nada pero en la cuenta crece de montones y podría estar en bancarrota como miles de personas

O invertir en esa casa que ha ahorrado por tanto tiempo y lo puede comprar a mitad precio, o el auto que soñó de niño y está seguro de comprarlo mejor es gastar un poco más en un lugar seguro que en un lugar que desconoce y podría perder no solo el auto sino su dinero.

Interrupción al servicio privado

Hoy en día suele resultar vital para la marcha de muchos negocios disponer de una conexión a Internet ininterrumpida. La mejor manera de asegurar este servicio permanentemente consiste en utilizar conexiones redundantes. Es una buena idea contratar una segunda línea de conexión con un proveedor de servicios de Internet (PSI) diferente. Esta conexión de respaldo no tiene por que ofrecer la misma velocidad que la principal, auque si debería proporcionar un ancho de banda capaz de suplir las necesidades de conectividad en caso de que la línea principal deje de funcionar. Además de contar con una línea duplicada, suele ser necesario replicar todo el equipamiento de red: servidores, routers, switches, tarjetas de red, etc.

Recuperación de sistemas

Cuando todo falla, cuando los archivos han sido destruidos, cuando la información ha desaparecido, solo existe una solución para retomar a la normalidad: tirar de backup, esto es, acudir a las copias de respaldo y restaurar el sistema al estado en que se encontraba cuando se realizo la ultima copia de seguridad.

El respaldo de archivos resulta esencial para asegurar la integridad y disponibilidad de los datos. Los sistemas pueden fallar por muy variadas causas, naturales o provocadas.

Copias de seguridad del sistema de archivos

Todos estos interrogantes vienen a la cabeza cuando uno se plantea como organizar una política de copias de seguridad, tarea nada trivial. A lo largo de esta sección se irá dando respuesta a cada una de las preguntas.

Denegación de servicio

La denegación de servicio es una interrupción del servicio, bien debido a la destrucción del sistema, bien debido a que temporalmente no está disponible. Entre los ejemplos más claros se incluye la destrucción del disco duro de una computadora, los daños en la infraestructura física y el uso de toda la memoria disponible en un recurso.

Muchos de los ataques más comunes son instigados desde protocolos de red, como IP.

Algunos ataques pueden ser evitados aplicando parches del fabricante al software afectado. Muchos fabricantes han parchado sus implementaciones IP para impedir que los intrusos se aprovechen de los fallos de reensamblaje IP. No es posible detener unos pocos ataques, pero si es posible limitar el alcance de las áreas afectadas.

Los efectos de un ataque de inundación SYN de TCP pueden ser mitigados o eliminados limitando el número de conexiones TCP que puede aceptar un sistema, así como reduciendo la cantidad de tiempo que una conexión permanece semiabierta (es decir, el tiempo durante el cual se ha iniciado el intercambio de señales TCP de tres vías, pero no se ha completado). Normalmente, la limitación del número de conexiones TCP se lleva a cabo en los puntos de entrada y salida de las infraestructuras de red corporativas. Una explicación más detallada de los ataques de denegación de servicio más comunes.

Desabilitación de herramientas de seguridad

La Herramienta de seguridad es una opción que nos ayuda a tener el ordenador actualizado para que cada vez que encuentre una amenaza lo expulse automáticamente por medio del Internet.

En primer lugar, es vital que se instale un cortafuego (firewall) la característica de esta aplicación es la de permitirnos el acceso a través de puertos y protocolos permitidos por nosotros, de forma que cualquier intento de acceso extraño puede ser detectado y evitado para eso tiene que siempre estar activado.

Y es la única opción que nos viene gratis en el servicio de Windows y casi en todos los servidores viene activado y cada vez que encuentra una amenaza lo elimina instantáneamente y nos ayuda a tener el computador siempre actualizado, ósea, cada vez que encuentre un aplicación nueva y mejor para la computadora lo descarga automáticamente y lo instala en el ordenador.

Pero esa no es la única herramienta de seguridad que existe hay varias desde los antivirus hasta las páginas Web seguras, en antivirus la mayoría de veces para que se active la herramienta de seguridad tienen que tener la versión original y tener actualizado continuamente el antivirus y el caso de las páginas Web se pueden configurar como es el **"Explorer" 7** y **8** (menos la versión 6), el **"MOZILLA FIREFOX"** (todas las versiones),el **"opera"** (todas las versiones y el **"Safira"**(versiones de la iMAC) .

Causas

Las causan son porque los quipos que se actualizan continuamente se llegan a llenar los discos duros por la excesivos tamaños que puede descargar gratuitamente y que puede llegar a descargar más de 100 archivos en un solo día.

Por ese motivo la mayoría de usuarios lo que hacen es deshabilitar esta opción de herramienta de seguridad en el panel de control ósea lo que hacen es que el ordenador no se actualice continuamente o sea el computador ya no descargara los archivos y no ocupara espacio en el disco duro y la velocidad del Internet subirá de lo normal.

Consecuencias

Las consecuencias es que podríamos victimas de miles de amenazas como son los **virus** especialmente y hasta el robo de identidades.

La mayoría de computadoras con las herramientas desactivadas, son las computadoras que están llenas de virus y son fáciles de contagiar mediante el envió de archivos en la red o las memorias USB, y si son virus demasiado malicioso como los troyanos podrían malograr el sistema operativo y dañar por completo archivos y documentos y hasta el mismo computador.

Pero los virus no son los que afectan tanto sino son los robos de identidad ósea extraen información personal de la persona mediante lo famosos phishing y los Spam y nos tratan de vaciar no solo las cuentas bancarias sino que se adueñan de las cuentas de correo electrónicos y las cuentas de otros servicios.

Plan de Acción

La tendencia del mercado informático y de las comunicaciones se orienta en un claro sentido: unificación de recursos. Cada vez, ambos campos, comunicaciones e informática, se encuentran más vinculados. Este aspecto es una de las principales variables que determinan la necesidad por parte de las empresas, de contar con proveedores especializados en instalaciones complejas, capaces de determinar el tipo de topología más conveniente para cada caso, y los vínculos más eficientes en cada situación particular. Todo ello implica mucho más que el tendido de cables.

El edificio de Casino Hotel Emperador consta de 7 plantas, donde funcionan varias dependencias de carácter administrativo y de hospedaje. En la planta baja (Planta baja y Subsuelo) están localizadas las oficinas del Departamento de Contabilidad, Departamento de Recursos Humanos, la Dirección General (Gerencia), Departamento de Seguridad, Departamento de Alimentos y Bebidas,

Departamento de Sistemas, Tesorería, Mantenimiento, todos estos departamentos en el área de subsuelo; en el área de Planta baja encontramos recepción, cajas de casino, supervisores de casino, y, un cyber center.

Todas estas áreas están dentro de nuestro diseño para el cableado e implementación de conexiones, así:

Planta Subsuelo

- ✓ Departamento de Contabilidad
- ✓ Departamento de Seguridad
- ✓ Departamento de Sistemas
- ✓ Recursos humanos
- ✓ Gerencia General
- ✓ Departamento de Alimentos y Bebidas
- ✓ Departamento de Tesorería
- ✓ Departamento de Mantenimiento

Planta Primer Piso

- ✓ Departamento de Recepción
- ✓ Cajas Casino
- ✓ Supervisores Casino
- ✓ Cyber Center
- ✓ Área de sonido

Planta Primer Piso

- ✓ Mesas Casino
- ✓ Supervisor Casino
- ✓ Discoteca

Plantas Segundo a Quinto piso

- ✓ Habitaciones
- ✓ Dentro de segundo piso se encuentra Departamento de Marketing

- ✓ En tercer piso se localiza Departamento de Ama de Llaves.

Planta Sexto piso

- ✓ SPA
- ✓ Restaurante
- ✓ Departamento de Sonido

Para definir el sistema de cableado por el cual se regirá el proyecto, se considerarán las normas que establece el sistema de cableado estructurado, específicamente se adoptará la norma 568-A, la cual se fundamenta en que permite diseñar e instalar el cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán.

Como medio físico se utilizará el cable UTP nivel 5e, ya que éste permite mayor rapidez para el manejo de información y es el más utilizado y recomendado en el mercado. Este medio físico tendrá una longitud máxima de 90 mts, tal y como lo establecen las normas del C.E.

Descripción

Cableado Vertical

El cableado vertical está formado por los cables que se extienden a través del ducto del edificio, desde el cuarto de telecomunicaciones ubicado en el área de Sistemas hasta cada oficina del edificio. Este cableado consta de cables par trenzado UTP categoría 5e en topología en estrella.

Las canaletas son utilizadas para distribuir y soportar el cableado horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Cada punto terminal de conexión está conectado al Patch Panel del cuarto de equipo al que depende.

El cableado vertical del edificio cumple con la máxima distancia permitida entre el Patch Panel y el terminal de conexión que es de 90 metros; y con la longitud máxima del punto terminal hasta la estación de trabajo que es de 3 metros.

El ducto por el cual se envía el cablea es de 25 metros entre todos los pisos del edificio.

Cableado Horizontal

El cableado horizontal para el edificio, está formado por el cable UTP que sube a cada planta del edificio y se conecta con las oficinas que están ubicados en cada planta.

Cuarto de Telecomunicaciones

El área donde funcionará el cuarto de telecomunicaciones es estratégico en cuanto a la seguridad que brinda a los equipos de comunicación de la red; además, en esa dependencia labora personal capacitado para solventar algún tipo de problema que pueda presentarse con éstos.

El Departamento de Sistemas administrará y controlará toda la red del Edificio.

En ese cuarto estará presente el siguiente hardware:

- 9 switch marca D-Link, 48 puertos de salidas UTP a 10/100 Mbps.
- 5 UPS.
- 4 Servidores
- 2 racks (voz y datos)
- Central telefónica

Desde el cuarto de telecomunicaciones se le proporcionan dos cables independientes a cada cuarto de equipo de la red: uno para uso de datos y otro de voz.

Cuarto de equipos

Se necesita tener en cuenta 3 cuartos de equipos, de modo que se facilite la administración de la red. Los mismos que están en:

- Tesorería, administración de Casino
- Sistemas, administración de servidores Internet, servidor sistema hotelero
- Discoteca, control de Discoteca

Para la instalación de los Access Point se tomará en cuenta la siguiente distribución:

- En cada piso de habitaciones se instalará 2 Access Point. Pisos 2, 3, 4 y 5.
- En el área de Restaurante un Access Point.
- En salón de eventos Tres Juanes un Access Point.
- Mezanine un Access Point.
- Área de Recepción un Access Point.

Con esta distribución se abarca las áreas que más impacto tienen los usuarios para acceder a Internet.

Hay que tomar en cuenta que Hotel, Casino, Discoteca son redes independientes.

El hardware que se utilizará para la red inalámbrica es el siguiente:

- 12 Access Point – TEW 430apb
- 1 Router – TEW 632brp

En resumen, los equipos ubicados deberán dar soporte a 63 habitaciones, Salón de Eventos, Restaurante, Recepción y Mezanine, distribuidos de la manera anteriormente descrita.

Las conexiones de Internet se encuentran en el Departamento de Sistemas.
A continuación se describe la distribución de los racks y central telefónica:

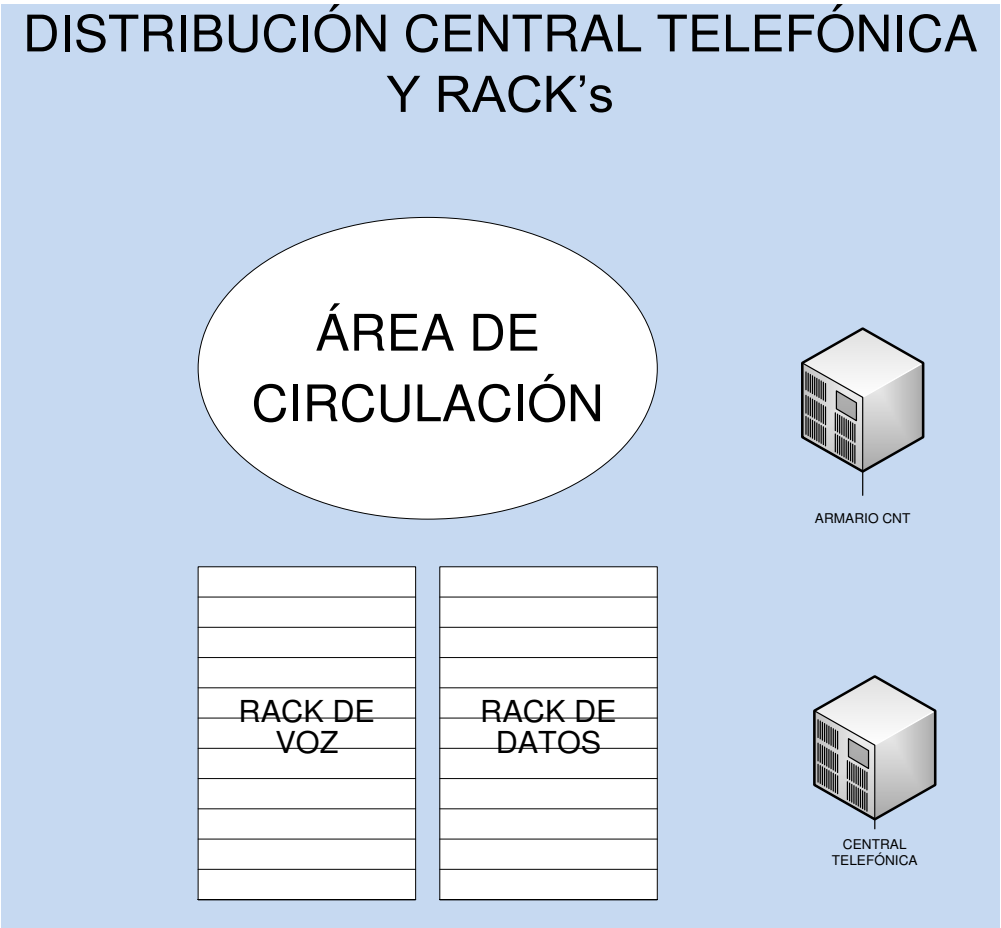


Gráfico 29. Distribución central telefónica y Rack's

Identificación y prevención de problemas de seguridad

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente como deben protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deben implementarse para evitar problemas de seguridad.

La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad.

Antes de establecer los procedimientos de seguridad, debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo.

En muchas ocasiones es tentador empezar a implementar procedimientos como el siguiente, sin haber definido la política de seguridad de la red: "Nuestro sitio necesita ofrecer a los usuarios acceso telnet a los hosts internos y externos, evitar acceso NFS a los hosts internos, pero negarlo a los usuarios externos, tener tarjetas inteligentes para registrarse desde afuera, tener módems de contestación de Llamada..."

Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas tengan más protección de la que necesitan, y que otras áreas más importantes no tengan suficiente protección.

Establecer una política de seguridad eficaz requiere considerable esfuerzo. Se necesita cierto esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario para que los usuarios de la red la entiendan adecuadamente.

Además de realizar el análisis de riesgo de los recursos de la red, usted debe identificar otros puntos vulnerables. La siguiente lista es un intento de describir algunas de las tareas más problemáticas. Esta lista lo puede orientar en la dirección correcta, pero de ningún modo esta completa, ya que es probable que su sitio tenga algunos puntos vulnerables particulares.

- ✓ Puntos de acceso
- ✓ Sistemas configurados inadecuadamente
- ✓ Problemas de software
- ✓ Amenazas internas
- ✓ Seguridad física

A continuación presentamos una explicación de estos aspectos.

Puntos de Acceso

Los puntos de acceso son los puntos de entrada (también llamados de ingreso) para los usuarios no autorizados. Tener muchos puntos de acceso incrementa los riesgos de seguridad de la red.

El gráfico muestra una red simplificada de una organización en la que existen varios puntos de ingreso a la red. Los puntos de acceso son el servidor terminal y el router del segmento A de la red. La estación de trabajo del segmento A tiene un módem privado, que se usa para conexiones telefónicas. El host B de segmento B de la red también es un punto de ingreso a este segmento. Ya que el router une los dos segmentos de la red, cualquier intruso puede usar estos puntos de acceso en cada segmento de la red para penetrar a la red completa.

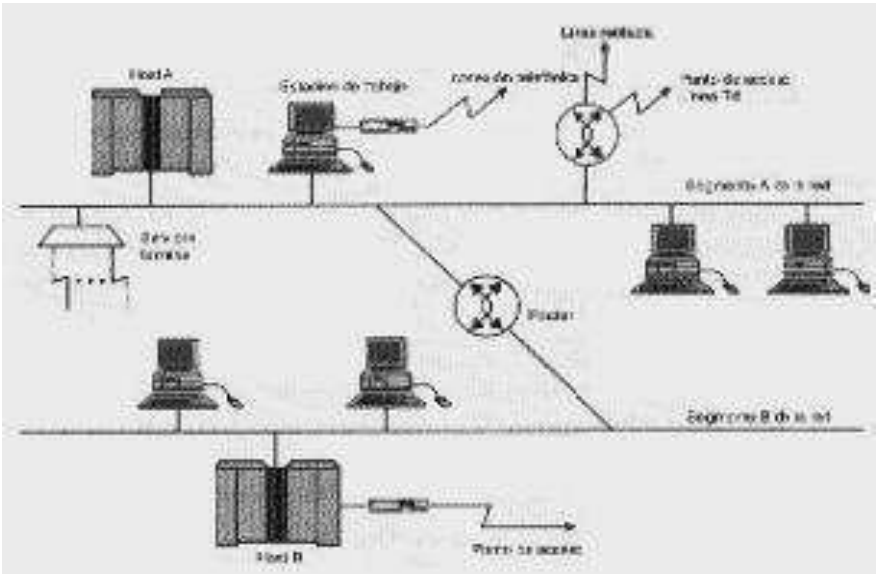


Gráfico 30. Red simplificada.

Se puede asegurar los puntos de acceso en la figura, pero es fácil que se olvide de la estación de trabajo del segmento A, que iba a ser usada para conexiones telefónicas al exterior, quizá para simples boletines electrónicos.

Considere la siguiente situación: el usuario de la estación de trabajo del segmento A puede tener una cuenta con un proveedor de acceso a Internet. Suponga que este usuario utiliza una conexión de Protocolo Internet de Línea Serial (SLIP, Serial Line Internet Protocol) o de Protocolo de Punto a Punto (PPP, Point to Point Protocol) para acceder a este proveedor de acceso a Internet.

Si el software TCP/IP que este usuario ejecuta en la estación de trabajo está configurado también como router es posible que un intruso tenga acceso a toda la red. Así mismo, si en la estación de trabajo se habilita un protocolo de enrutamiento como el protocolo de información de enrutamiento (RIP, Routing Information Protocol) o el de Abrir Primero la Ruta más Corta (OSPF, Open, Shortest Path First), la estación de trabajo puede exponer a la red interna a ataques basados en los protocolos de enrutamiento.

Observe que quizá el usuario no haya habilitado deliberadamente a la estación de trabajo como router el sistema operativo de la estación de trabajo podría estar habilitado como router en forma predeterminada. Este es el caso de muchos sistemas Unix, así como de los paquetes TCP/IP para DOS y Windows. Aún cuando la estación de trabajo haya sido configurada adecuadamente por el personal de la red, el usuario podrá conectar su computadora laptop a la red y usar un módem para tener acceso telefónico al proveedor de acceso a Internet. Si el usuario estuviera utilizando acceso telefónico (también llamado cuenta shell), donde el usuario ejecuta software de emulación de terminal en la estación de trabajo y no software TCP/IP, quizás no producirá daños. Sin embargo, si el usuario empleara una conexión SLIP o PPP, creara otro punto de acceso sin darse cuenta, el cual podrá pasar inadvertido para el personal de administración de la red.

Esto podrá representar un riesgo para la seguridad de toda la red. Puede evitarse la situación de la figura anterior si la política de seguridad de la red le informa al usuario que están prohibidas las conexiones privadas a través de las estaciones de trabajo individuales. Esta situación también subraya la importancia de tener una

política de seguridad en la que se define con claridad la política de uso aceptable para la red.

Si quiere conectarse a Internet, debe tener por lo menos un vínculo con redes fuera de la organización. Él vinculo de red hace disponibles numerosos servicios de red, tanto dentro como fuera de esta, y cada servicio es susceptible de ser comprometido.

Los servidores terminales pueden representar un riesgo si no están protegidos adecuadamente. Muchos de los servidores terminales que hay en el mercado no requieren ningún tipo de autentificación. Pregúntele a su distribuidor acerca de la capacidad de autentificación del servidor terminal. Los intrusos pueden utilizar a dichos servidores para disfrazar sus acciones, marcando al servidor terminal y teniendo acceso a la red interna. Si el servidor terminal lo permite, el intruso puede tener acceso a la red interna desde dicho servidor, y después utilizar telnet para salir de nuevo, lo que dificulta rastrearlo. Asimismo, si el intruso lo utiliza para atacar a otra red, parecer que el ataque se origen en la red de usted.

Según su configuración, las líneas telefónicas pueden dar acceso tan solo a un puerto de conexión de un solo sistema. Si está conectada a un servidor terminal, la línea de telefónica puede dar acceso a toda la red. Como se menciona al explicar la figura 3.6, una línea telefónica en una estación de trabajo que ejecute software TCP/IP puede dar acceso a toda la red.

Sistemas mal configurados

Cuando los intrusos penetran en la red, por lo general tratan de alterar el funcionamiento los hosts del sistema.

Los blancos preferidos son los hosts que actúan como servidores telnet. Si el host está mal configurado, el sistema puede ser alterado con facilidad. Los sistemas mal configurados son responsables de numerosos problemas de seguridad de red.

Antecedentes de la seguridad en redes

Los modernos sistemas operativos y su software correspondiente se han vuelto tan complicados, que entender cómo funciona el sistema no solo es un trabajo de tiempo completo, sino que requiere conocimientos especializados. Los distribuidores también pueden ser responsables de la mala configuración de los sistemas. Muchos distribuidores envían los sistemas con la seguridad totalmente abierta. Las contraseñas de cuentas importantes pueden no estar establecidas, o usar combinaciones de contraseñas y logins fácilmente descifrables. El libro The Cuckoo's Egg, de Cliff Stoll, narra la historia real de una cacería global de un espía de computadoras y menciona cómo el intruso obtuvo el acceso a los sistemas mediante una combinación de logins y contraseñas como 'Sistema/administrador "campo / servicio", etcétera.

Problemas de software

Al aumentar la complejidad del software, también aumenta el número y la complejidad de los problemas de un sistema determinado. A menos que se encuentren formas revolucionarias de crear software, éste nunca estar por completo libre de errores.

Las fallas de seguridad conocidas públicamente se vuelven métodos comunes de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida (como es la de Unix), el intruso puede usar los puntos débiles del código de software que se ejecuta en modo privilegiado para tener acceso privilegiado al sistema. Los administradores de sistemas deben estar conscientes de los puntos débiles de sus sistemas operativos y tienen la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se descubran esos problemas. También usted debe tener la política de reportar al proveedor los problemas cuando se encuentren, de modo que pueda implementarse y distribuirse la solución.

Amenazas Internas

Por lo general, los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario interno decide alterar el funcionamiento la red, puede representar una considerable amenaza a la seguridad de la red. Si usted tiene acceso físico a los componentes de un sistema, este es fácil de alterar el funcionamiento. Por ejemplo, pueden manipularse fácilmente las estaciones de trabajo para que otorguen acceso privilegiado. Puede ejecutarse fácilmente decodificación de protocolo y software de captura para analizar él trafico de protocolo. La mayoría de los servicios de aplicación estándar TCP/IP como telnet, rlogin y ftp, tienen mecanismos de autentificación muy débiles, en los que las contraseñas se envían en forma clara. Debe evitarse el acceso a estos servicios desde cuentas privilegiadas, ya que esto puede comprometer fácilmente las contraseñas de dichas cuentas.

Seguridad Física

Si la computadora misma no está físicamente segura, pueden ignorarse fácilmente los mecanismos de seguridad del software. En el caso de las estaciones de trabajo DOS (Windows ni siquiera existe un nivel de contraseña de protección. Si se deja desatendida una estación de trabajo Unix, sus discos pueden ser cambiados o si se deja en modo privilegiado, la estación estar por completo abierta. Asimismo, el intruso puede parar la máquina y regresarla a modo privilegiado, y después plantar programas tipo caballo de Troya, o tomar cualquier medida para dejar al sistema abierto para ataques futuros.

Todos los recursos importantes de la red, como las backbons, los vínculos de comunicación, los hosts, los servidores importantes y los mecanismos clave deben estar ubicados en una rea físicamente segura. Por ejemplo, el mecanismo de autentificación Kerberos requiere que su servidor está físicamente seguro. Físicamente seguro significa que la máquina está guardada en una habitación o colocada de tal modo que se restrinja el acceso fisco a ella.

En ocasiones no es fácil asegurar físicamente las máquinas. En esos casos, debe tenerse cuidado para no confiar demasiado en esas máquinas. Usted debe limitar el acceso desde máquinas no seguras hacia las más seguras. En particular, usted no debe permitir acceso a hosts que usen mecanismos de acceso confiable como las utileras Berkeley-r* (rsh, rlogin, rcp, rexec).

Aún cuando la máquina está segura físicamente, debe tener cuidado en quién tiene acceso a ella. Las tarjetas electrónicas "inteligentes" para tener acceso a la habitación en la que están aseguradas las máquinas pueden limitar el número de personas con acceso y proporcionar un registro de la identidad y hora de las personas que entraron en la habitación. Debe establecer en la política que los empleados con acceso no podrán introducir a otras personas en la sala segura cuando está abierta la puerta, aun cuando se conozca la identidad de esas personas.

Si usted permite que entre alguien junto con una persona autorizada, no podrá llevar un registro adecuado de quién y cuando entre en la habitación.

Recuerde que el personal de mantenimiento y limpieza del edificio quizá tenga acceso a la sala de seguridad. Asegúrese de tomar esto en cuenta al diseñar el sistema de seguridad.

Confidencialidad

La confidencialidad puede definirse como el hecho de mantener las cosas ocultas o secretas. Esta es una consideración muy importante para varios tipos de datos delicados.

Las siguientes son algunas de las situaciones en las que la información es vulnerable de ser divulgada:

- ✓ Cuando la información está almacenada en un sistema de cómputo.
- ✓ Cuando la información está en tránsito hacia otro sistema en la red.

- ✓ Cuando la información está almacenada en cintas de respaldo.

El acceso a la información que está almacenada en una computadora está controlado mediante los permisos de archivo, las listas de control de acceso (ACL) y otros mecanismos similares.

La información en tránsito puede protegerse mediante la encriptación o los gateways de las firewalls. La encriptación puede usarse para proteger la información en las tres situaciones.
El acceso a la información almacenada en cintas puede controlarse mediante la seguridad física; como puede ser, guardar las cintas en una caja de seguridad o en una red inaccesible.

Implementación de controles económicos viables para la política

Deben seleccionarse los controles y los mecanismos de protección de modo que estos puedan hacer frente adecuadamente a las amenazas detectadas en la evaluación de riesgos.

Estos controles deben implementarse en forma económicamente viable. Tiene poco sentido gastar grandes cantidades de dinero y sobreproteger y restringir el uso de un recurso, si especifico el riesgo de exposición.

El sentido común es, en muchas ocasiones, una herramienta muy eficaz para establecer la política de seguridad. Si bien son impresionantes los elaborados planes y mecanismos de seguridad, estos pueden ser bastante costosos. En ocasiones, el costo de esta implementación está oculto. Por ejemplo, usted podría implementar una solución de seguridad mediante software gratuito, sin tomar en cuenta el costo de administrar ese sistema y mantenerlo actualizado.

Además, si la solución de seguridad es muy elaborada, puede ser difícil de implementar y administrar. Si la administración constituye un paso único, los comandos para administrar tal sistema pueden ser fáciles de olvidar.

También debe mantener la perspectiva de que, por muy elaborada que sea la solución, una contraseña débil o robada puede comprometer a todo el sistema.
A continuación damos algunos lineamientos para implementar controles costeadles para la política.

Selección de controles relacionados con las políticas

Los controles que usted seleccione serán la primera línea de defensa en la protección de su red. Estos controles deben representar con precisión lo que usted intenta proteger, tal como está definido en la política de seguridad. Si las intrusiones externas son una gran amenaza contra su sistema, quizá no sea económicamente emplear dispositivos biométricos para autentificar a los usuarios internos. En cambio, si la amenaza mayor a sus sistemas es el uso no autorizado de los recursos de computadora por los usuarios internos, usted necesitar establecer buenos procedimientos de contabilidad automatizados. Si la amenaza principal a la red son los usuarios externos, usted tendrá que construir routers de selección y firewalls.

Uso de estrategias de reserva

Si el análisis de riesgo indica que proteger un recurso es vital para la seguridad de la red, necesitará usar diversas estrategias para hacerlo, lo cual le da a usted la seguridad de que, si una estrategia falla o es alterada, otra puede entrar en acción y seguir protegiendo el recurso de la red.

Puede resultar más económico y sencillo usar varias estrategias, de fácil implementación pero eficaz, que seguir una sola estrategia complicada y

sofisticada. Este último es el principio del todo o nada. Si el mecanismo elaborado es vencido, no hay ninguno de reserva que proteja al recurso.

Ejemplos de controles sencillos son los módems de devolución de llamada, que pueden usarse en combinación con mecanismos tradicionales de conexión. Esto puede reforzarse con tarjetas inteligentes y autentificadores manuales de un paso.

Detección y vigilancia de actividades no autorizadas

Si ocurre una intrusión o un intento de intrusión, debe detectarse tan pronto como sea posible.

Usted puede implantar varios procedimientos sencillos para detectar el uso no autorizado de un sistema de cómputo. Algunos procedimientos se basan en herramientas proporcionadas con el sistema operativo por el proveedor. También se dispone públicamente de tales herramientas en Internet.

Inspección del uso del sistema

El administrador del sistema puede realizar periódicamente la inspección. Si no, puede usarse software elaborado con este fin. La inspección de un sistema implica revisar varias de sus partes y buscar cualquier cosa que sea inusual. En esta sección se explican algunas de las formas para hacer esto.

La inspección debe hacerse con regularidad. No es suficiente hacerla cada mes o cada semana, ya que esto provocaría una brecha de seguridad que no sería detectada en mucho tiempo.

Algunas violaciones de seguridad pueden detectarse unas cuantas horas después de haberse cometido, en cuyo caso no tiene sentido la inspección semanal o mensual. El objetivo de la inspección es detectar la brecha de seguridad en forma oportuna, de modo que se pueda reaccionar adecuadamente a ella.

Si usted utiliza herramientas de inspección, debe examinar periódicamente la información de estas. Si los registros son voluminosos, tal vez necesite usar los scripts awk o perl para analizar la información. Estas herramientas también están disponibles para sistemas que no son Unix.

Mecanismos de inspección

Muchos sistemas operativos almacenan la información de conexiones en archivos de registro especiales. El administrador del sistema debe examinar regularmente estos archivos de registro para detectar el uso no autorizado del sistema. La siguiente es una lista de métodos que puede utilizar en su sitio.

Puede comparar las listas de los usuarios que estén conectados en ese momento con los registros de las conexiones anteriores. La mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días.

Una cuenta que muestre actividad fuera del horario "normal" del usuario debe inspeccionarse de cerca. Quizá un intruso este usando esa cuenta. También puede alertarse a los usuarios para que observen el último mensaje de conexión que aparece al momento de hacer su primera conexión. Si notan algún horario inusual, deben avisarle al administrador del sistema.

Muchos sistemas operativos llevan registros de contabilidad para efectos de cobranza. También pueden examinarse esos registros para detectar cualquier pauta desacostumbrada de uso del sistema. Los registros de contabilidad inusuales pueden indicar una penetración ilegal en el sistema.

El sistema operativo quizá tenga también utilerías de registro de conexión, como el syslog usado en Unix. Deben revisarse los registros producidos por dichas herramientas para detectar cualquier mensaje de error desacostumbrado producido por el software del sistema. Por ejemplo, un gran número de intentos fallidos de

conexión en un periodo corto puede indicar que alguien está tratando de adivinar contraseñas. También debe inspeccionar el número de intentos de registro de conexión en las cuentas delicadas como root, sysadm, etcétera.

Muchos sistemas operativos tienen comandos, como el ps de Unix, que enlistan los procesos que se están ejecutando en ese momento. Pueden usarse estos comandos para detectar si los usuarios están ejecutando programas a los cuales no están autorizados, así como para detectar programas no autorizados que quizá hayan sido iniciados por un intruso.

Pueden usarse los gateways de las firewalls para crear un registro del acceso a la red. Esta debe inspeccionarse con regularidad. Más adelante se explican con detalle las firewalls.

Si usted tiene recursos especiales que desee inspeccionar, puede construir sus propias herramientas con las utileras estándar del sistema operativo. Por ejemplo, puede combinar los comandos **ls** y **find** de Unix en un script de shell para revisar las configuraciones de propiedades y permisos privilegiados de archivo. Puede guardar la salida de esta actividad de inspección en listas que se pueden comparar y analizar mediante herramientas comunes de Unix como diff, awk o perl. Las diferencias en los permisos de archivos importantes pueden indicar modificaciones no autorizadas en el sistema.

Horario de inspección

Los administradores del sistema deben inspeccionar con frecuencia y regularidad a lo largo de todo el día. Puede resultar muy fastidioso inspeccionar por horarios fijos, pero pueden ejecutarse comandos de inspección a cualquier hora, en los momentos desocupados, por ejemplo, cuando usted está hablando de negocios por teléfono.

Si ejecuta los comandos de inspección con frecuencia, se familiarizará rápidamente con la información normal de estas herramientas de inspección. Esto le ayudar a detectar la información inusual. Es posible intentar automatizar este proceso ejecutando herramientas de búsqueda sobre la información, y se pueden buscar ciertos patrones fijos, pero generalmente es difícil detectar toda la información inusual causada por la intrusión en el sistema. El cerebro humano sigue siendo mejor que la mayoría de los programas para detectar sutiles diferencias en los registros de inspección.

Si ejecuta diversos comandos de inspección a diferentes horas del día, será difícil que un intruso prediga sus acciones. El intruso no puede saber cuándo el administrador correrá el comando de inspección para desplegar a los usuarios conectados, por lo que corre mayor riesgo de ser detectado. Por otra parte, si el intruso sabe que todos los días, a las seis de la tarde, el sistema se revisa para ver que todos se hayan desconectado, esperará a que concluya esta revisión antes de conectarse.

La inspección es útil, pero también puede ser alterada. Algunos intrusos pueden darse cuenta de los mecanismos estándar de registro de conexiones que se usen en el sistema y pueden tratar de desactivarlos. La inspección periódica puede detectar a los intrusos, pero no ofrece ninguna garantía de que el sistema está a salvo. No es un método infalible para detectar a los intrusos.

Herramientas para los problemas de seguridad

Las herramientas que se han escogido para evitar problemas de seguridad y establecer un mejor control son las que a continuación detallamos:

Mozilla Thunderbird

Anteriormente **Minotaur,** es un cliente de correo electrónico de la Fundación Mozilla. Su objetivo es desarrollar un Mozilla más liviano y rápido mediante la

extracción y rediseño del gestor de correo del Mozilla oficial. Es multiplataforma, utiliza el lenguaje de interfaz XUL y es software libre.

Características

- IMAP y POP.
- Correo HTML.
- Noticias.
- RSS.
- Etiquetas.
- Corrector ortográfico incorporado.
- Soporte de extensiones y skins.
- Buscadores.
- Cifrado PGP.
- Filtro bayesiano de spam.

Enigmail

Es una extensión adicional para Mozilla y Mozilla Thunderbird para las versiones que funcionan bajo los sistemas Microsoft Windows y de tipo Unix, como GNU/Linux. Enigmail no es un motor criptográfico por sí mismo, sino que utiliza el GNU Privacy Guard (GnuPG o GPG) para realizar las operaciones de cifrado criptográfico, facilitando el trabajo ya que no es necesario cifrar o firmar ficheros de texto desde la línea de comandos y luego pegarlos manualmente al mensaje de correo electrónico.

Mozilla Firefox

Es un navegador web libre y de código abierto, y que cualquier usuario puede ayudar a su desarrollo. Descendiente de Mozilla Application Suite y actualmente desarrollado por la Corporación Mozilla, la Fundación Mozilla.[] Mozilla Firefox es el segundo navegador más utilizado de Internet, con una cuota de mercado del

22,81% a finales de diciembre de 2010, según la firma Net Applications.[] Otras fuentes de medición global sitúan el uso de Firefox entre el 20% y el 31%.[]
Para visualizar páginas web, Firefox usa el motor de renderizado Gecko, que implementa estándares web actuales además de otras funciones, algunas de las cuales están destinadas a anticipar probables adiciones a los estándares web.

Incluye navegación por pestañas, corrector ortográfico, búsqueda progresiva, marcadores dinámicos, un administrador de descargas, navegación privada, navegación con georreferenciación y un sistema de búsqueda integrado que utiliza el motor de búsqueda que desee el usuario. Además se pueden añadir funciones a través de complementos desarrollados por terceros,[] entre los que hay una amplia selección, característica que ha atraído a muchos de los usuarios actuales del navegador.
[]

Firefox es un navegador multiplataforma y está disponible en varias versiones de Microsoft Windows, Mac OS X, GNU/Linux y algunos sistemas basados en Unix.[] Su código fuente es software libre, publicado bajo una triple licencia GPL/LGPL/MPL.[

TOR

Tor (The Onion Router) es una implementación libre de un sistema de encaminamiento llamado onion routing que permite a sus usuarios comunicarse en Internet de manera anónima. Originado en el US Naval Research Laboratory y hasta noviembre de 2005 patrocinado por la Electronic Frontier Foundation, Tor es desarrollado por Roger Dingledine y Nick Mathewson junto con otros desarrolladores.

Tor provee un canal de comunicación anónimo y está diseñado para ser resistente a ataques de análisis de tráfico (traffic analysis). Por lo tanto, usando Tor es posible realizar una conexión a un equipo sin que este o ningún otro tenga posibilidad de conocer el número de IP de origen de la conexión.

Tor es usualmente combinado con Privoxy para acceder a páginas web de forma anónima y segura. Privoxy es un proxy HTTP diseñado para proteger la privacidad en la navegación de internet. La interfaz de Tor es un proxy SOCKS (usualmente en el puerto 9050).

Es importante saber que Tor no es 100% fiable en lo que se refiere al cifrado de la información. Su función principal es asegurar el anonimato del usuario, de forma que no se pueda rastrear la información que envía para llegar hasta él. La red Tor cifra la información a su entrada y la descifra a la salida de dicha red, con lo cual es imposible saber quién envió la información. Sin embargo, el propietario de un servidor de salida puede ver toda la información cuando es descifrada antes de llegar a Internet, por lo que aunque no pueda conocer el emisor sí que puede acceder a la información.

Esto quedó de sobra demostrado por Dan Egerstad, un sueco experto en seguridad informática. Consciente de esa debilidad de Tor, creó un servidor de la red Tor y controló toda la información que salía por su servidor hacia su destino correspondiente en Internet, y de esta forma pudo conseguir importantes contraseñas de empresas, embajadas de todo el mundo y otras instituciones, ya que éstas usaban la red Tor sin cifrar la información primero. Efectivamente, Dan no pudo conocer la identidad del emisor, pero sí el contenido del mensaje y su destino.

Para conseguir el anonimato en internet y, además, la seguridad de que nadie accede a la información que se está enviando, es recomendable utilizar también algún sistema de cifrado como SSL. Además de esto, los desarrolladores del Tor recomiendan bloquear las cookies y los plugins Java, ya que pueden averiguar la ip del emisor. Otra buena opción es deshabilitar el registro (historial) de webs, para tener mayor seguridad en el ámbito de atacantes físicos, como por ejemplo alguna persona del mismo edificio.

CustomizeGoogle

Es una extensión para Firefox que mejora los resultados de búsqueda en Google, añadiendo información extra (como enlaces a Yahoo, Msn, etc) y eliminando información no deseada (como spam y publicidad). Todas las características son opcionales.

ClamWin

Es un antivirus libre para Microsoft Windows 98/Me/2000/XP/2003/Vista/2008. Provee una interfaz gráfica de usuario al motor ClamAV. El antivirus libre ClamWin viene con su propio instalador fácil de usar, siendo software libre y gratuito.

Características

- ✓ Alto porcentaje de detección de virus y programas espía.
- ✓ Planificador de búsqueda de virus.
- ✓ Actualizaciones automáticas de la base de datos de virus. El equipo de ClamAV actualiza su base de datos de manera regular y casi inmediata cada vez que se reportan virus nuevos.
- ✓ Buscador de virus a petición del usuario.
- ✓ Integración con los menús contextuales de Microsoft Windows Explorer.
- ✓ Soporte de integración con Microsoft Outlook.

También hay una extensión para Mozilla Firefox que utiliza **ClamWin Free Antivirus** para escanear virus en los ficheros descargados (actualmente sólo soporta Firefox 1.5). Se puede encontrar la misma extensión, funcional para la versión 2.0 en outraged-artists

ClamAV

Es un software antivirus open source (de licencia GPL) para las plataformas Windows, Linux y otros sistemas operativos semejantes a Unix

Características

- ✓ Licenciado bajo GNU General Public License 2.
- ✓ POSIX compatible y portable.
- ✓ Escaneo rápido.
- ✓ Detecta alrededor de 320 000 virus, gusanos y troyanos, incluyendo virus programados como macros de Microsoft Office.
- ✓ Escaneo de archivos y ficheros comprimidos:
  - o ZIP
  - o RAR
  - o ARJ
  - o TAR
  - o Gzip
  - o Bzip2
  - o MS OLE2
  - o MS Cabinet File
  - o MS CHM
  - o MS SZDD
  - o BinHex
  - o SIS
  - o AutoIt
- ✓ Soporta plataformas de 32/64 bit.
- ✓ Soporta la mayoría de formatos de correo electrónico.
- ✓ Soporta formatos especiales como:
  - o HTML
  - o RTF
  - o PDF
  - o CryptFF

- SCREnc
- uuencode
- TNEF

Truecrypt

Es una aplicación para cifrar y ocultar en el ordenador datos que el usuario considere reservados empleando para ello diferentes algoritmos de cifrado como AES, Serpent y Twofish o una combinación de los mismos. Permite crear un volumen virtual cifrado en un archivo de forma rápida y transparente.

Existen versiones para sistemas operativos Windows XP/2000/2003/Vista/7, Mac OS X, Linux y MorphOS (en este último bajo el nombre Kryptos). La última versión es la 7.0, publicada el 19 de julio de 2010.
TrueCrypt se distribuye gratuitamente y su código fuente está disponible, aunque bajo una licencia restrictiva.

Algoritmos de cifrado

TrueCrypt soporta AES, Serpent y Twofish algoritmos de cifrado.
Adicionalmente soporta distintas combinaciones de los algoritmos mencionados anteriormente:

- ✓ AES-Twofish
- ✓ AES-Twofish-Serpent
- ✓ Serpent-AES
- ✓ Serpent-Twofish-AES
- ✓ Twofish-Serpent.

Keepas

Un gestor de contraseñas es un programa que se utiliza para almacenar una gran cantidad de parejas usuario/contraseña. La base de datos donde se guarda esta

información está cifrada mediante una **única clave** (**contraseña maestra** o en inglés **master password**), de forma que el usuario sólo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente.

Implementación

La mayoría de los navegadores de Internet actuales, como Firefox o Internet Explorer, llevan incorporado un gestor de contraseñas en forma de plugin que opcionalmente se puede proteger mediante una contraseña maestra. De esta manera cuando visitamos una página web que requiere autenticación, el navegador escribe automáticamente el usuario y la clave en los campos correspondientes sin necesidad de que el usuario intervenga.

También existen aplicaciones independientes del navegador de Internet que tienen el mismo cometido y a menudo son más seguras, como por ejemplo LastPass (open source) o **KeePass Password Safe (open source).** Una opción especialmente conveniente es instalar el programa en una memoria USB para llevarlo con nosotros. Esto sólo es posible si el gestor de contraseñas elegido dispone de una versión portátil.

Una manera alternativa de gestionar las contraseñas, es almacenarlas en páginas web que ofrezcan este tipo de servicio. De esta manera podemos acceder a ellas desde cualquier lugar con conexión a Internet. En este caso la seguridad de nuestras claves dependerá fundamentalmente del nivel de confianza que otorguemos a quien nos ofrece el servicio.

Seguridad

La seguridad del gestor de contraseñas depende de varios parámetros:

- ✓ La robustez de la clave maestra elegida.

- ✓ La seguridad del algoritmo de cifrado utilizado.
- ✓ La calidad del código fuente de la aplicación.
- ✓ La forma de almacenar la clave cuando el usuario la solicita.
- ✓ La existencia de virus u otro tipo de malware en nuestro ordenador. La solidez de la clave maestra y del gestor de contraseñas sirven de poco si tenemos un keylogger instalado.

Se debe tener en cuenta que algunos gestores de contraseñas almacenan la contraseña en texto claro en la memoria del ordenador de manera que existe la posibilidad de que ésta sea robada por un programa parásito, como por ejemplo un troyano.

IPCop

IPCop es una distribución Linux que implementa un cortafuegos (o firewall) y proporciona una simple interfaz web de administración basándose en una computadora personal. Originalmente nació como una extensión (fork) de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo. **IPCop** tiene como objetivos ser un cortafuegos sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas (SOHO), administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. **IPCop** se actualiza desde la Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

IPCop está capado y solo tiene instaladas las herramientas justas para su función como firewall, limitando el daño que podría hacer un intruso que comprometiera el sistema. Si se desea ampliar la funcionalidad existen extensiones, comunes con SmoothWall, que permiten instalar todo tipo de utilidades como por ejemplo instalar Nmap para escanear IPs.

La distribución Linux se puede bajar desde el sitio oficial en inglés, consiste de una imagen ISO de menos de 100Mb la cual puede ser grabada en un CD e instalada en cualquier computador que tenga al menos dos interfaces de red.

Topologías de red soportadas: Permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

Las diferentes zonas las divide en colores, siendo:
Roja = zona de Internet,
Verde = Red de Área Local (LAN) cableada,
Naranja = zona desmilitarizada (DMZ, para la granja de servidores),
Azul = zona inalámbrica (Wireless).

Avast

Es un software antivirus de la firma checa AVAST Software. Cuenta con varias versiones, que cubren desde el usuario doméstico hasta el corporativo.

Avast! 5

El día 19 de enero de 2010 aparece la nueva versión de avast!, denominada avast! 5, que sustituye a la anterior en algunos productos y, además, incorpora una nueva gama al lineal (avast! 5 Internet Security). Esta fecha implica una reconversión completa de avast!, tanto a nivel de empresa, como a nivel técnico y de interfaz de usuario, en el que representa el cambio más importante de AVAST Software en toda su historia. Poco antes de la aparición de avast! 5, la compañía celebraba su usuario número 100 millones, todo un hito en una empresa de seguridad informática.

La nueva gama de productos se compone de:

- ✓ **avast! 5 Free**: sustituye al anterior avast! Home. Sigue siendo gratuito para uso doméstico sin ámbito comercial, y está enfocado al usuario que hace un uso poco intensivo de internet (navegación y correo electrónico). Avast! Free también es el producto escogido por Google para su paquete de aplicaciones gratuitas.

- ✓ **avast! 5 Pro**: sustituye al anterior avast! Profesional. Destinado a empresas para proteger sus puestos de trabajo y a usuarios avanzados que no necesitan funciones adicionales como cortafuegos o antispam. Incorpora todas las funciones de avast! Free más un escudo de scripts y el nuevo avast! Sandbox (para protección web), además de actualizaciones más frecuentes.
- ✓ **avast! 5 Internet Security**: la nueva estrella del catálogo, que aglutina todo lo que ofrece avast! Pro y le añade un cortafuegos inteligente y un módulo antispam.

Nuevas tecnologías en avast! 5 que no estaban presentes en la versión 4:

- ✓ **avast! Sandbox**: Permite que los programas potencialmente explotables (como navegadores de Internet) o los ejecutables sospechosos puedan ser ejectudos en un entorno virtual seguro. Esta característica de avast! 5 es única en el mundo de los antivirus y funciona tanto en sistemas de 32 bits como de 64 bits.

- ✓ **Emulador de código**: Cuando avast! encuentra un ejecutable sospechoso (en el escáner automático o bajo demanda) es capaz de emular el código del programa en un entorno totalmente aislado y seguro. El emulador de código se usa con dos propósitos: primero, como descompresor genérico, y segundo como apoyo al motor de heurísticas. Técnicamente, esto se produce usando un proceso denominado dynamic translation, que es mucho más rápido que las técnicas habituales de emulación.

✓ **Motor de heurística**: Desde su versión 5, avast! integra un nuevo motor de heurística diseñado para proteger proactivamente contra malware que no es detectado en base a las definiciones habituales de virus. Este motor es capaz de trabajar con archivos ejecutables y scripts.

✓ **Detección de programas potencialmente no deseados**: También desde su versión 5, avast! detecta programas potencialmente no deseados, como programas de gestión remota y keyloggers comerciales. El usuario podrá aplicar reglas para trabajar de forma voluntaria con este tipo de programas.

✓ **Despertar para escaneo**: avast! te permitirá despertar a tu Windows del modo de hibernación o suspensión para realizar un escaneo programado. Una vez finalizado, el equipo volverá a su estado de reposo.

✓ **Escáner inteligente**: Este novedoso sistema permite reducir el número de archivos a escanear en un 80% a través de una lista de programas probadamente inofensivos. Los ficheros que se marcan como no dañinos no serán escaneados hasta que los mismos no cambien.

✓ **Escudo de comportamiento**: Monitoriza la actividad del sistema usando varios sensores (sistema de ficheros, registro y red), avisando y bloqueando en caso de encontrar una actividad sospechosa. Además, estos ficheros podrán ser enviados a nuestros laboratorios para ser analizados en profundidad y así contribuir a la Inteligencia Colectiva de avast!

✓ **avast! iTrack**: Gráficos en tiempo real de los escaneos y actividad del antivirus.

✓ **Firewall silencioso**: El cortafuegos permite controlar todo el tráfico entrante y saliente de tu ordenador. La protección se basa en

sistemas heurísticos y de análisis de comportamiento, además de una lista blanca de aplicaciones benignas.

✓ **Antispam**: Nuevo y exhaustivo sistema antispam (control del correo basura) con filtro de mensajes fraudulentos. Proporciona protección contra correos electrónicos no deseados y que pueden llevar a páginas falsas de bancos u otras empresas como PayPal. Trabaja como una extensión para Outlook y como un proxy genérico para el resto de clientes de correo.

Una de las cosas que también cambia con avast! 5 es el método de licenciamiento: ahora avast! se vende en paquetes de licencias, siguiendo la tendencia generalizada en el mundo de los antivirus en la actualidad. Avast! Pro cuenta con paquetes de 1, 3, 5 y 10 licencias y avast! Internet Security con paquetes de 3, 5 y 10 licencias.

Software Libre (corre con SO Windows y GNU/Linux)	Cliente para manejar correo electrónico	**Mozilla Thunderbird** http://www.mozilla-europe.org/es/products/thunderbird/
	Software para cifrar y firmar correos electrónicos (complemento para aplicaciones de Mozilla)	**Enigmail** http://enigmail.mozdev.org/home/index.php
	Navegar en Internet	**Mozilla Firefox** http://www.mozilla-europe.org/es/
	Navegación anónima en la Internet	**TOR** http://www.torproject.org/index.html.es
	Configurar privacidad de Google con Firefox	**CustomizeGoogle** http://www.customizegoogle.com/
	Antivirus	**ClamWin** http://es.clamwin.com/ **ClamAV (para GNU/Linux)** http://www.clamav.net/
	Protección de archivos mediante unidades y documentos cifrados	**Truecrypt** [16] **:** http://www.truecrypt.org
	Sistema para manejo seguro de contraseñas	**Keepass:** http://www.keepass.info
	Programa para Firewall o Cortafuegos	**IPCop** http://www.ipcop.org/
Software Privativo	Antivirus gratuito (no es código abierto)	**Avast** http://www.avast.com/esp/

Gráfico 31. Herramientas para problemas de seguridad

Propuesta para seguridad de red inalámbrica de Emperador Hotel Casino

Dentro de la propuesta para mejorar el nivel de seguridad de la red inalámbrica y cableada de Emperador Hotel Casino se analizó algunos paquetes de software que ayudarán a mejorar la seguridad.

Nivel de seguridad en el acceso a Internet de Emperador Hotel Casino

El nivel de seguridad para acceder a Internet en Emperador Hotel Casino es **CERO** ya que no se cuenta con ninguna restricción para impedir el acceso a cualquier persona, es por esto que se propone trabajar con algunas aplicaciones que ayudarán a dar seguridad a la red inalámbrica y cableada de la empresa.

La empresa al no contar con ninguna restricción en el acceso a la red inalámbrica y cableada está propensa a recibir ataques cibernéticos a sus servidores. La empresa cuenta con dos redes físicamente independientes; la red Administrativa (cableada) la cual tiene acceso solo el personal que labora dentro de la empresa; y, la red para clientes (huéspedes) la cual es inalámbrica y cableada, la misma que es accesible a toda persona.

Las redes antes descritas al no estar protegidas, no contar con restricciones de acceso pueden ser causa de infección a los usuarios que se conecten a estas redes; motivo por el cual se llevó a cabo un monitoreo con la herramienta Wireshark para constatar posibles ataques que se esté recibiendo.

Wireshark es la herramienta que se utilizó para monitorear la red de Emperador Hotel Casino en la parte de la red inalámbrica y cableada en las áreas de Habitaciones, Restaurante, Discoteca, Casino, SPA, Recepción y salones de eventos; y de igual manera la parte Administrativa; a la vez el software NetworkMiner realiza una interfaz más amigable de los datos monitoreados por Wireshark y poder entender de mejor manera lo que se está monitoreando. Se observará que en una captura se encontró un archivo sospecho.

Wireshark

Analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

Aspectos importantes de Wireshark

- Mantenido bajo la licencia GPL.
- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Basado en la librería pcap.
- Tiene una interfaz muy flexible.
- Gran capacidad de filtrado.
- Admite el formato estándar de archivos tcpdump.

- Reconstrucción de sesiones TCP
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.

Seguridad

Para capturar paquetes directamente de la interfaz de red, generalmente se necesitan permisos de ejecución especiales. Es por esta razón que Wireshark es ejecutado con permisos de Superusuario. Tomando en cuenta la gran cantidad de analizadores de protocolo que posee, los cuales son ejecutados cuando un paquete llega a la interfaz, el riesgo de un error en el código del analizador podría poner en riesgo la seguridad del sistema (como por ejemplo permitir la ejecución de código externo).

Una alternativa es ejecutar tcpdump o dumpcap que viene en la distribución de Wireshark en modo Superusuario, para capturar los paquetes desde la interfaz de red y almacenarlos en el disco, para después analizarlos ejecutando Wireshark con menores privilegios y leyendo el archivo con los paquetes para su posterior análisis.

NetworkMiner

Es un analizador pasivo de tráfico de red, como Wireshark puede capturar tráfico, pero su enfoque y su mayor potencial no es tanto la captura sino más bien al análisis, específicamente al análisis forense del tráfico de red. Es un excelente complemento de Wireshark, está basado en Windows y es Open Source por lo que no hay nada que impida bajarla y ejecutarla.

A continuación se enumeran algunas características de este software:

- Permite la identificación de sistemas operativos y alguna información adicional sobre los hosts que detecta (OS Fingerprinting)
- Reconstrucción de archivos - Supongamos que tenemos un archivo capturado en Wireshark (con extensión pcap) al abrirlo en NetworkMiner, reconstruirá los archivos que se encuentren presentes en la captura.
- Extracción de imágenes - Como en el caso anterior, si tenemos una captura y la abrimos en NetworkMiner, reconstruirá todas las imágenes presente que hay en la captura.
- Identificación de credenciales - Identificara usuarios y passwords dentro de una captura.

Captura de archivo sospechoso

A continuación se muestra una captura en la que se detectaron algunos archivos sospechosos.

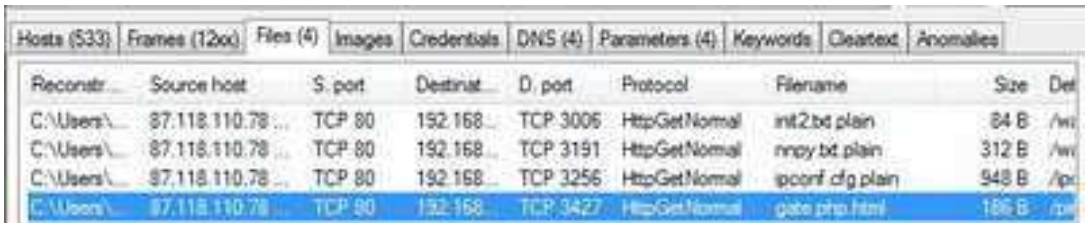


Gráfico 32. Detección archivos sospechosos.

Se puede observar detalladamente las propiedades de la captura esto es, nombre de archivo, dirección de que proviene, dirección de usuario, tamaño, puerto.

Con esto se observó en este monitoreo de la red que hay archivos sospechosos y se puede dar seguimiento y prevenir infecciones o ataques cibernéticos.

De igual manera NetworkMiner permite reconstruir las imágenes que detecta en una captura, supongamos que por ejemplo has hecho una captura en wireshark del tráfico de tu conexión a internet, en la pestaña **images** mostrara que imágenes han estado viendo los usuarios de la red, podrías descubrir contenido no permitido.

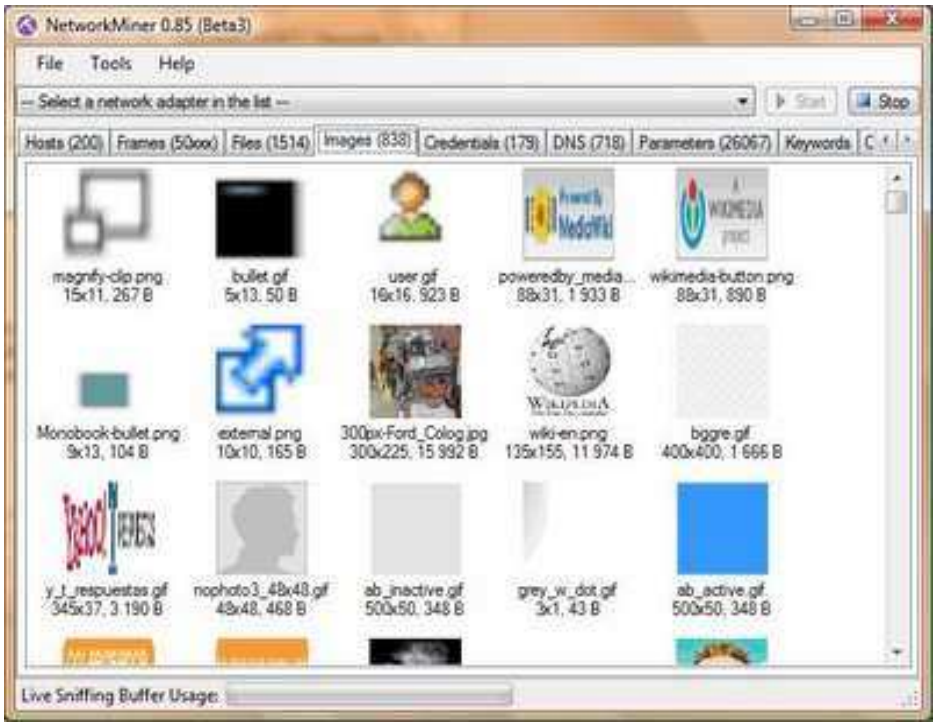


Gráfico 33. Pestaña Images NetworkMiner

NetworkMiner también es capaz de detectar credenciales que han sido utilizadas, si durante una captura, un usuario estableció una conexión a telnet a un router, en la pestaña **credentials**, se verá el usuario y password que se usó y se dará cuenta que es de suma importancia utilizar métodos más seguros para conectar equipos de red (como SSH).

Las dos herramientas se complementan perfectamente por lo que el uso de las mismas ayudará en la seguridad contra ataques cibernéticos, máquinas zombis, virus, etc., puesto que al momento de detectar cualquier inconveniente en algún computador cliente se lo podrá impedir el acceso a la red.

Se realizó el monitoreo de la red por un lapso de tiempo de 45 minutos, tiempo en el cual se logró detectar estos archivos sospechosos y también un cierto control de imágenes que se encuentran en la red.

Propuesta de solución al problema de acceso inalámbrico a servicio de Internet

Emperador Hotel Casino cuenta con una red inalámbrica ya instalada, el inconveniente que presenta es que en ciertos puntos se pierde el acceso (señal) lo que es molestoso para el cliente, es por esto que se propone ubicar 4 Access Point en lugares donde se pierde la señal de la red inalámbrica (mayormente en habitaciones internas).

En ANEXO se adjunta planos de Emperador Hotel Casino indicando puntos instalados y puntos propuestos para mejorar la señal de Internet.

En los planos mencionados se podrá observar la distribución de la parte de habitaciones, restaurante, recepción.

Los puntos que se encuentran en estudio son de las habitaciones internas habitaciones que son: 214, 215, 216, 314, 315, 316, 414, 415, 416, 513, 514, 515; habitaciones que tienen baja señal de la red inalámbrica.

Propuesta de seguridad para Emperador Hotel Casino

Para brindar seguridad informática a los usuarios de la empresa se propone la instalación de restricciones en la red inalámbrica, es decir, que el acceso sea por contraseña.

De la misma manera la instalación de un servidor Proxy para poder controlar las conexiones que realizan los clientes con el servidor destino, logrando así un control de la navegación de los mismos; logrando seguridad, rendimiento, anonimato.

Se describe a continuación las ventajas de usar un Servidor Proxy:

Proxy

Es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina **a** solicita un recurso a una **c**, lo hará mediante una petición a **b**; **C** entonces no sabrá que la petición procedió originalmente de **a**. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Servicio Proxy o Proxy Web

Su funcionamiento se basa en el del Proxy HTTP y HTTPs, pero la diferencia fundamental es que la petición se realiza mediante una Aplicación Web embebida en un Servidor HTTP al que se accede mediante una dirección DNS, esto es, una página web que permite estos servicios.

Proxy Caché

Su método de funcionamiento es similar al de un proxy HTTP o HTTPs. Su función es precargar el contenido web solicitado por el usuario para acelerar la respuesta Web en futuras peticiones de la misma información de la misma máquina u otras.

Características

La palabra **proxy** se usa en situaciones en donde tiene sentido un intermediario.

- El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
    - De ellos, el más famoso es el **servidor proxy web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web,

por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
        - También existen proxies para otros protocolos, como el **proxy de FTP**.
        - El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.
- Fuera de la informática, un proxy puede ser una persona autorizada para actuar en **representación** de otra persona; por ejemplo, alguien a quien le han delegado el derecho a voto.
- Una guerra proxy es una en la que las dos potencias usan a terceros para el enfrentamiento directo.

Como se ve, **proxy** tiene un significado muy general, aunque siempre es sinónimo de **intermediario**. También se puede traducir por **delegado** o **apoderado** (el que tiene el poder).

Ventajas

En general (no sólo en informática), los proxies hacen posibles varias cosas nuevas:

- **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para

darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- **Abuso**. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- **Carga**. Un proxy ha de hacer el trabajo de muchos usuarios.
- **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- **Incoherencia**. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.
- **Irregularidad**. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (comoTCP/IP).

Funcionamiento

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.

2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo

captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

Otros usos

Como método extra y de ayuda en las descargas mediante aplicaciones P2P; el cual es usado en Lphant y algunos Mods del Emule.

Ventajas

- **Ahorro de Tráfico**: las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
- **Velocidad en Tiempo de respuesta**: el servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
- **Demanda a Usuarios**: puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- **Filtrado de contenidos**: el servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- **Modificación de contenidos**: basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas

- Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.

Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.
- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

Analizado los beneficios de la instalación de un servidor Proxy, se realiza un comparativo entre 2 distribuciones dedicadas especialmente a la seguridad.

Estas son:

- ✓ ClearOS
- ✓ Zentyal (Ebox)

ClearOS

ClearOS está muy enfocada en su utilización como router gateway (puerta de enlace), servidor proxy, dns, firewall… muy al estilo de ipcop o cualquiera de las distribuciones que repasamos en el artículo Router, firewall, proxy… bajo una máquina potente o poco potente.

Pero al igual que eBox Plataform, está mucho más orientada a ofrecer muchos más servicios muy adecuados para PYMES (pequeñas y medianas empresas).

Entre los servicios más destacados de ClearOS (aparte de los ya nombrados) encontramos:

- Escaneo de virus y spam a través de la pasarela de paso para tráfico http así como imap, pop y smtp (parecido al plugin copfilter de ipcop).
- Filtrado de contenidos/protocolos a través de proxy de una manera realmente fácil y rápida.
- Firewall sencillo con detección de intrusiones.

- Servidor LDAP con autenticación de SAMBA como PDT (muy fácilmente configurable).
- Sistema de impresión (CUPS) y recursos compartidos (sistema de ficheros e impresoras) a través de SAMBA.
- Servidor FTP (ProFTPD), WEB (apache 2 con módulo de php) y MySQL con administración a través del proyecto phpMyAdmin.
- Servidor de correo electrónico (postfix) con soporte de captura de correo de otras cuentas (maildrop), SMTP, POP y WebMail.
- Sistema de backup de configuración del servidor (tanto local como remotamente en el servidor del proyecto).
- Informes de logs sobre cada uno de los servicios.

Zentyal

Zentyal (anteriormente conocido como **eBox Platform**) es un servidor de red unificada de código abierto (o una plataforma de red unificada) para las PYMEs. Zentyal puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad (UTM), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo (un framework) para facilitar el desarrollo de nuevos servicios basados en Unix.

- **Gestión de redes**
    - Cortafuegos y encaminamiento
        - Filtrado de tráfico
        - NAT y redirección de puertos
        - VLAN 802.1Q
        - Soporte para múltiples puertas de enlace PPPoE y DHCP
        - Reglas para múltiples puertas de enlace, balanceo de carga y auto-adaptación ante la pérdida de conectividad

        - Moldeado de tráfico (soportando filtrado a nivel de aplicación)
        - Monitorización gráfico de tráfico
        - Sistema de detección de intrusos en la red
        - Cliente dinámico DNS

- Infraestructura de red

    - Servidor DHCP
    - Servidor NTP
    - Servidor DNS
        - Actualizaciones dinámicos mediante DHCP
    - Servidor RADIUS

- Soporte de redes privadas virtuales

    - Autoconfiguración de rutas dinámicas

- Proxy HTTP

    - Caché
    - Autenticación de usuarios
    - Filtrado de contenido
    - Antivirus transparente
    - Delay pools

- Sistema de detección de intrusos

- Servidor de correo

    - Dominios virtuales
    - Quotas

        - Soporte para SIEVE
        - Recuperación de cuentas externas
        - POP3 e IMAP con SSL/TLS
        - Filtro de Spam y Antivirus
            - Listas blancas, negras y grises
        - Filtro transparente de POP3
        - Catch-all account

- **Webmail**

- **Servidor web**

    - Dominios virtuales

- **Autoridad de Certificación**

- **Trabajo en grupo**

    - Gestión centralizada de usuarios y grupos

        - Soporte maestro/esclavo
        - Sincronización con un controlador de dominio Windows Active Directory

    - Controlador Primario de Dominio (PDC) de Windows

        - Política de contraseña
        - Soporte para clientes de Windows 7

    - Compartición de recursos

        - Servidor de archivos

        - Antivirus
        - Papelera
    - Servidor de impresión

  - Groupware: Compartición de calendarios, agendas, webmail, wiki, etc.

  - Servidor VozIP

    - Buzón de voz
    - Salas de conferencias
    - Llamadas a través de un proveedor externo
    - Transferencia de llamadas
    - Aparcamiento de llamadas
    - Música de espera
    - Colas
    - Registros

- **Servidor Jabber/XMMP**
  - Salas de conferencias

- **Rincón del Usuario de Zentyal**

- **Informes y monitorización**

  - Dashboard para centralizar la información de los servicios
  - Monitorización del CPU, carga, espacio del disco, temperatura, memoria
  - Estado del RAID por software e información del uso de disco duro
  - Informes completos y resumidos de sistemas
  - Notificación de eventos vía correo, subscripción de noticias (RSS) o Jabber/XMPP

- **Actualizaciones de software**

- **Copias de seguridad (backup de configuración y remoto de datos)**

Cuadro comparativo ClearOS vs Zentyal

Servicios	ClearOS	ZENTYAL
Cortafuegos y encaminamiento	X	X
Sistema de detección de intrusos	X	X
Soporte de redes privadas virtuales	X	X
Servidor de correo	X	X
Servidor de archivos	X	X
Informes y monitorización	X	X
Servicio para e-mail	X	X
Escaneo de virus	X	X
Filtrado de contenidos sencillo, fácil y rápido	X	-

Cuadro 32. Cuadro Comparativo ClearOS vs Zentyal

Se propone ClearOS, debido a que está orientado a ofrecer servicios para PYMES (pequeñas y medianas empresas), indicando que Zentyal es mucho más completo pero el momento de utilizar los servicios algunos no serían utilizados y por ende se perdería el potencial de Zentyal.

Dentro de los servicios a utilizar para ClearOS tenemos:

- Escaneo de virus y spam a través de la pasarela de paso para tráfico http así como imap, pop y smtp.

- Filtrado de contenidos/protocolos a través de proxy de una manera realmente fácil y rápida.
- Firewall sencillo con detección de intrusiones.
- Informes de logs sobre cada uno de los servicios.
- Monitorización de tráfico

Estos servicios son los principales para poder brindar seguridad a la red inalámbrica de Emperador Hotel Casino, y así a los clientes ofrecer un mejor servicio en el acceso a Internet.

CONCLUSIONES Y RECOMENDACIONES DE LA PROPUESTA

Conclusiones

- ✓ Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas

- ✓ Con los resultados obtenidos en el Análisis de Riesgo para la empresa Emperador Hotel Casino se determinó que la seguridad informática tiene un nivel **ALTO** de probabilidad de daño, en especial por el no cumplimiento de las políticas de seguridad.

- ✓ La política de seguridad debe ser firme y su cumplimiento debe monitorearse constantemente, pero la implementación de las medidas es mucho más ágil si todos y todas comprendemos la importancia de los procedimientos. Por eso, la capacitación y los acuerdos son fundamentales.

- ✓ Es muy importante que el uso de herramientas informáticas para seguridad implique un proceso continuado en el tiempo.

Recomendaciones

- ✓ Dar cumplimiento a las tareas de monitoreo y gestión eficaz de las tecnologías de seguridad para brindar un servicio de excelencia para todos los usuarios de Emperador Hotel Casino.

- ✓ Ser firmes y dar cumplimiento a las políticas de seguridad, para así evitar daños y/o pérdidas de información delicada dentro de la empresa Emperador Hotel Casino.

- ✓ Dar uso de las herramientas informáticas para la seguridad de la información y de los usuarios que acceden a la misma, para precautelar cualquier probabilidad de daño e incluso de pérdida, robo/hurto que pueda ser afectado.

BIBLIOGRAFÍA

- ✓ Alain Puyo Alfarisk, 23 Marzo 2009, Ataques informáticos: Una realidad creciente
  http://www.alainpuyo.com/ataques-informaticos-una-realidad-creciente/

- ✓ El blog de de Inforc del Ecuador, Noviembre 4 2010, Algunos consejos de ISACA para evitar fugas de datos
  http://www.cavaju.net/

- ✓ Juan José Sánchez Aguila – Collantes, Ciberterrorismo
  http://www.inforc.ec/ciberterrorismo.htm

- ✓ ALFA - REDI, Revista de Derecho Informático.
  http://www.alfa-redi.org/rdi-articulo.shtml?x=6961

- ✓ Informationtechnology@ecuador, Septiembre 3 de 2009, Ciberdelincuencia en Ecuador, avanza sin parar
  http://www.itecuador.com/2009/09/ciberdelincuencia-en-ecuador-avanza-sin-parar/

- ✓ Mejía David, Agosto 3de 2007, Ventajas y desventajas del internet. Análisis personal.
  http://damr.net/2007/08/03/ventajas-y-desventajas-del-internet-analisis-personal

- ✓ Masadelante.com, ¿Qué es un servidor? Definición de servidor
  http://www.masadelante.com/faqs/servidor

- ✓ Wikipedia, La enciclopedia libre, Octubre 8 de 2008, Seguridad Informática.
  http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

- ✓ Wikipedia, La enciclopedia libre, Mayo 11 de 2004, WLAN
  http://es.wikipedia.org/wiki/WLAN

- ✓ Van Der Henst Christina, Junio 5 de 2006, La historia de Internet
  http://www.maestrosdelweb.com/editorial/internethis/

- ✓ Wikipedia, La enciclopedia libre, Febrero 7 de 2002, Servidor
  http://es.wikipedia.org/wiki/Servidor

- ✓ Daganzo José C., PC World Digital, Octubre 1 de 2002, Qué es realmente una WLAN
  http://www.idg.es/pcworld/Que-es-realmente-una-WLAN/art142368.htm

- ✓ Universidad Incca de Colombia
  http://www.unincca.edu.co/boletin/indice.htm

- ✓ Huidrobo José Manuel, Nuevas tecnologías. Impacto en las empresas.
  http://www.monografias.com/trabajos15/nvas-tecnologias/nvas-tecnologias.shtml

- ✓ Mujeresdeempresa.com, Octubre 6 de 2000,Como aplicar Internet en la empresa
  http://www.mujeresdeempresa.com/negocios/negocios001002.shtml

- ✓ Levene Ricardo, Delitos Informáticos
  http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3925&Itemid=426

- ✓ Huilcapi Peñafiel Arturo Oswaldo, El Delito Informático
  http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426

- ✓ Lic. Suárez Vélez Ivis, Junio 1 de 2008, Las redes informáticas http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas2.shtml

- ✓ Wikipedia, La enciclopedia libre, Febrero 21 de 2006, Seguridad en Internet http://es.wikipedia.org/wiki/Seguridad_en_Internet

- ✓ ALEGSA.com.ar, Diccionario online ,Definición de ataque informático http://www.alegsa.com.ar/Dic/ataque%20informatico.php

- ✓ José, Investigación documental http://html.rincondelvago.com/investigacion-documental_1.html

- ✓ Wolf Gunnar, Febrero 28 de 2008, Seguridad en redes: ¿Qué es? ¿Cómo lograrla? http://www.gwolf.org/files/seg_en_redes.pdf

- ✓ Clubplaneta, Factibilidad técnica, económica y financiera http://www.trabajo.com.mx/factibilidad_tecnica_economica_y_financiera.htm

- ✓ Sena Leonardo, Agosto 2004, Introducción a Riesgo Informático http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

- ✓ Salellas Luciano, Análisis de Riesgo http://www.cabinas.net/informatica/analisis_riesgos_informaticos.asp

- ✓ Salellas Luciano, Seguridad Informática – Análisis de Riesgos http://www.cabinas.net/informatica/seguridad-informatica-gestion-de-riesgos.asp

- ✓ Ferrer Rodrigo, Metodología de análisis de Riesgo
  http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

- ✓ Martínez Beatriz, Diciembre 6 de 2007, Introducción al análisis de riesgos
  http://seguinfo.wordpress.com/2007/12/06/introduccion-al-analisis-de-riesgos/

- ✓ Erb Markus, Gestión de Riesgo en la seguridad Informática
  http://protejete.wordpress.com/gdr_principal/matriz_riesgo/

- ✓ Wikipedia, La encyclopedia libre, Mayo 23 de 2006, Ley Orgánica de protección de datos de carácter personal de España
  http://es.wikipedia.org/wiki/Ley_Org%C3%A1nica_de_Protecci%C3%B3n_de_Datos

- ✓ AVAST, Free Antivirus V. 5.1.889
  www.avast.com

- ✓ Ipcop, Ipcop V.1.4.21
  www.ipcop.org

- ✓ Keepass, Keepass V. 2.14
  https://keepass.info

- ✓ Truecrypt, Truecrypt V7.0a
  www.truecrypt.org

- ✓ Clamav, Clamav V. 0.97
  www.clamav.net

- ✓ Clamwin, Free antivirus, Clamwin V. 0.97
  www.clamwin.com

- ✓ Customizegoogle, Octubre 23, 2008, Customizegoogle V 0.76
  www.customizegoogle.com

- ✓ TOR, Tor V. 0.2.1.29
  http://tor.eff.org

- ✓ Firefox, Mozilla Firefoz V 3.6
  www.firefox.com

- ✓ Enigmail, Enigmail V. 1.1.2
  http://enigmail.mozdev.org

- ✓ Thunderbird, Thunderbird V. 3.1
  http://www.mozillamessaging.com/es-ES/thunderbird/

- ✓ Carmona Miguel, 25 enero de 2010, ClearOS Introducción y primeras impresiones
  http://miguelcarmona.name/blog/clearos-introduccion-y-primeras-impresiones/

- ✓ Meredith Martin, Junio 19 de 2010, 7 of the best Linux Firewalls
  http://www.techradar.com/news/software/applications/7-of-the-best-linux-firewalls-697177

- ✓ Wikipedia, Zentyal
  http://es.wikipedia.org/wiki/EBox

- ✓ Marzo 4 de 2010, ClearOS
  http://www.playhd.com/index.php?option=com_content&view=article&id=1442:clearos-servidor-gratuito-para-hogar-y-empresas&catid=4:software&Itemid=74

ANEXOS

ANEXO 1

ENCUESTA

GRACIAS por realizar la encuesta de Emperador Hotel Casino que será de gran ayuda para mejorar los servicios que presta la empresa.
Por favor seleccione tan solo una respuesta a cada pregunta.

Usted visita Emperador Hotel Casino por:

- ✓ Placer
- ✓ Negocios
- ✓ Trabajo

¿Qué área de Emperador Hotel Casino es la que más frecuenta durante su estadía?
Restaurante

- ✓ SPA
- ✓ Salones de eventos
- ✓ Casino
- ✓ Discoteca
- ✓ Habitación

¿Qué tipo de conexión utiliza para acceder a Internet en su trabajo y/o domicilio?

- ✓ Conexión mediante cable
- ✓ Conexión Inalámbrica

Usted, ¿utiliza alguna aplicación específica al momento de acceder a Internet y conectarse con su empresa?

- ✓ Si
- ✓ No

Para tener acceso a Internet usted prefiere que sea:

- ✓ Sin restricciones
- ✓ Con contraseña

¿Con qué frecuencia usted se conecta a Internet?

- ✓ A diario
- ✓ Una vez por semana
- ✓ Una vez al mes

¿Al navegar por Internet usted está seguro que sus datos son enviados y recibidos con seguridad, sin que sean manipulados o vistos por otros?

- ✓ Si
- ✓ No

¿Ha sido víctima de ataques cibernéticos con su información?

- ✓ Si
- ✓ No

¿Su computador personal ha sido infectado por algún virus informático por razones desconocidas?

- ✓ Si
- ✓ No

Al conectarse a Internet, ¿cree Usted que otras personas pueden ingresar a su información?

- ✓ Si
- ✓ No

ANEXO 2

ANEXO 3

ANEXO 4

ANEXO 5

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]

Actos originados por la criminalidad común y motivación política

Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
Probabilidad					2	2	1	2	3	2	3	3	4	4	3	3	3
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Finanzas	x	x	x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Servicios bancarios	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
RR.HH	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Directorio de Contactos	x		x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Correo electrónico	x		x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Bases de datos internos	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Bases de datos externos	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Bases de datos colaborativos	x		x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Página Web interna (Intranet)	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Página Web externa	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Respaldos	x	x	x	1	2	2	1	2	3	2	3	3	4	4	3	3	3
Infraestructura (Planes, Documentación, etc.)	x	x	x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Informática (Planes, Documentación, etc.)	x	x	x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Base de datos de Contraseñas	x		x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Datos e información no institucionales			x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Navegación en Internet	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Chat interno	x			2	4	4	2	4	6	4	6	6	8	8	6	6	6
Chat externo	x			3	6	6	3	6	9	6	9	9	12	12	9	9	9
Llamadas telefónicas internas	x		x	1	2	2	1	2	3	2	3	3	4	4	3	3	3
Llamadas telefónicas externas	x	x	x	3	6	6	3	6	9	6	9	9	12	12	9	9	9

Sucesos de origen físico

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Probabilidad	1	3	3	3	3	2	2	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	3	9	9	9	9	6	6	6	6
Finanzas	3	9	9	9	9	6	6	6	6
Servicios bancarios	2	6	6	6	6	4	4	4	4
RR.HH	2	6	6	6	6	4	4	4	4
Directorio de Contactos	2	6	6	6	6	4	4	4	4
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	3	9	9	9	9	6	6	6	6
Correo electrónico	2	6	6	6	6	4	4	4	4
Bases de datos internos	3	9	9	9	9	6	6	6	6
Bases de datos externos	2	6	6	6	6	4	4	4	4
Bases de datos colaborativos	2	6	6	6	6	4	4	4	4
Página Web interna (Intranet)	2	6	6	6	6	4	4	4	4
Página Web externa	2	6	6	6	6	4	4	4	4
Respaldos	1	3	3	3	3	2	2	2	2
Infraestructura (Planes, Documentación, etc.)	3	9	9	9	9	6	6	6	6
Informática (Planes, Documentación, etc.)	3	9	9	9	9	6	6	6	6
Base de datos de Contraseñas	2	6	6	6	6	4	4	4	4
Datos e información no institucionales	2	6	6	6	6	4	4	4	4
Navegación en Internet	2	6	6	6	6	4	4	4	4
Chat interno	2	6	6	6	6	4	4	4	4
Chat externo	3	9	9	9	9	6	6	6	6
Llamadas telefónicas internas	1	3	3	3	3	2	2	2	2
Llamadas telefónicas externas	3	9	9	9	9	6	6	6	6

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
Probabilidad	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Finanzas	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Servicios bancarios	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
RR.HH	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Directorio de Contactos	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Correo electrónico	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Bases de datos internos	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Bases de datos externos	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Bases de datos colaborativos	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Página Web interna (Intranet)	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Página Web externa	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Respaldos	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Infraestructura (Planes, Documentación, etc.)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Informática (Planes, Documentación, etc.)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Base de datos de Contraseñas	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Datos e información no institucionales	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Navegación en Internet	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Chat interno	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Chat externo	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Llamadas telefónicas internas	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Llamadas telefónicas externas	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6

Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común y motivación política

Sistemas e Infraestructura	Clasificación: Acceso exclusivo	Clasificación: Acceso ilimitado	Clasificación: Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	2	3	2	3	3	4	4	3	3	3
Equipos de la red cableada (router, switch, etc.)	x		x	4	8	8	4	8	12	8	12	12	16	16	12	12	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x		x	4	8	8	4	8	12	8	12	12	16	16	12	12	12
Cortafuego	x		x	4	8	8	4	8	12	8	12	12	16	16	12	12	12
Servidores	x		x	4	8	8	4	8	12	8	12	12	16	16	12	12	12
Computadoras	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Portátiles	x	x	x	1	2	2	1	2	3	2	3	3	4	4	3	3	3
Programas de administración (contabilidad, manejo de personal, etc.)	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Programas de manejo de proyectos	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Programas de producción de datos	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x	x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Impresoras	x		x	1	2	2	1	2	3	2	3	3	4	4	3	3	3
Memorias portátiles	x		x	4	8	8	4	8	12	8	12	12	16	16	12	12	12
PBX (Sistema de telefonía convencional)	x		x	3	6	6	3	6	9	6	9	9	12	12	9	9	9
Celulares		x		3	6	6	3	6	9	6	9	9	12	12	9	9	9
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		x	x	2	4	4	2	4	6	4	6	6	8	8	6	6	6
Vehículos	x	x	x	1	2	2	1	2	3	2	3	3	4	4	3	3	3

Sucesos de origen físico

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
	1	3	3	3	3	2	2	2	2
Equipos de la red cableada (router, switch, etc.)	4	12	12	12	12	8	8	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	4	12	12	12	12	8	8	8	8
Cortafuego	4	12	12	12	12	8	8	8	8
Servidores	4	12	12	12	12	8	8	8	8
Computadoras	2	6	6	6	6	4	4	4	4
Portátiles	1	3	3	3	3	2	2	2	2
Programas de administración (contabilidad, manejo de personal, etc.)	3	9	9	9	9	6	6	6	6
Programas de manejo de proyectos	3	9	9	9	9	6	6	6	6
Programas de producción de datos	3	9	9	9	9	6	6	6	6
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	2	6	6	6	6	4	4	4	4
Impresoras	1	3	3	3	3	2	2	2	2
Memorias portátiles	4	12	12	12	12	8	8	8	8
PBX (Sistema de telefonía convencional)	3	9	9	9	9	6	6	6	6
Celulares	3	9	9	9	9	6	6	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	2	6	6	6	6	4	4	4	4
Vehículos	1	3	3	3	3	2	2	2	2

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información si cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegio y restricciones del personal	Falta de mantenimiento físico (proces repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acces a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación d normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Equipos de la red cableada (router, switch, etc.)	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
Equipos de la red inalámbrica (router, punto de acceso, etc.)	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
Cortafuego	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
Servidores	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
Computadoras	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Portátiles	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Programas de administración (contabilidad, manejo de personal, etc.)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Programas de manejo de proyectos	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Programas de producción de datos	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Impresoras	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Memorias portátiles	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
PBX (Sistema de telefonía convencional)	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Celulares	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Vehículos	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2

Matriz de Análisis de Riesgo

Personal	Clasificación: Imagen pública de alto perfil, indispensabl para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]
Junta Directiva	x	x		3
Dirección / Coordinación	x			3
Administración	x			4
Personal técnico		x		2
Recepción		x		3
Piloto / conductor		x		3
Informática / Soporte técnico interno		x		3
Soporte técnico externo		x		2
Servicio de limpieza de planta		x		2
Servicio de limpieza externo			x	2
Servicio de mensajería de propio		x		2
Servicio de mensajería de externo		x		2

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Actos originados por la criminalidad común y motivación política

Personal	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
Probabilidad	2	2	1	2	3	2	3	3	4	4	3	3	3
Junta Directiva	6	6	3	6	9	6	9	9	12	12	9	9	9
Dirección / Coordinación	6	6	3	6	9	6	9	9	12	12	9	9	9
Administración	8	8	4	8	12	8	12	12	16	16	12	12	12
Personal técnico	4	4	2	4	6	4	6	6	8	8	6	6	6
Recepción	6	6	3	6	9	6	9	9	12	12	9	9	9
Piloto / conductor	6	6	3	6	9	6	9	9	12	12	9	9	9
Informática / Soporte técnico interno	6	6	3	6	9	6	9	9	12	12	9	9	9
Soporte técnico externo	4	4	2	4	6	4	6	6	8	8	6	6	6
Servicio de limpieza de planta	4	4	2	4	6	4	6	6	8	8	6	6	6
Servicio de limpieza externo	4	4	2	4	6	4	6	6	8	8	6	6	6
Servicio de mensajería de propio	4	4	2	4	6	4	6	6	8	8	6	6	6
Servicio de mensajería de externo	4	4	2	4	6	4	6	6	8	8	6	6	6

Sucesos de origen físico

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Probabilidad	1	3	3	3	3	2	2	2	2
Junta Directiva	3	9	9	9	9	6	6	6	6
Dirección / Coordinación	3	9	9	9	9	6	6	6	6
Administración	4	12	12	12	12	8	8	8	8
Personal técnico	2	6	6	6	6	4	4	4	4
Recepción	3	9	9	9	9	6	6	6	6
Piloto / conductor	3	9	9	9	9	6	6	6	6
Informática / Soporte técnico interno	3	9	9	9	9	6	6	6	6
Soporte técnico externo	2	6	6	6	6	4	4	4	4
Servicio de limpieza de planta	2	6	6	6	6	4	4	4	4
Servicio de limpieza externo	2	6	6	6	6	4	4	4	4
Servicio de mensajería de propio	2	6	6	6	6	4	4	4	4
Servicio de mensajería de externo	2	6	6	6	6	4	4	4	4

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información si cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegio y restricciones del personal	Falta de mantenimiento físico (proces repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acces a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso n autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación d normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
Probabilidad	3	3	4	2	3	4	3	3	3	3	3	2	1	1	1	1	1	2	2	2	1	3	1	2	2	2
Junta Directiva	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Dirección / Coordinación	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Administración	12	12	16	8	12	16	12	12	12	12	12	8	4	4	4	4	4	8	8	8	4	12	4	8	8	8
Personal técnico	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Recepción	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Piloto / conductor	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Informática / Soporte técnico interno	9	9	12	6	9	12	9	9	9	9	9	6	3	3	3	3	3	6	6	6	3	9	3	6	6	6
Soporte técnico externo	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Servicio de limpieza de planta	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Servicio de limpieza externo	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Servicio de mensajería de propio	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4
Servicio de mensajería de externo	6	6	8	4	6	8	6	6	6	6	6	4	2	2	2	2	2	4	4	4	2	6	2	4	4	4