UNIVERSIDAD MAYOR DE SAN ANDRÉS
Facultad de Ciencias Puras y Naturales
CARRERA DE INFORMÁTICA

PROYECTO DE GRADO

Evaluación de la Seguridad en las Tecnologías de Internet

CASO: Dirección Nacional de Tecnología de la Información (DNTI)

Centro de Datos La Paz

PARA OPTAR EL TÍTULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN INGENIERÍA DE SISTEMAS INFORMÁTICOS

POSTULANTE:	Univ. Carla Machicado Lucia
TUTOR:	Mg. Sc. Fátima Consuelo Dolz de Moreno
REVISOR:	Lic. Aldo Ramiro Valdez Alvarado
ASESOR:	Ing. Esteban Enrique Lima Torricos

La Paz – Bolivia
2011

DEDICATORIA

Dedico este proyecto de grado:

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud, cuidándome y dándome fortaleza para continuar y lograr mis objetivos, además de su infinita bondad y amor.

A mi mamita adorada Lidia Lucia.

Quien a lo largo de mi vida ha velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ella que soy lo que soy ahora.

A mi papito Pedro (Blue) y abuelito Felipe (Abu).

Por todos los mágicos momentos que en mi corazón están, por sus enseñanzas y sé que desde el cielo ellos me cuidan y apoyan.

A mi novio Vaitoo.

Porque recibo fortaleza y apoyo en todo momento, tú representas gran esfuerzo y tesón en momentos de decline y cansancio.

GRACIAS !!!

Que sin ellos, no hubiese podido ser posible.

Carla Machicado Lucia

AGRADECIMIENTOS

El presente Proyecto de Grado es un esfuerzo en el cual, directa o indirectamente, participaron varias personas leyendo, opinando, corrigiendo, teniéndome paciencia, dando ánimo, acompañando en los momentos de crisis y en los momentos de felicidad.

Comenzare este apartado de agradecimientos, dándole las gracias a la docente tutor Msc. Fátima Consuelo Dolz de Moreno y al docente revisor Lic. Aldo Ramiro Valdez Alvarado, tener la paciencia, dedicación de hacer el seguimiento y revisión del presente proyecto de grado.

Agradezco al Ing. Esteban Enrique Lima Torricos por los consejos, el apoyo y el ánimo que me brindó, por haber confiado en mi persona y por la dirección de este trabajo. Al Ing. José Manual Ajhuacho Vargas, por la atenta lectura de este trabajo y observaciones y sus atinadas correcciones, y por último pero no menos importante, al Ing. Mario Rolando Ramírez Bottani por sus comentarios en todo el proceso de elaboración del Proyecto de Grado.

Gracias también a mis queridos amigos (as), que me apoyaron y me permitieron entrar en su vida durante estos años de convivir dentro y fuera de la universidad. Fanny, Cecilia, Patty, Dennis, Vladimir, Adán y Reynaldo, gracias.

Gracias a todos…

RESUMEN

Proteger la información es una de las tareas más importantes; cuando se utiliza el Internet se vuelve aún más vulnerable por lo que se necesitan mecanismos de seguridad para protegerla.

Generalmente, la Seguridad Informática consiste en asegurar que los recursos del sistema de información (Software, hardware y datos) de una organización sean utilizados de la manera como se planeó. Hoy en día, los sistemas informáticos son herramientas muy útiles. Básicamente, en ellos, se registra y procesa la información de las empresas; pero son susceptibles de amenazas; por tal razón, la Auditoria Informática se encarga de evaluar si se están cumpliendo con las medidas de control para minimizar los riesgos que conlleva la utilización de sistemas informáticos.

Este trabajo consta de seis capítulos los cuales se describen a continuación.

El capítulo I trata sobre la parte introductoria de presente proyecto de grado identificando los problemas y objetivos a tratarse en la seguridad de las tecnologías de Internet dentro del caso elegido, la Dirección Nacional de Tecnologías de Internet (DNTI).

En el capítulo II se muestra información teórica que ayudara a comprender el ámbito de la seguridad en tecnologías de Internet, como la seguridad de la información, los factores, amenazas, vulnerabilidades, ataques y contramedidas relacionadas a la misma.

En el capítulo III se muestra la evaluación a las tecnologías de Internet en la DNTI dando a lugar a un conjunto de Check List con el objetivo de mostrar datos para la evaluación.

El capítulo IV describe el análisis de dichos resultados obtenidos en el capítulo III y se brinda resultados finales de la evaluación que se hizo.

En el capítulo V se muestra una evaluación financiera donde se aplican costos de cuánto costaría una evaluación de esa magnitud como se muestra en el presente proyecto de grado costo de análisis de seguridad sobre el protocolo

Por último en el capítulo VI brindar las respectivas conclusiones y recomendaciones de acuerdo a todo el estudio elaborado en el presente proyecto de grado.

SUMMARY

Protecting information is one of the most important; when using the Internet becomes even more vulnerable to what security mechanisms are needed to protect it.

Generally, information security is to ensure that resources information system (software, hardware and data) of an organization are used in the way as planned. Today, computer systems are very useful tools. Basically, they are recorded and processed the information from companies, but are susceptible to threats, for this reason, the Computer Audit is responsible for assessing whether they are complying with control measures to minimize the risks associated with the use of computer systems.

This paper consists of six chapters which are described below.

Chapter I deal with the introductory part of this graduation project by identifying problems and objectives addressed in the security of Internet technologies in the chosen example, the National Internet Technologies (DNTI).

Chapter II shows theoretical information to help understand the field of Internet security technologies, including information security, factors, threats, vulnerabilities, attacks and countermeasures related to it.

Chapter III shows the evaluation of Internet technologies in the DNTI giving rise to a set of check list in order to display data for evaluation.

Chapter IV describes the analysis of the results obtained in Chapter III and provides final results of the evaluation was done.

Chapter V is a financial evaluation cost where they apply what it would cost an evaluation of the magnitude as shown in this draft grade security cost analysis on the protocol

Finally in Chapter VI provide the respective findings and recommendations according to the study developed in this project grade.

ÍNDICE

ÍNDICE DE FIGURAS

CAPITULO I

MARCO INTRODUCTORIO

CAPITULO II

MARCO TEORICO

CAPITULO IV

EVALUACION DE RESULTADOS

ÍNDICE DE TABLAS

CAPITULO III

MARCO APLICATIVO

CAPITULO IV

EVALUACION DE RESULTADOS

CAPITULO V

COSTO Y BENEFICIOS

CAPÍTULO I

MARCO INTRODUCTORIO

La seguridad no tiene que durar para siempre,
sólo más tiempo que cualquier otra cosa
que puede ser que note que ha desaparecido.

1.1 Introducción

La orientación inicial en el diseño de Internet como red abierta, fue creada para un entorno benigno del que ahora existe pues sus intereses se centraban en un intercambio libre de información. No obstante, tan pronto como el Internet ha dejado de ser una red experimental para convertirse en un entorno extremadamente útil, otras personas con diferentes intereses éticos y diversos comportamientos se han incorporado a la misma.

Es evidente que actualmente el entorno de Internet es poco confiable pues se pueden encontrar muchos estados de riesgo. La desconfianza está presente en la mayoría de las ocasiones, y de esta forma es difícil que la Red pueda conseguir el nivel de penetración que está llamada a tener dentro de las estructuras organizativas.

Esta situación ha derivado que en la Seguridad sea, en la actualidad, un tema a debate. Más una si tenemos en cuenta que el mayor campo de aplicación de Internet parece estar reservado a la transmisión de datos y servicios, donde los aspectos de seguridad son esenciales para su desarrollo.

Se muestra claramente que la Seguridad es un pilar básico en cualquier iniciativa tendente a solucionar el problema del desarrollo de las infraestructuras de información. Es evidente que los procedimientos y aplicaciones son las herramientas fundamentales para tal fin pues permiten, entre otras, la transmisión confidencial, la salvaguarda de la integridad de los datos y la autentificación de usuarios de una red abierta, como es el caso de Internet.

Cuando se hace referencia a la Seguridad en Internet se tiene los aspectos más típicos de la misma, como son la seguridad en el sistema Cliente, en el sistema Servidor, y en la propia transmisión.

Sobre la importancia de la Seguridad de Internet dentro de una organización, este proyecto evaluara la Seguridad de las Tecnologías de Internet, para identificar de manera adecuada, cuales son los posibles riesgos y vulnerabilidades que ocurra dentro de la Dirección Nacional de Tecnología de la Información (DNTI) Centro de Datos La Paz, que forma parte de la empresa nacional Yacimientos Petrolíferos Fiscales Bolivianos (YPFB), para poder realizar un buen tratamiento de la información protegiéndola.

1.2 Antecedentes

1.2.1 Entorno Institucional

Yacimientos Petrolíferos Fiscales Bolivianos (YPFB), es una empresa pública boliviana dedicada a la exploración, explotación, destilación y venta del petróleo y sus productos derivados.

Incrementando la producción de hidrocarburos con una explotación racional y sostenible mediante el estricto cumplimiento y control.

La Guerra del Chaco, un conflicto originado en el control del Chaco Boreal y la supuesta existencia de petróleo en esa región, fue el marco que rodeó la creación de YPFB. En efecto, el cese de hostilidades dejó al descubierto una serie de estructuras corruptas e ineficientes que demandaban un cambio urgente/ **[1]**.

Así fue como, el 21 de diciembre de 1936 el Gobierno del Coronel David Toro se promulgo el decreto de creación de YPFB.

Durante los años `40 y `50, YPFB sale adelante gracias a la construcción de refinerías, oleoductos e importante infraestructura, también se logra transformar al país en importador de petróleo a país exportador, a principios de los años `60, la empresa se ve obligada a tomar créditos internacionales para desarrollar nuevos trabajos de exploración y perforación. En los años `70, se promulga la Ley General de Hidrocarburos, en los `80 existe inestabilidad económica y YPFB sufre las consecuencias de la crisis económica y en los `90 se firma el polémico convenio perjudicial para la empresa.

Ya en el periodo de la nacionalización a partir de 2006, YPFB renace, se firman nuevos contratos con las compañías petroleras privadas estableciendo hasta el 82% de regalías en favor al Estado Boliviano, en la mejor negociación lograda jamás para el país. La soberanía y seguridad energética son derechos constituidos por y para el soberano el pueblo boliviano, y se hacen patentes en la política de Estado delegada a Yacimientos Petrolíferos Fiscales Bolivarianos YPFB Corporación, "El gas natural, debe beneficiar primero a los bolivianos", con una visión de crecimiento sostenible y planificado dentro de la organización/ **[1]**.

El control y dirección de la cadena de hidrocarburos, constituye probablemente el salto cualitativo más importante desde el punto de vista de la gestión de los hidrocarburos, en el fondo aquello implica planificar. La propiedad lo es todo en sentido material, pero una gestión no pública de dicha propiedad o laxa en el sentido de no estar a tono con los objetivos de la Nacionalización echaría por tierra el poder de ser propietarios/ **[1]**.

A continuación se muestra la misión y visión de la corporación/ **[1]**: *(Definidas por YPFB)*

> **Misión:** Operar y desarrollar la cadena de hidrocarburos, garantizando el abastecimiento del mercado interno, el cumplimiento de los contratos de exportación y la apertura de nuevos mercados, generando el mayor valor para beneficio de los bolivianos.
>
> **Visión:** Corporación estatal de hidrocarburos, pilar fundamental del desarrollo de Bolivia, reconocida como un modelo de gestión eficiente, rentable y transparente, con responsabilidad social y ambiental y presencia internacional.

La empresa cuenta con los siguientes valores corporativos/ **[1]**: *(Definidos por YPFB)*

- ***Integridad:*** Conducta ética, respeto, honestidad y transparencia.
- ***Seguridad:*** Cuidado de la salud de las personas, el medio ambiente y los activos de la Corporación.
- ***Excelencia:*** Mejora continua, orientación a resultados, innovación, pasión por el trabajo.
- ***Proactividad:*** Generación y aprovechamiento de oportunidades, liderazgo, iniciativa y creatividad.
- ***Trabajo en Equipo:*** Creación de sinergias para el logro de objetivos comunes.
- ***Compromiso:*** Con nuestra gente, la Corporación y el país. Lo hacemos por convicción y no por imposición ni obligación.
- ***Responsabilidad:*** Asumir los resultados de nuestros actos, de manera individual y colectiva.
- ***Diversidad e Inclusión:*** Trato justo e igualdad de oportunidades para todos.

Se hará referencia a la Estructura Orgánica de la empresa, en la siguiente figura:

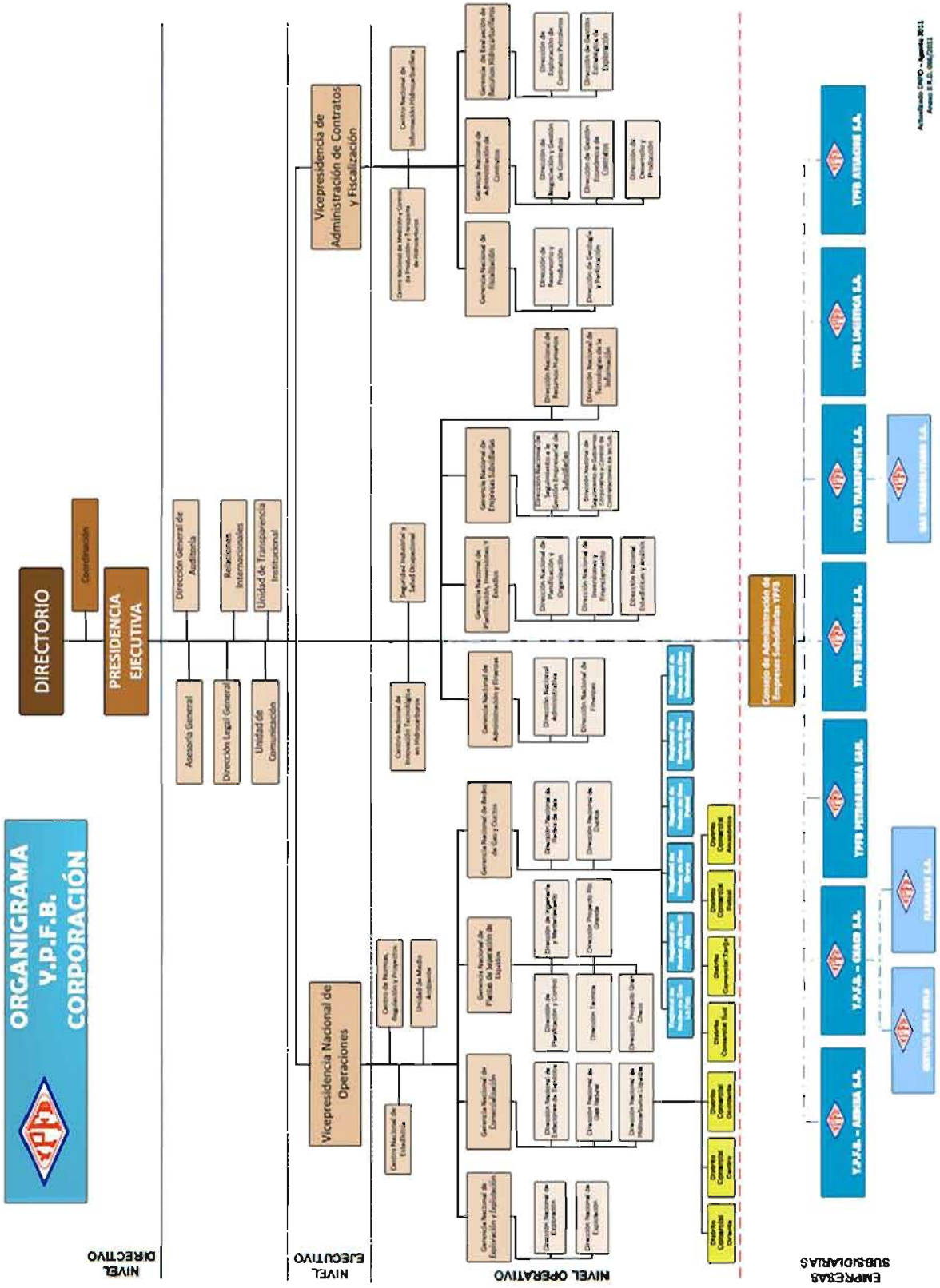


Figura 1.1. Organigrama de Yacimientos Petrolíferos Fiscales Bolivianos (YPFB)

FUENTE: [YPFB, 2011]

1.2.2 Dirección Nacional de Tecnología de la Información (DNTI)

A partir del año 2009 inicia el funcionamiento de la nueva Dirección Nacional de Tecnología de la Información (DNTI), encontrándose en el Nivel Operativo dentro del organigrama de Yacimientos Petrolíferos Fiscales Bolivianos YPFB, brindando servicios de transmisión de datos a nivel nacional, información que está distribuida en distintos puntos estratégicos, trabajando en mejorar todos los aspectos tecnológicos dentro de la corporación.

A continuación se muestra la estructura orgánica dentro de la Dirección Nacional de Tecnología de la Información (DNTI), con los principales involucrados:

Figura 1.2. Organigrama de la Dirección Nacional de Tecnologías de la Información (DNTI)
FUENTE: [Machicado, C, 2011]

1.2.3 Antecedentes de proyectos similares

a) **Guía de auditoría de seguridad de la información:** Revisar regularmente todos los procesos que en ellas se llevan a cabo, con el fin de verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad, para que las medidas adoptadas sean efectivas y mantener un compromiso con los planes de seguridad/ **[2]**.
Autor: Zenteno Flores, Lorena Michele
Año de publicación: 2006

1.3 Planteamiento y formulación del problema

1.3.1 Problema central

¿De qué manera, se puede controlar y mejorar la seguridad de tecnologías de Internet en los servicios de información, en la Dirección Nacional de Tecnología de la Información (DNTI)?

1.3.2 Problemas secundarios

Los problemas identificados son los siguientes:

- Uso inadecuado del servicio de Internet en horarios de trabajo por el personal de la empresa.
- No se tiene control sobre el consumo de ancho de banda, de los usuarios finales.
- Inexistencia de procedimiento de verificación de vulnerabilidades en el centro de datos.
- La seguridad de los servicios no se ajusta a ninguna norma de seguridad.
- Ausencia de procedimiento de testeo de seguridad de aplicaciones de Internet.
- Carencia de herramientas de búsqueda de vulnerabilidades.

1.4 Objetivos

1.4.1 Objetivo general

Evaluar la seguridad en las tecnologías de Internet, para poder identificar de manera oportuna los riesgos y amenazas externas e internas en el tráfico de red, para mejorar la protección de los servicios de información en la empresa.

1.4.2 Objetivos específicos

- Evaluar metodologías de seguridad de tecnologías de Internet y elegir la que mejor se adecue a la DNTI, bajo el contexto actual de trabajo.
- Determinar si la información de la empresa en términos de disponibilidad, integridad y confidencialidad está expuesta y tiene algún tipo de riesgo.
- Ajustar la seguridad de los servicios de Internet de la DNTI a la norma recomendado en la metodología.
- Evaluar el cumplimiento de políticas de seguridad que protejan la información de la empresa.

1.5 Justificación

A continuación se tomara los siguientes aspectos:

1.5.1 Justificación económica

La evaluación de riesgos y amenazas de la seguridad de información en las tecnologías de Internet reduce costos o pérdidas económicas a la empresa; como la caída de servicios provocando la disminución de producción, llevando a la pérdida de información causada por salidas no permitidas de la misma. Por tanto este proyecto contribuye a realizar un estudio de evaluación ayudando a mejorar los aspectos de seguridad que debe existir en la DNTI.

1.5.2 Justificación social

La información que se tiene en la empresa está de alguna manera insegura, por consiguiente con el proyecto se pretende brindar una evaluación de seguridad para mejorar la protección a la información que cada usuario final de empresa tiene a su cargo y esta sea confiable al mismo tiempo.

1.5.3 Justificación técnica

En el presente proyecto se mostrara cuan necesario es el uso de herramientas técnicas para realizar la evaluación de seguridad de la información de forma externa (Internet), de esa forma se defenderá y controlara el flujo de información dentro la empresa, teniendo un mejor control la Dirección Nacional de Tecnología de la Información.

1.6 Límites

Los límites del presente proyecto están dados en relación a las características de funcionamiento de la DNTI.

- El proyecto solo realizara la evaluación en el entorno de tecnologías de Internet, todos los servicios y aplicaciones que se pueden usar en la misma.
- No se considerara la evaluación de seguridad de los procesos de trabajo, esto hace referencia al testeo de solicitud, testeo de sugerencia dirigida y testeo de las personas confiables.

- No se considerara la seguridad de las comunicaciones de voz, como ser testeo de PBX, testeo de correo de voz, revisión del FAX y testeo del modem.
- El proyecto no realizara la revisión en la seguridad inalámbrica, no se tomaran en cuenta los siguientes puntos: la verificación de radiación electromagnética (EMR), verificación de dispositivos de transacción inalámbricos, verificación de dispositivos de vigilancia inalámbricos.
- No se realizara la implementación del presente proyecto. Solo se realizara la evaluación de seguridad en los campos ya definidos.

1.7 Alcances

Los alcances que se desea con el proyecto son los siguientes:

- El proyecto contempla con posterioridad realizar la implementación de la metodología de seguridad que se propone, con la evaluación que se realizara dentro la empresa.
- Se busca que la evaluación sea realizada de manera detalla buscando las falencias mínimas en el servicio de Internet.
- Dar lineamientos de normas y políticas de seguridad en base a estándares internacionales establecidos para obtener certificaciones, como empresa líder en tecnología de Internet segura.
- Recomendar planes de contingencia en caso de daños de gran magnitud respecto a la información que se tiene en el centro de datos, que puedan ocasionar grandes pérdidas.

1.8 Aportes

El aporte que se brinda con el presente proyecto es de proponer y adecuar una Metodología de Seguridad en Internet que cumpla y cubra todas las necesidades tecnológicas en empresas petroleras como es el caso de YPFB realizando dicha evaluación, dentro del territorio Boliviano, el diagnostico, evaluación y solución que se dará con la metodología, permitirá mejorar la seguridad en Internet, de esta manera realizando pruebas de verificación de datos entrantes y salientes, tal control está a cargo de la DNTI que cumple con la administración Tecnológica a nivel nacional de la empresa Yacimientos Petrolíferos Fiscales Bolivianos YPFB.

1.9 Diseño metodológico

1.9.1 Método científico

El método científico es el procedimiento planteado que se sigue en la investigación para descubrir las formas de existencia de los procesos objetivos, para desentrañara sus conexiones internas y externas, para generalizar y profundizar los conocimientos así adquiridos, para llegar a demostrarlos con rigor racional y para comprobarlos en el experimento y con las técnicas de su aplicación/ **[3]**.

Es el modo ordenado de proceder para el conocimiento de la verdad, en el ámbito de determinada disciplina científica. Tiene como fin determinar las reglas de la investigación y de la prueba de las verdades científica. Toda ciencia tiene su método específico pero podemos encontrar ciertas características generales:

- ***Es fáctico***: Porque su fuente de información son el hecho, los cuales pueden constituirse tanto en su pregunta como en su respuesta.
- ***Trasciende los hechos***: Porque tiene la capacidad para ir más allá de los hechos. Traspasar los límites de la experiencia objetiva y trascender al campo conceptual, general y universal.
- ***Se atiende a reglas metodológicas:*** Formular preguntas, proponer problemas y plantear hipótesis. Ejecutar observaciones, medidas y evaluaciones. Elaborar explicaciones y revisar conclusiones, ideas u opiniones que estén en desacuerdo con las observaciones o con las respuestas resultantes.
- ***Verificación empírica:*** Porque utiliza un conjunto de pruebas empíricas que demuestran y confirman una hipótesis.
- ***Es autocorrectivo:*** Como resultado de sus propias conclusiones está en condición de ir corrigiendo y sustentando sus procedimientos a los niveles de las exigencias que demanda el proceso de investigación.
- ***Es progresivo***: Por su apertura a nuevos aportes, procedimientos y técnicas, con el propósito de adaptarse a las exigencias superiores y siempre en desarrollo de la realidad que investiga y estudia.
- ***Es general***: El método científico no está en condiciones de realizar formulaciones que no sean más que generales, ya que los hechos particulares y singulares tienen

sentido y significado, no como elementos aislados, sino en el contexto y en el marco de la generalidad.

- ***Es objetivo:*** Porque rechaza como hecho científico todo aquello que no es examinado y basado en la prueba y razón humana/ **[3]**.

1.9.2 Metodología sistemática

Es uno de los instrumentos lógicos más contemporáneos en el ámbito de la metodología, orientado a la percepción holística (total) de la realidad de donde se extraerá la propia problemática y las soluciones correspondientes.

Como nuevo enfoque, forma los tres conjuntos que interactúan formando un sistema que integra los conceptos básicos fundamentales para el desarrollo del estudio y aplicación de sistemas. Se analizan sus características, sus tendencias de divergencia o convergencia y de síntesis que se presentan/ **[4]**.

1.10 Herramientas y técnicas a utilizar en la evaluación

1.10.1 Check List

Además del examinar los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados Check List, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad.

Las Check List tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados por la empresa auditora. La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método.

El profesionalismo para utilizar los Check List, pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. Salvo excepciones, las Check Lists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma/ **[5]**.

El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que este le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

- **Rango:** Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido.
- **Binaria:** Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

1.10.2 Trazas o Huellas

Por lo general, los auditores se apoyan en software que les permiten rastrear los caminos que siguen los datos a través del programa. Las Trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. No deben modificar en absoluto el Sistema.

Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo/ **[5]**.

1.10.3 Software de auditoría

Los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo/ **[5]**.

CAPÍTULO III

MARCO APLICATIVO

Tres reglas de instrumentos de seguridad:

1. herramientas no sabemos cuándo mienten,

2. las herramientas son tan inteligentes como sus diseñadores, y

3. Herramientas sólo pueden trabajar correctamente dentro de los límites del entorno para el que ellos fueron hechos.

2.1 Internet

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.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea/ **[6]**.

2.2 Tecnología de Internet

2.2.1 Acceso a Internet

Internet incluye aproximadamente 5.000 redes en todo el mundo y más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red. Los servicios disponibles en la red mundial de PC, han avanzado mucho gracias a las nuevas tecnologías de transmisión de alta velocidad, como ADSL y Wireless, se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite (ver tu casa desde el cielo), observar el mundo por webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego multijugador en 3D, un buen libro PDF, o álbumes y películas para descargar.

El método de acceso a Internet vigente hace algunos años, la telefonía básica, ha venido siendo sustituido gradualmente por conexiones más veloces y estables, entre ellas el

ADSL, Cable Módems, o el RDSI. También han aparecido formas de acceso a través de la red eléctrica, e incluso por satélite (generalmente, sólo para descarga, aunque existe la posibilidad de doble vía, utilizando el protocolo DVB-RS).

Internet también está disponible en muchos lugares públicos tales como bibliotecas, bares, restaurantes, hoteles o cibercafés y hasta en centros comerciales. Una nueva forma de acceder sin necesidad de un puesto fijo son las redes inalámbricas, hoy presente en aeropuertos, subterráneo, universidades o poblaciones enteras/ **[7]**.

2.2.2 Nombres de dominio

La Corporación de Internet para los Nombres y los Números Asignados (ICANN) es la autoridad que coordina la asignación de identificadores únicos en Internet, incluyendo nombres de dominio, direcciones de Protocolos de Internet, números del puerto del protocolo y de parámetros. Un nombre global unificado (es decir, un sistema de nombres exclusivos para sostener cada dominio) es esencial para que Internet funcione.

El ICANN tiene su sede en California, supervisado por una Junta Directiva Internacional con comunidades técnicas, comerciales, académicas y ONG. El gobierno de los Estados Unidos continúa teniendo un papel privilegiado en cambios aprobados en el Domain Name System. Como Internet es una red distribuida que abarca muchas redes voluntariamente interconectadas, Internet, como tal, no tiene ningún cuerpo que lo gobierne/ **[7]**.

2.3 Seguridad en Internet

El concepto de Seguridad en Internet va tomando matices más complejos y especializados. Actualmente, incluye servicios y estrategias para resguardar el intercambio de información y quienes la emiten o reciben. Paralelamente, se incrementa la necesidad de que la Seguridad en Internet sea reforzada. Y cada vez existen instrumentos más precisos que proporcionan seguridad en toda la red protegiendo los servidores con acceso a Internet y a redes privadas.

Asimismo, la Seguridad en Internet se ha convertido en un asunto vital para las Organizaciones que transmiten información confidencial por las redes. De ella depende la confianza de los visitantes a su sitio web porque los consumidores se resisten a facilitar

datos personales, números de tarjetas de crédito, contraseñas o cualquier información confidencial por temor a que sea interceptada y manipulada con malas intenciones y los exponga a riesgos como fraude o robo de identidad/ **[8]**.

Un sistema debe tener protegida su información, se tienen los siguientes atributos para la seguridad:

- ***Confidencialidad:*** Se refiere a tener la información restringida a aquellos sujetos que no tienen autorización, solamente usuarios definidos por la dirección de la empresa tendrán acceso a la información.
- ***Integridad:*** Para la empresa es muy importante que su información se mantenga sin modificación y que los sujetos que estén autorizados para hacerlo trabajen bajo estrictas normas de operación.
- ***Disponibilidad:*** Es muy importante que la información de los sistemas esté disponible en cualquier momento que lo necesiten los usuarios designados o procesos autorizados.

Figura 2.1. Requisitos para mantener de privacidad en sistemas de información
FUENTE: [Machicado C, 2011]

- ***Autenticidad:*** Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envié una información haciéndose pasar por otro. Confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control de acceso a determinados servicios y datos, la autentificación de los sitios web, etc.

2.4 Auditoría informática para Internet

En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos, los cuales no pueden pasar por alto el auditor informático:

- Evaluación de los riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.
- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

2.5 Política de seguridad

A la descripción, bajo la forma de reglas, en la que se incluyan las propiedades de integridad, confidencialidad y disponibilidad, en la medida requerida por una organización, se le conoce como Políticas de seguridad.

El objetivo de las políticas de seguridad es definir qué están haciendo los usuarios con la información de la empresa, se deberá hacer un buen uso de los recursos de hardware y software y por supuesto eficientizar los costos.

Cada uno de los procesos administrativos o técnicos que se manejen en los sistemas de información deberán contar con su propia política de seguridad, los atributos descritos con anterioridad deberán ser aplicados al definir estas políticas.

La política de seguridad nos indica:

- Qué hay que proteger
- Qué principios hemos de tener en cuenta
- Cuáles son los objetivos de seguridad a conseguir
- La asignación de cometidos y responsabilidades

La política de seguridad se expresa mediante principios y objetivos. Un principio es una norma o idea fundamental que rige la política de seguridad, y que se acepta en esencia. Un objetivo de seguridad es la declaración expresa de la intención de conseguir algo que

contribuye a la seguridad de la información, bien porque se opone a una de las amenazas identificadas o bien porque satisface una exigencia de la política de seguridad de la información/ **[9]**.

2.6 Normas de seguridad

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por estas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

Proporcionar las directrices necesarias para la correcta administración del SSI, bajo un entorno normativamente regulado e interpretable por los usuarios de la misma red institucional y ajustada a las necesidades de la empresa, esto hace referencia a:

"Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc."

Por lo anterior, además de detallar un conjunto de reglas o ajustes a las actividades relacionadas con el que hacer de los usuarios de las tecnologías de información, buscando la integridad, confidencialidad y disponibilidad de la información y recursos informáticos, se hace referencia a otros documentos como manuales o procedimientos, que sirven de guía en el cumplimiento de lo estipulado/ **[10]**.

2.7 Riesgos de la información en Internet

Los expertos en seguridad de Tecnologías de la Información (TI) clasifican los riesgos de seguridad de la información en tres amplias categorías:

- ***Riesgos de confidencialidad:*** Estos riesgos representan las amenazas a la propiedad intelectual de una organización por parte de usuarios no autorizados y código malintencionado que intentan tener acceso a lo que se ha dicho, escrito y creado en una organización.
- ***Riesgos de integridad:*** Estos riesgos representan las amenazas a los recursos del negocio por parte de usuarios no autorizados y código malintencionado que intentan dañar los datos profesionales de los que depende la organización. Los riesgos de

integridad ponen en peligro los activos de negocio que contienen información crítica para una organización, como servidores de bases de datos, archivos de datos y servidores de correo electrónico.

- ***Riesgos de disponibilidad:*** Estos riesgos representan las amenazas a los procesos de negocio por parte de usuarios no autorizados y código malintencionado que intentan perjudicar el modo en que funciona el negocio y el modo en que los trabajadores de la información realizan su trabajo. Los riesgos de disponibilidad pueden afectar a todos los procesos de inteligencia empresarial, a las capacidades y las características de las aplicaciones y a los procesos de flujo de trabajo.

Para ayudar a garantizar la protección de la organización frente a estas tres categorías de riesgo, se recomienda una estrategia de seguridad de defensa en profundidad; es decir, una estrategia de seguridad que incluya varios niveles superpuestos de defensa contra usuarios no autorizados y código malintencionado. Estos niveles suelen ser los siguientes:

- Protección de la red perimetral, como los firewall y los servidores proxy.
- Medidas de seguridad física, como centros de datos físicamente seguros y salas de servidores.
- Herramientas de seguridad de escritorio, como firewall personales, programas antivirus y detección de spyware.

Figura 2.2. Situaciones de riesgo

FUENTE: [Machicado C, 2011]

2.7.1 Tipos de riesgos en Internet

Riesgos relacionados con la Información:

- ***Acceso a información poco fiable y falsa.*** Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red.
- ***Dispersión, pérdida de tiempo.*** A veces se pierde mucho tiempo para localizar la información que se necesita.
- ***Acceso de los niños a información inapropiada y nociva.*** Existen webs que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas para niños y menores por el modo en el que se abordan los temas o la crudeza de las imágenes (sexo, violencia, drogas, determinados relatos históricos y obras literarias...).
- ***Acceso a información peligrosa, inmoral, ilícita***. Existe información con contenidos considerados delictivos que incitan (la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo de drogas, participar en ritos satánicos y en sectas ilegales, realizar actos delictivos). La globalidad de Internet y las diferentes culturas y legislaciones de los países hacen posible la existencia de la policía dedicada a delitos informáticos.

Riesgos relacionados con la comunicación interpersonal:

- ***Recepción de "mensajes basura".*** Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) que envían indiscriminadamente empresas de todo el mundo. En ocasiones su contenido es de naturaleza sexual o proponen oscuros negocios. Otras veces pueden contener archivos con virus.
- ***Recepción de mensajes personales ofensivos.*** Al comunicarse en los foros virtuales, como los mensajes escritos (a menudo mal redactados y siempre privados del contacto visual y la interacción inmediata con el emisor) se prestan más a malentendidos que pueden resultar ofensivos para algunos de sus receptores, a veces se generan fuertes discusiones que incluyen insultos e incluso amenazas.
- ***Pérdida de intimidad.*** En ocasiones, hasta de manera inconsciente al participar en los foros, se puede proporcionar información personal, familiar o de terceras

personas a gente desconocida. Y esto siempre supone un peligro. También es frecuente hacerlo a través de los formularios de algunas páginas web que proporcionan determinados servicios gratuitos (buzones de e-mail, alojamiento de páginas web, música y otros recursos digitales...)

- ***Acciones ilegales.*** Proporcionar datos de terceras personas, difundir determinadas opiniones o contenidos, plagiar información, insultar, difamar o amenazar a través de los canales comunicativos de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").
- ***Malas compañías.*** Especialmente en los chats, redes sociales, blogs, etc., se puede entrar en contacto con personas que utilizan identidades falsas con oscuras intenciones, en ocasiones psicópatas que buscan víctimas para actos violentos o delictivos a las que prometen estímulos, experiencias y amistad.

Riesgos relacionados con las adicciones:

- ***Adicción a buscar información de todo tipo:*** noticias, webs temáticas, webs personales, servicios ofrecidos por empresas... Muchas veces incluye pornografía, imágenes o escenas que incluyen violencia... Se buscan sensaciones más que información.
- ***Adicción a frecuentar los entornos sociales:*** Los usuarios no dependientes tienen más tendencia a comunicarse con las personas conocidas. Los adictos buscan más conocer gente nueva y buscar el apoyo en los grupos de la red; a veces se crean varias personalidades virtuales.
- ***Juego compulsivo:*** Internet está lleno de webs con todo tipo de juegos, algunos de ellos tipo casino con apuestas en dinero; otros muy competitivos o violentos..., que pueden fomentar ludopatías en determinadas personas.
- ***Compras compulsivas:*** comercio electrónico, subastas, banca electrónica...

2.8 Vulnerabilidades de la información en Internet

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits).

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, hotfixs o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

Las vulnerabilidades se descubren muy seguidas en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.

- Algunas vulnerabilidades típicas suelen ser:
- Desbordes de pila y otros buffers.
- Symlink races.
- Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.
- Secuesto de sesiones.
- Ejecución de código remoto.
- XSS.

2.8.1 Tipos de vulnerabilidades en Internet

Vulnerabilidades que afectan a todos los sistemas:

- ***Instalaciones por defecto de sistemas y aplicaciones:*** La mayoría del software, incluyendo sistemas operativos y aplicaciones, viene con scripts de instalación o programas de instalación. La meta de estos programas de instalación es dejar los sistemas operativos lo más rápido posible, con la mayor parte de funciones disponibles o habilitadas, y con la ayuda de muy poco trabajo por parte del administrador. Para lograr esta meta, los scripts típicamente instalan más componentes de los que se necesitan en realidad. La filosofía de los fabricantes es que resulta mejor habilitar funciones que no son utilizadas que hacer que el usuario

instale funciones adicionales a medida que las vaya requiriendo. Esta aproximación, aunque conveniente para el usuario, genera la mayoría de las vulnerabilidades de seguridad debido a que los usuarios no mantienen activamente o aplican los parches a los componentes de software que utilizan. Más aún, muchos usuarios no son conscientes de lo que está realmente instalado en sus propios sistemas, dejando peligrosos programas de demostración en ellos por el simple hecho de que no saben que están ahí.

- ***Cuentas sin contraseña o contraseñas débiles:*** La mayoría de los sistemas se encuentran configurados para usar contraseñas secretas como primera y única línea de defensa. Los nombres de usuario (user IDs) son relativamente fáciles de conseguir y la mayoría de las compañías tienen accesos telefónicos que se saltan los cortafuegos. Es por esto que si un atacante puede determinar el nombre de una cuenta y su contraseña correspondiente, él o ella pueden entrar en la red. Dos grandes problemas lo constituyen las contraseñas fáciles de adivinar y las contraseñas por defecto, pero aun así, uno mucho mayor son las cuentas sin contraseña. En la práctica, todas las cuentas con contraseñas débiles, contraseñas por defecto o contraseñas en blanco deben de ser eliminadas de su sistema.
  Adicionalmente, muchos sistemas contienen cuentas que vienen incluidas o cuentas por defecto. Estas cuentas generalmente tienen la misma contraseña para todas las instalaciones del software. Los atacantes habitualmente buscan estas cuentas ya que son bien conocidas por su comunidad. Por esta razón, cualquier cuenta preexistente o por defecto, debe ser identificada y eliminada del sistema.
- ***Gran número de puertos abiertos:*** Tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente. El resto de los puertos deben ser cerrados.
- ***Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas:*** La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Por ejemplo, el popular ataque "smurf" hace uso de una característica de los enrutadores (routers) para enviar una secuencia de paquetes a miles de máquinas. Cada paquete contiene una dirección IP de origen que es suplantada de una víctima. Las máquinas a las que estos paquetes falsificados son enviados inundan a la máquina víctima generalmente

deteniendo sus servicios o bien deteniendo los servicios de una red completa. Utilizar un mecanismo de filtrado sobre el tráfico que entra en la red (ingress filtering) y el que sale (egress filtering) le ayudará a lograr un alto nivel de protección.

- ***Registro de eventos (logging) incompleto o inexistente:*** Una de los máximos objetivos de la seguridad es, "*la prevención es ideal, pero la detección es fundamental*". Mientras usted permita fluir el tráfico entre su red y la Internet, la probabilidad de que un atacante llegue silenciosamente y la penetre está siempre latente. Cada semana se descubren nuevas vulnerabilidades y existen muy pocas formas de defenderse de los ataques que hagan uso de las mismas. Una vez que usted ha sido atacado, sin registros (logs) hay muy pocas probabilidades de que descubra qué hicieron realmente los atacantes. Sin esa información su organización debe elegir entre recargar completamente el sistema operativo desde el soporte original y luego esperar que los respaldos se encuentren en buenas condiciones, o bien correr y asumir el riesgo que representa seguir utilizando un sistema que un atacante controla.
- ***Programas CGI vulnerables:*** La mayoría de los servidores Web, permiten el uso de programas CGI (Common Gateway Interface) para proporcionar interactividad a las páginas web, habilitando funciones tales como recolección de información y verificación. De hecho, la mayoría de los servidores web vienen con programas CGI de ejemplo preinstalados. Desgraciadamente demasiados programadores de CGIs pasan por alto el hecho de que sus programas proporcionan un vínculo directo entre cualquier usuario en cualquier parte de Internet y el sistema operativo en la máquina que se encuentra ejecutando el servidor Web. Los programas CGI vulnerables resultan especialmente atractivos para los intrusos ya que son relativamente fáciles de localizar y de operar con los mismos privilegios y poder que tiene el software del servidor Web. Es de sobra conocido el hecho de que los intrusos abusan de los programas CGI para modificar páginas Web, robar información de tarjetas de crédito e instalar puertas traseras que les servirán para posteriormente tener acceso a los sistemas comprometidos. Cuando el sitio web del Departamento de Justicia de los Estados Unidos fue vulnerado, una auditoría exhaustiva concluyó que un fallo en un programa CGI fue la ruta más probable para perpetrar el ataque. Las aplicaciones en los servidores web son igualmente vulnerables a amenazas creadas por programadores descuidados o no muy bien instruidos. Como regla general, los programas de ejemplo deben ser siempre eliminados de los sistemas de producción.

Figura 2.3. Situaciones de vulnerabilidades
FUENTE: [Machicado C, 2011]

2.9 Ataques a la información en Internet

Un "*ataque*" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques siempre se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos. Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas.

Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema;
- Robar información, como secretos industriales o propiedad intelectual;
- Recopilar información personal acerca de un usuario;
- Obtener información de cuentas bancarias;
- Obtener información acerca de una organización (la compañía del usuario, etc.);
- Afectar el funcionamiento normal de un servicio;
- Utilizar el sistema de un usuario como un "rebote" para un ataque;

- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

2.9.1 Tipos de ataques en Internet

Los ataques se pueden clasificar de la siguiente manera:

- ***Acceso físico:*** En este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:
  - ✓ Interrupción del suministro eléctrico.
  - ✓ Apagado manual del equipo.
  - ✓ Vandalismo.
  - ✓ Apertura de la carcasa del equipo y robo del disco duro.
  - ✓ Monitoreo del tráfico de red.
- ***Intercepción de comunicaciones:***
  - ✓ Secuestro de sesión.
  - ✓ Falsificación de identidad.
  - ✓ Redireccionamiento o alteración de mensajes.
- ***Denegaciones de servicio:*** El objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:
  - ✓ Explotación de las debilidades del protocolo TCP/IP.
  - ✓ Explotación de las vulnerabilidades del software del servidor.
- ***Intrusiones:***
  - ✓ Análisis de puertos.
  - ✓ Elevación de privilegios: Este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio.
  - ✓ Ataques malintencionados (virus, gusanos, troyanos).

- ***Ingeniería social:*** en la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.
- ***Puertas trampa:*** son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento.

Es por ello que los errores de programación de los programas son corregidos con bastante rapidez por su diseñador apenas se publica la vulnerabilidad. En consecuencia, queda en manos de los administradores (o usuarios privados con un buen conocimiento) mantenerse informados acerca de las actualizaciones de los programas que usan a fin de limitar los riesgos de ataques. Además, existen ciertos dispositivos (firewalls, sistemas de detección de intrusiones, antivirus) que brindan la posibilidad de aumentar el nivel de seguridad.

Figura 2.4. Situaciones de ataques
FUENTE: [Machicado C, 2011]

2.10 Tipos de medidas de seguridad o contramedidas

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

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variados. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos y vulnerabilidades del sistema. La definición de una apolítica de seguridad y su implementación a través de una serie de medidas.

En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, también se hace obvio que a mayores y restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambio de las mismas/ **[11]**.

2.11 Planes de contingencia

Cada día es más la importancia que cobra el uso de la tecnología informática en todos los aspectos tanto laborales como personales. Si al utilizar el Internet con frecuencia, en el momento en que no se puede acceder al buzón de correo, o conectarse a la Web, se siente que algo hace falta.

Realmente solo intervenían tres componentes en el proceso de la información: el equipo, los programas, y los datos y solo a estos tres componentes se remontaba la posible falla.

Las razones externas que podrían causar una falla incluían un problema laboral (como una huelga que impedía el acceso al centro de cómputo), o un desastre natural.

Hoy se mantienen los mismos problemas externos, pero se ha complicado y aumentado el número de componentes que se pueden ver afectados por una falla, incluyendo las redes de comunicación, las estaciones de trabajo, y la multiplicidad de equipos de almacenamiento distribuido.

Las implicaciones pueden ser de cuantía menor para una persona que trabaje con un PC pero igualmente desastrosas para la continuidad de su trabajo.

Lo único que realmente permite que una empresa (o una persona) pueda reaccionar adecuadamente a una falta en un proceso crítico es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia. El plan es precisamente lo que su nombre indica, una serie de actividades tendientes a restablecer la operación normal, en el evento de una calamidad (interna o externa).

A manera de comparación, cuando el sistema era centralizado, el proceso era por lotes, y la interface con la máquina era una terminal, lo único que se requería para tener en pié un plan de contingencia de fácil ejecución, era un contrato de reciprocidad con una empresa que tuviera un equipo similar al de uno, y una copia alterna de la información más reciente, de tal manera que se pudiera trasladar el proceso a la instalación de la empresa recíproca. Normalmente se utilizaban horarios nocturnos que por lo general no se ocupaban en el proceso de la empresa que prestaba el servicio.

El proceso de la información era ejecutado en su mayoría, por no decir en su totalidad, por personal del Departamento de Sistemas, por lo que no se requería mayor contenido en un plan de contingencia y se puede decir que tampoco ningún entrenamiento. Se ejecutarían las actividades necesarias para restablecer el servicio. Por último, la información era un reflejo de actividades históricas, no necesariamente se requería de la información para la toma de decisiones.

Para que hoy en día, con lo complejo de los sistemas de información actuales, además de la responsabilidad del usuario en el proceso de su información, los Planes de Contingencia formalizados y probados cobran una importancia máxima al interior de las empresas, e inclusive en el ámbito personal.

Está tan dependiente nuestro trabajo de la información que tengamos a la mano, que se reducen los espacios para estar sin acceso a la misma.

El Plan de Contingencia debe obedecer a un proceso formal y debe ser la conclusión de un proyecto de elaboración del mismo que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba REAL del mismo plan, una capacitación de las personas involucradas y una constante actualización/ **[12]**.

2.12 Análisis y evaluación de metodologías de seguridad de las tecnologías de la información

2.12.1 Metodología de Prevención de Riesgos Informáticos Abierta (PRIMA)

Es un conjunto de metodologías españolas desarrolladas entre los años 1990 y la actualidad con un enfoque subjetivo/ **[13]**. Sus características esenciales son:

- Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad.
- Fácilmente adaptable a cualquier tipo de herramienta.
- Posee cuestionarios de preguntas para la identificación de debilidades o faltas de controles.
- Posee listas de ayuda para los usuarios menos experimentados de debilidades, riesgos y contramedidas (sistema de ayuda).
- Permite fácilmente la generación de informes finales.
- Las "Listas de Ayuda" (Ver Figura 2.6.) y los cuestionarios son abiertos, y por tanto es posible introducir información nueva o cambiar la existente. De ahí la expresión abierta de su nombre.
- Tiene un "¿Qué pasa si...?" cualitativo, y capacidad de aprendizaje al poseer una base de conocimiento o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo.

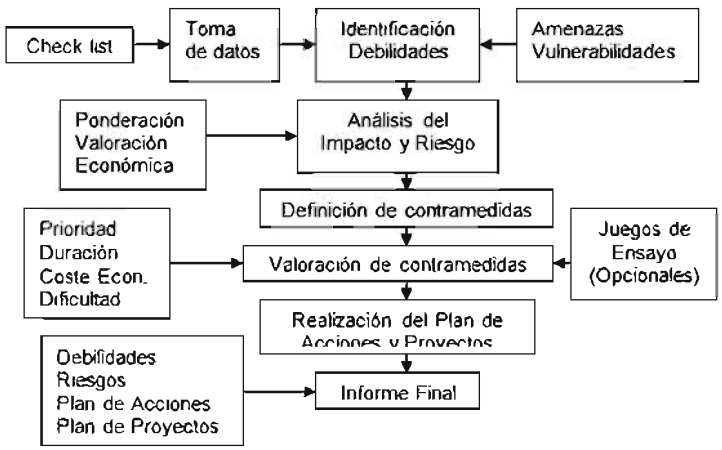


Figura 2.5. Modelo PRIMA

FUENTE: [Navarro S, 2008]

2.12.2 Metodología de análisis y gestión de riesgos de IT (MAGERIT)

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Administraciones Publica.

La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 2.0, publicada en 2006.

Se trata de una metodología abierta, dispone de una herramienta de soporte PILAR II (Proceso Informático – Lógico para el Análisis de la gestión de Riesgos).

La metodología consta de tres volúmenes:

- ***Volumen I – Método,*** es el volumen principal en el que se explica detalladamente la metodología.
- ***Volumen II – Catalogo de elementos,*** complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología.
  Los inventarios que incluye son:
  - ✓ Tipos de activos
  - ✓ Dimensiones y criterios de valoración
  - ✓ Amenazas
  - ✓ Salvaguardas
- **Volumen III – Guía de técnicas**, complementa el volumen principal proporcionando una introducción de algunas técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que presenta son:

  Técnicas específicas para el análisis de riesgos:
  - ✓ Análisis mediante tablas
  - ✓ Análisis algorítmico
  - ✓ Arboles de ataque

  Técnicas generales
  - ✓ Análisis costo-beneficio
  - ✓ Diagramas de flujo de datos (DFD)
  - ✓ Diagramas de procesos

- ✓ Técnicas graficas
- ✓ Planificación de proyectos
- ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
- ✓ Valoración Delphi

La metodología MAGERIT se puede resumir gráficamente de la siguiente forma/ **[14]**:

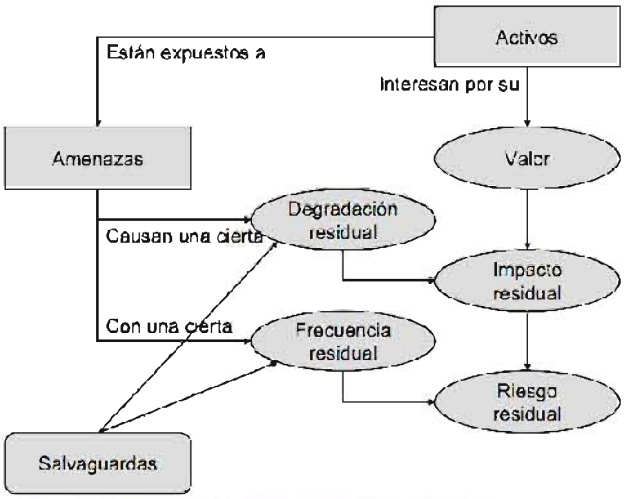


Figura 2.6. Modelo MAGERIT
FUENTE: [Matalobos JM, 2009]

2.12.3 Metodología Abierta de Testeo de Seguridad (OSSTMM)

El objetivo es de crear un método aceptado para ejecutar un test de seguridad minucioso y cabal. Detalles como las credenciales del profesional evaluador de seguridad, el tamaño de la empresa de seguridad, las finanzas, o el respaldo de ventas impactan en la escala y la complejidad del test, pero cualquier experto en redes o en seguridad que cumpla con los requisitos de este manual habrá completado un exitoso perfil de seguridad.

No se encontrará ninguna recomendación a seguir la metodología como si se tratase de un diagrama de flujo. En cambio, se presenta una serie de pasos que deben ser vistos y revistos (repetidas veces) durante la realización de la evaluación exhaustiva. La gráfica de metodología es la manera óptima de llevar a cabo esto, convenientemente de a dos evaluadores, tengan la posibilidad de realizar la metodología/ **[15]**.

Para mayor claridad, ISECOM quienes crearon la metodología OSSTMM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para la Evaluación de la Seguridad de Internet:

Figura 2.7. Sistemas y testeos de seguridad en redes
FUENTE: [OSSTMM, 2009]

1. **Búsqueda de Vulnerabilidades:** Se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. **Escaneo de la Seguridad**: Se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
3. **Test de Intrusión:** Se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.
4. **Evaluación de Riesgo:** Se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. **Auditoría de Seguridad:** hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6. **Hacking Ético:** se refiere generalmente al test de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto. Es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad.

   Los puntos a abarcar en este manual OSSTM son:

   1) *Seguridad de la Información*
   2) *Seguridad de los Procesos*
   3) *Seguridad en las tecnologías de Internet*
   4) *Seguridad en las Comunicaciones*
   5) *Seguridad Inalámbrica*
   6) *Seguridad Física*

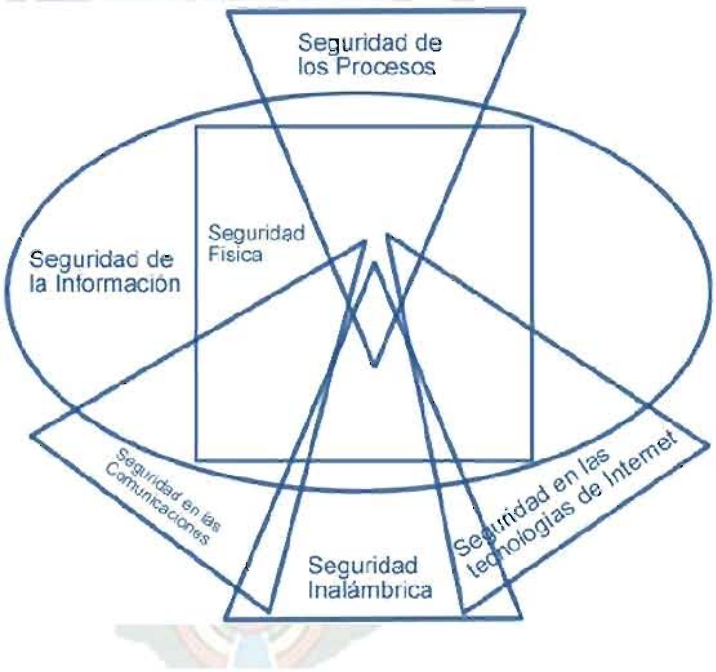


Figura 2.8. Secciones de seguridad en OSSTM
FUENTE: [OSSTMM, 2009]

CAPÍTULO III

MARCO APLICATIVO

Tres reglas de instrumentos de seguridad:

1. herramientas no sabemos cuándo mienten,

2. las herramientas son tan inteligentes como sus diseñadores, y

3. Herramientas sólo pueden trabajar correctamente dentro de los límites del entorno para el que ellos fueron hechos.

3.1 Evaluación de metodologías de seguridad de la información

Se ha recabado información sobre las metodologías de seguridad y permite realizar una mejor y exhaustiva evaluación de seguridad, el proceso de un análisis de seguridad, se concentra en evaluar las áreas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad.

A continuación se presenta la evaluación de metodologías que se realizó:

Puntos a Evaluar	*Metodología de Prevención de Riesgos Informáticos Abierta (PRIMA)*	*Metodología de Análisis y Gestión de Riesgos de IT (MAGERIT)*	*Metodología Abierta de Testeo de Seguridad (OSSTMM)*
Evaluar en el control y logística	**SI**	**SI**	**SI**
Evaluar del sondeo de red dentro de la metodología	**SI**	NO	**SI**
Identificar sobre los servicios de sistemas	NO	NO	**SI**
Revisar de seguridad en el manejo de la privacidad	NO	NO	**SI**
Evaluar sobre la obtención de documentos	**SI**	**SI**	**SI**
Evaluar en la búsqueda y verificación de vulnerabilidades	**SI**	**SI**	**SI**
Evaluar de testeo de aplicaciones de Internet	NO	NO	**SI**
Evaluar sobre seguridad en enrutamiento	NO	NO	**SI**
Evaluar de control de acceso	NO	NO	**SI**
Evaluar en seguridad en sistema de detección de intrusos	NO	NO	**SI**
Evaluar de medidas de contingencia	NO	**SI**	**SI**
Evaluar en descifrado de contraseña	NO	NO	**SI**
Evaluar de Políticas de Seguridad	**SI**	**SI**	**SI**

Tabla 3.1. Evaluacion de las Metodologias de Seguridad

FUENTE: [Machicado ,C. 2011]

3.2 Seguridad en las tecnologías de Internet

El objetivo de esta investigación es evaluar las tecnologías de Internet aplicadas en la DNTI, para mejorar las medidas de resguardo y seguridad de transmisión de datos y de información a través del Internet, mejorando las políticas y normas de seguridad, medidas de control para la aprobación y cumplimiento de estas. La empresa utiliza el Internet para el desarrollo de sus actividades, viendo como un medio rápido y económico de comunicación con las unidades dependientes de la misma ubicadas en otras áreas de la ciudad y en otros departamentos.

Adecuándose al proceso de migración a software libre que se implementando actualmente cumpliendo la actual Ley de Telecomunicaciones, Tecnologías de Información y Comunicación (LEY Nº 164). Requiere, la necesidad de regular:

- Las tecnologías de la información y comunicación,
- Firma y documentos digitales,
- Comercio electrónico,
- Gobierno electrónico, y postal.

La evaluación hace referencia a la sección: "Seguridad en las Tecnologías de Internet", a continuación se muestra que puntos se evaluaran en el presente proyecto:

Seguridad en las tecnologías de Internet
Logística y Controles
Sondeo de Red
Identificación de los Servicios de Sistemas
Revisión de Privacidad
Obtención de Documentos
Búsqueda y Verificación de Vulnerabilidades
Testeo de Aplicaciones de Internet
Enrutamiento
Testeo de Control de Acceso
Testeo de Sistema de Detección de Intrusos
Testeo de Medidas de Contingencia
Descifrado de Contraseña
Evaluación de Políticas de Seguridad

Tabla 3.2. Seguridad en las tecnologías de Internet
FUENTE: [OSSTMM, 2009]

3.2.1 Logística y controles

El propósito es reducir los falsos positivos y negativos realizando los ajustes necesarios en las herramientas de análisis, esto dentro de la Dirección Nacional de Tecnologías de la Información (DNTI).

3.2.1.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Monitorear, medir y controlar el ancho de banda
- Monitorear el tráfico de red
- Monitorea e identificar problemas de enrutamiento

3.2.1.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Controlar los puertos y protocolos de comunicación en Internet
- Controlar el servidor Proxy
- Identificar los protocolos y puertos abiertos
- Monitorear los puertos abiertos
- Probar perdida de paquetes de los protocolos
- Configurar los enrutadores de red
- Controlar y monitorear de consumo de ancho de banda en base a herramientas
- Monitorear y controlar el uso y acceso del Internet por parte de los usuarios

3.2.1.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Discrepancia por el Ancho de Banda usado en el Testeo
- Paquetes TCP perdidos
- Paquetes UDP perdidos
- Paquetes ICMP perdidos
- Problemas de enrutamiento

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(1) Logística y controles

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se tiene control sobre los puertos y protocolos de comunicación en Internet?			
2. ¿Se cuenta con un servidor de control Proxy?			
3. ¿Se tiene identificados los protocolos y puertos abiertos?			
4. ¿Se *monitorea los puertos abiertos*?			
5. ¿Se tiene pruebas e informes sobre la perdida de paquetes de los protocolos?			
6. ¿Se tienen configurados enrutadores de red?			
7. Determine qué tipos de enrutadores tienen configurados (a) interno ☐ (b) externo ☐ (c) ambos ☐			
8. ¿Existen pruebas e informes sobre problemas de enrutamiento interno?			
9. ¿Existen pruebas e informes sobre problemas de enrutamiento externo?			
10. ¿Se tiene control sobre sobre el consumo de ancho de banda?			
11. ¿Se tiene herramientas para el control y monitoreo de consumo de ancho de banda?			
12. ¿Se tiene monitoreo y control para el uso por parte de los usuarios del acceso a internet?			
13. ¿El control al acceso de Internet es personalizado?			
14. ¿Qué tipo de TCP IP se tiene? (a) IPv4 ☐ (b) IPv6 ☐			
15. ¿Se monitorea y se controla el acceso a las páginas web por partes de los usuarios?			

Tabla 3.3. CheckList Logística y controles

FUENTE: [Machicado C, 2011]

3.2.2 Sondeo de red

El sondeo de red sirve como introducción a los sistemas a ser analizados dentro de la DNTI. Sé define como una combinación de recolección de datos, obtención de información y política de control.

3.2.2.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Identificar nombres de dominio
- Identificar nombres de servidores
- Identificar direcciones IP
- Obtener un mapa de red
- Identificar información ISP / ASP
- Identificar propietarios del sistema y del servicio

3.2.2.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Verificar que la empresa cuenta con un dominio propio
- Verificar que la página web pública está configurada en un servidor propio
- Configurar el servidor DNS
- Controlar y monitorear sobre el servidor DNS
- Verificación sobre la configuración de subdominios
- Tener el control y monitoreo en el tráfico de red de datos

3.2.2.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Obtención de nombres de dominio
- Obtención de nombres de servidores
- Direcciones IP
- Mapa de red
- Información ISP / ASP
- Propietarios del sistema y del servicio
- Posibles limitaciones del test

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(2) Sondeo de red

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿La empresa cuenta con un dominio propio?			
2. ¿Cuenta con una página web publica?			
3. ¿La página web pública está configurada en un servidor propio?			
4. ¿Se tiene configurado servidor DNS?			
5. La configuración del servidor DNS es: (a) primario ☐ (b) secundario ☐			
6. ¿Se tiene control y monitoreo sobre el servidor DNS?			
7. ¿Se tiene *configurado subdominios*?			
8. ¿Se tiene servidor web?			
9. ¿Se tiene aplicaciones en el servidor web?			
10. Cuenta con aplicaciones web: (a) publica ☐ (b) privada ☐ (c) ambos ☐			
11. ¿Se tiene control y monitoreo sobre las aplicaciones web?			
12. ¿Las aplicaciones web *están* debidamente protegidas?			
13. ¿Se lleva control y monitoreo en el código fuente y scripts, aplicaciones web en busca de bugs?			
14. ¿Se tiene un diagrama de red actualizado?			
15. ¿Se tiene el control y monitoreo en el tráfico de red de datos?			

Tabla 3.4. CheckList Sondeo de red

FUENTE: [Machicado C, 2011]

3.2.3 Identificación de los servicios de sistemas

Se deben enumerar los servicios de Internet activos o accesibles así como traspasar los cortafuegos con el objetivo de encontrar más máquinas activas.

3.2.3.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Identificar puertos abiertos, cerrados y filtrados
- Identificar direcciones IP de los sistemas activos
- Identificar tipos de servicios
- Identificar tipo y nivel de parcheado de las aplicaciones de los servicios
- Identificar tipo de Sistema Operativo
- Listar los sistemas activos
- Mapeo de la red

3.2.3.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Detallar los servidores de la DNTI
- Control de accesos a los servidores de la DNTI
- Tener personal capacitado para elaborar las configuraciones en los servidores de la DNTI
- Tener políticas de control de accesos a los servicios de la DNTI

3.2.3.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Puertos abiertos, cerrados y filtrados
- Direcciones IP de los sistemas activos
- Tipos de servicios
- Tipo y nivel de parcheado de las aplicaciones de los servicios
- Tipo de Sistema Operativo
- Lista de sistemas activos

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(3) Identificación de los servicios de sistemas

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se tiene detalle de los servidores?			
2. ¿Se tiene procedimientos de la instalación de cada uno de los servidores?			
3. ¿Se tiene el control de accesos a los servidores?			
4. ¿Se tiene el personal capacitado para elaborar las configuraciones en los servidores?			
5. ¿Se tiene políticas de copias de seguridad de la información de los servidores?			
6. ¿Se elaboraron pruebas de intrusión en los servidores?			
7. ¿Se tiene todos los parches actualizados en todos los servidores?			
8. ¿Se tiene identificada las aplicaciones y sus versiones en sus sistemas?			
9. ¿Se tiene relacionado los puertos abiertos con cada servicio y protocolos?			
10. ¿Se tiene identificado los componentes de servicios en escucha?			
11. ¿Se elaboraron tiempos de respuesta de los sistemas y los sistemas operativos?			
12. ¿Se han hecho pruebas de intrusión al firewall de la conexión de Internet?			
13. ¿Se tiene listado de los servicios?			
14. ¿Se tiene políticas de control de accesos a los servicios?			
15. ¿Se tiene procedimientos de la instalación de cada uno de los servicios?			

Tabla 3.5. CheckList Identificación de los servicios de sistemas

FUENTE: [Machicado C, 2011]

3.2.4 Revisión de privacidad

La revisión de privacidad se centra en cómo se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a los empleados.

3.2.4.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Listar cualquier revelación
- Listar las inconsistencias entre la política que se ha hecho pública y la práctica actual que se hace de ella
- Listar los sistemas involucrados en la recolección de datos
- Listar las técnicas de recolección de datos
- Listar los datos recolectados

3.2.4.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Identificar la política de privacidad pública
- Identificar los formularios web
- Identificar el tipo y la localización de la base de datos donde se almacenan los datos recolectados
- Identificar los datos recolectados por la organización
- Identificar la localización de los datos almacenados
- Identificar los tipos de cookies
- Identificar el tiempo de expiración de las cookies

3.2.4.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Listado de cualquier revelación
- Listado de las inconsistencias entre la política que se ha hecho pública y la práctica actual que se hace de ella
- Listado de los sistemas involucrados en la recolección de datos
- Listado de las técnicas de recolección de datos

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(4) Revisión de privacidad

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen políticas y normas de seguridad para las medidas preventivas y reactivas?			
2. ¿Existen medidas preventivas y reactivas para garantizar la confidencialidad de la información?			
3. ¿Existen medidas preventivas y reactivas para garantizar la disponibilidad de los servicios?			
4. ¿Existen medidas preventivas y reactivas para garantizar la integridad de los servidores?			
5. ¿Existen medidas preventivas y reactivas para garantizar la confiabilidad de los sistemas tecnológicos?			
6. ¿Existen medidas preventivas y reactivas que permitan resguardar y proteger la información?			
7. ¿Existen normas y políticas de los niveles de clasificación de la información?			
8. ¿Existen medidas y servicios para resguardar de los sistemas de transferencia de información?			
9. ¿Existen medidas de control en códigos ocultos?			
10. ¿Existen medidas de control en datos de revisión?			
11 ¿Existen políticas y normas de control y resguardo de la información de empleados?			
12. Se cuenta con formularios de registro de empleados: (a) web ☐ (b) digital ☐ (b) documento ☐			
13. ¿Existen controles que se realiza para el acceso y salida de los empleados?			
14. ¿Existen controles sobre resguardo de la información de la dirección que poseen los empleados?			
15. ¿Existe control de transmisión de datos de información?			

Tabla 3.6. CheckList Revisión de privacidad

FUENTE: [Machicado C, 2011]

3.2.5 Obtención de documentos

Es importante para la verificación de gran cantidad de la información probada y pertenece a muchos de los niveles de lo que se considera seguridad de la información.

3.2.5.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar el perfil de la organización
- Evaluar el perfil de los empleados
- Evaluar el perfil de la red de la organización
- Evaluar el perfil de las tecnologías utilizadas por la organización

3.2.5.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Ajustar la estructura orgánica actual a las disposiciones jurídicas vigentes
- Contar con ordenamientos legales en que se sustenta la dirección de informática
- Contar con una estructura encaminada a la consecución de los objetivos del área
- Permitir que la estructura actual que se lleven a cabo con eficiencia las atribuciones encomendadas
- Permitir que la estructura actual que se lleven a cabo con eficiencia las funciones establecidas
- Tener niveles jerárquicos establecidos actualmente es necesario y suficiente para el desarrollo de las actividades del área
- Permitir que los niveles jerárquicos actuales que se desarrolle adecuadamente la supervisión

3.2.5.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Un perfil de la organización
- Un perfil de los empleados
- Un perfil de la red de la organización

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(5) Obtención de documentos

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se ajusta la estructura orgánica actual a las disposiciones jurídicas vigentes?			
2. ¿Se cuenta con ordenamientos legales en que se sustenta la dirección de informática?			
3. ¿Se cuenta con una estructura encaminada a la consecución de los objetivos del área?			
4. ¿Permite la estructura actual que se lleven a cabo con eficiencia las atribuciones encomendadas?			
5. ¿Permite la estructura actual que se lleven a cabo con eficiencia las funciones establecidas?			
6. ¿Permite la estructura actual que se lleven a cabo con eficiencia las distribuciones del trabajo?			
7. ¿Permite la estructura actual que se lleven a cabo con eficiencia el control interno?			
8. ¿Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área?			
9. ¿Cuáles y por qué son sus recomendaciones? Respuesta. _____			
10. ¿Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la operación?			
11. ¿Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la supervisión?			
12. ¿Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente el control?			
13. ¿Permiten los niveles actuales que se tenga una ágil comunicación ascendente?			
14. ¿Permiten los niveles actuales que se tenga una ágil comunicación descendente?			
15. ¿Permiten los niveles actuales que se tenga una ágil toma de decisiones?			

Tabla 3.7. CheckList Obtención de documentos

FUENTE: [Machicado C, 2011]

3.2.6 Búsqueda y verificación de vulnerabilidades

La finalidad es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

3.2.6.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar tipo de aplicación o servicio por vulnerabilidad
- Evaluar niveles de parches de los sistemas y aplicaciones
- Listar posibles vulnerabilidades de denegación de servicio
- Listar vulnerabilidades actuales eliminando falsos positivos
- Listar sistemas internos o en la DMZ
- Evaluar el Mapa de red

3.2.6.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Identificación de los niveles de seguridad de la red interna
- Identificación de los niveles de seguridad de los servicios
- Identificación de los niveles de seguridad de los servidores
- Tener identificados los niveles de seguridad por los anillos de seguridad

3.2.6.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Tipo de aplicación o servicio por vulnerabilidad
- Niveles de parches de los sistemas y aplicaciones
- Listado de posibles vulnerabilidades de denegación de servicio
- Listado de vulnerabilidades actuales eliminando falsos positivos
- Listado de sistemas internos o en la DMZ
- Listado de convenciones para direcciones de e-mail, nombres de servidores, etc..
- Mapa de red

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(6) Búsqueda y verificación de vulnerabilidades

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se tiene identificados los niveles de seguridad de la red interna?			
2. ¿Se tiene identificados los niveles de seguridad de los servicios?			
3. ¿Se tiene identificados los niveles de seguridad de los servidores?			
4. ¿Existen herramientas que garanticen un buen resultado de los testeos realizados?			
5. ¿Existen medidas preventivas y reactivas para determinar vulnerabilidades en las herramientas de seguridad?			
6. ¿Existen medidas preventivas y reactivas para determinar vulnerabilidades en los equipos de comunicación?			
7. ¿Se tiene identificados los niveles de seguridad por los anillos de seguridad?			
8. ¿Se tiene identificado las posibles vulnerabilidades en la red interna?			
9. ¿Se tiene identificado las posibles vulnerabilidades en los servidores?			
10. ¿Se tiene identificado las posibles vulnerabilidades en los servicios?			
11. ¿Cuenta con las herramientas adecuadas para el testeo de vulnerabilidades?			
12. ¿Se realizan pruebas para identificar errores de configuración?			
13. ¿Se tiene identificado el flujo de datos de entrada y salida de red local (LAN)?			
14. ¿Se tiene identificado el flujo de datos de entrada y salida de red extensa (WAN)?			
15. ¿Se tiene identificado el flujo de datos de entrada y salida de red Internet?			

Tabla 3.8. Checklist Búsqueda y verificación de vulnerabilidades

FUENTE: [Machicado C, 2011]

3.2.7 Testeo de aplicaciones de Internet

En este módulo, nos referimos a aplicaciones cliente/servidor que sean desarrolladas por los administradores de sistema con propósitos de la empresa y programadas con cualquier tecnología y lenguaje de programación.

3.2.7.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Listar las aplicaciones
- Listar los componentes de las aplicaciones
- Listar las vulnerabilidades de las aplicaciones
- Listar los sistemas confiados por las aplicaciones

3.2.7.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Tener identificado las limitaciones de uso de ancho de banda
- Tener identificado las limitaciones de uso de transferencia de datos
- Determinar las Especificaciones de Protocolo de la Aplicación Cliente/Servidor
- Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones
- Determinar las limitaciones de control de acceso en las aplicaciones de permisos de acceso, duración de las sesiones, tiempo inactivo
- Determinar si la ID de sesión está formada con información de direcciones IP; mirar si la misma información de sesión puede ser recuperada y reutilizada en otra máquina

3.2.7.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Lista de Aplicaciones
- Lista de los Componentes de las Aplicaciones
- Lista de las Vulnerabilidades de las Aplicaciones
- Lista de los Sistemas Confiados por las Aplicaciones

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(7) Testeo de aplicaciones de Internet

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se cumplen las políticas de contraseña?			
2. ¿Se realizaron pruebas para determinar contraseñas débiles en las aplicaciones?			
3. ¿Se realizaron pruebas para determinar contraseñas débiles en el acceso de servidores y servicios?			
4. ¿Se realizaron pruebas para determinar contraseñas débiles en el acceso a las bases de datos?			
5. ¿Se realizaron pruebas de salto de autentificación?			
6. ¿Se realizaron pruebas de control de acceso en las aplicaciones?			
7. ¿Se realizaron pruebas de permisos de acceso a las aplicaciones (restricciones)?			
8. ¿Se realizaron pruebas de control de acceso en los servidores?			
9. ¿Se realizaron pruebas de permisos de acceso a los servidores (restricciones)?			
10. ¿Se realizaron pruebas de control de acceso en los servicios?			
11. ¿Se realizaron pruebas de permisos de acceso a los servicios (restricciones)?			
12. ¿Se tiene identificado las limitaciones de uso de ancho de banda?			
13. ¿Se tiene identificado las limitaciones de uso de transferencia de datos?			
14. ¿Se tiene identificado vulnerabilidades que se tiene al desbordamiento de memoria en las aplicaciones?			
15. ¿Se cuenta con permisos, autorización y directivas de seguridad de código?			

Tabla 3.9. CheckList Testeo de aplicaciones de Internet

FUENTE: [Machicado C, 2011]

3.2.8 Enrutamiento

Está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado.

3.2.8.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Listar las aplicaciones
- Listar los componentes de las aplicaciones
- Listar las vulnerabilidades de las aplicaciones
- Listar los sistemas confiados por las aplicaciones

3.2.8.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Deben existir políticas de enrutamiento en el tráfico de redes
- Contar con servicio de enrutamiento y acceso remoto
- Contar con conexiones seguras de red privada (VPN)
- Deben existir medidas para garantizar que el filtrado de la red interna hacia Internet sea el correcto
- Verificar el tipo de router con información reunida de la obtención de Inteligencia
- Verificar si el router está filtrando el tráfico de la red local hacia afuera
- Verificar que el router esté haciendo detección de direcciones falsas

3.2.8.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Tipo de router y Propiedades implementadas
- Información del router como servicio y como sistema
- Perfil de la política de seguridad de una red a partir de la ACL
- Lista de los tipos de paquetes que deben entrar en la red
- Mapa de las respuestas del router a varios tipos de tráfico
- Lista de los sistemas vivos encontrados

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(8) Enrutamiento

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen políticas de enrutamiento en el tráfico de redes?			
2. ¿Existen métodos seguros de autenticación en el tráfico de red?			
3. ¿Se cuenta con servicio de enrutamiento y acceso remoto?			
4. ¿Se cuenta con protocolos de enrutamiento dinámico?			
5. ¿Se cuenta con conexiones seguras de red privada (VPN)?			
6. ¿Se cuenta con un filtrado de paquetes IP para seguridad y rendimiento?			
7. ¿Se cuenta con una lista de control de acceso que acepta paquetes?			
8. ¿Se cuenta con una lista de control de acceso que niegue paquetes?			
9. ¿Existen medidas para garantizar que el router esté dando servicios de traducción de direcciones de red (NAT)?			
10. ¿Existen medidas para garantizar que el filtrado de la red interna hacia Internet sea el correcto?			
11. ¿Existen medidas para la detección de direcciones falsas?			
12. ¿Se tiene un diagrama de red que identifique varios tipos de tráfico de la red interna?			
13. ¿Se tienen servicios de red a las aplicaciones manejadas por los usuarios?			
14. ¿Existen medidas que garanticen la entrega confiable entre host?			
15. ¿Existen medidas que se encargan del direccionamiento y mejor ruta de los datos?			

Tabla 3.10. CheckList Enrutamiento

FUENTE: [Machicado C, 2011]

3.2.9 Testeo de control de acceso

Está diseñado para asegurar que solo lo que debe estar expresamente permitido puede ser aceptado dentro de la red, todo lo demás debe ser denegado.

3.2.9.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar la información en el firewall como servicio y como sistema
- Evaluar la información de las características implementadas en el firewall
- Listar los tipos de paquetes que deben entrar en la red
- Listar los tipos de protocolos con acceso dentro de la red
- Listar los paquetes, por número de puerto, que entran en la red
- Listar los protocolos que han entrado en la red
- Listar las rutas sin monitorizar dentro de la red

3.2.9.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Contar con herramientas para realizar el control para proteger la red Interna de Internet (firewall)
- Tener control de acceso a las páginas y servicios del servidor web
- Tener control y resguardo de la configuración del firewall
- Tener identificado los tipos de protocolos de comunicación de red que tienen acceso a la red

3.2.9.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Información en el firewall como servicio y como sistema
- Información de las características implementadas en el firewall
- Lista de los tipos de paquetes que deben entrar en la red
- Lista de tipos de protocolos con acceso dentro de la red
- Lista de paquetes, por número de puerto, que entran en la red
- Lista de protocolos que han entrado en la red

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(9) Testeo de control de acceso

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Se tiene herramienta para realizar el control para proteger la red Interna de Internet (firewall)?			
2. ¿Se tiene herramienta para realizar el control para proteger la red Interna hacia la Internet (firewall)?			
3. Está clasificado el control acceso en: (a) autenticación ☐ (b) sesión de derechos (autorización de privilegios) ☐			
4. ¿Se tiene control de acceso a las páginas y servicios del servidor web?			
5. ¿Se utiliza herramientas de encriptación (cifrado) para el tráfico de datos?			
6. ¿Se tiene control y resguardo de la configuración del firewall?			
7. ¿Existe políticas y normas de seguridad de la red a ACL?			
8. ¿Se tiene identificado los tipos de paquetes que deben entrar a la red?			
9. ¿Se tiene identificado los tipos de protocolos de comunicación de red que tienen acceso a la red?			
10. ¿Se tiene identificado el ingreso de paquetes por puertos de comunicación?			
11. ¿Se tienen medidas de monitoreo al tráfico de red?			
12. ¿Se tiene medidas de monitoreo de los servidores?			
13. ¿Se tiene medidas de monitoreo de los servicios?			
14. ¿Existe medidas para garantizar el filtrado de paquetes del firewall?			
15. ¿Existe medidas para garantizar que se deben tener los puertos adecuados abiertos?			

Tabla 3.11. CheckList Testeo de control de acceso

FUENTE: [Machicado C, 2011]

3.2.10 Testeo de sistema de detección de intrusos

Este test está enfocado al rendimiento y susceptibilidad de un IDS. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunos de estos tests están relacionados con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos tests.

3.2.10.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar el tipo de IDS
- Evaluar tipo de protocolos eliminados o no escaneados por el IDS
- Evaluar el tiempo de reacción y tipo del IDS
- Evaluar la susceptibilidad del IDS
- Listar los falsos positivos del IDS
- Listar las alarmas perdidas del IDS
- Listar las rutas no monitorizadas en la red

3.2.10.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Determinar la esfera de protección o influencia
- Testear los estados de alarma del IDS
- Encontrar alertas de IDS sobre escaneos de vulnerabilidades
- Encontrar alertas de IDS sobre descifrado de contraseñas
- Resultado de la evaluación

3.2.10.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Tipo de IDS
- Tipo de protocolos eliminados o no escaneados por el IDS
- Nota del tiempo de reacción y tipo del IDS
- Nota de la susceptibilidad del IDS
- Lista de falsos positivos del IDS
- Lista de alarmas perdidas del IDS

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(10) Testeo de detección de intrusos

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen medidas o sistemas de detección de Intrusos?			
2. ¿Existen medidas de rendimiento del IDS para soporte sobrecarga?			
3. ¿Existen medidas para identificar paquetes eliminados por el IDS?			
4. ¿Existe medidas para identificar protocolos de comunicación eliminados por el IDS?			
5. ¿Existe evaluación de tiempos de respuestas del IDS?			
6. ¿Existe evaluación de tipos de respuestas del IDS?			
7. ¿Existe mapa de reglas del IDS?			
8. ¿Se tiene identificado las alarmas perdidas del IDS?			
9. ¿Se tiene identificado las rutas no monitorizados en la red?			
10. ¿Se tiene identificado los estados de alarma del IDS?			
11. ¿Existen medidas para comprobar si la configuración del IDS soporta múltiples y variados ataques (inundación)?			
12. ¿Se tiene identificado las alertas del IDS sobre scaneo de vulnerabilidades?			
13. ¿Se tiene identificado las alertas del IDS sobre descifrado de contraseñas?			
14. ¿Se tiene identificado las alertas del IDS sobre testeo de sistemas confiados?			
15. ¿Se tiene herramientas de manejo de paquetes fragmentados?			

Tabla 3.12. CheckList Testeo de detección de intrusos

FUENTE: [Machicado C, 2011]

3.2.11 Testeo de medidas de contingencia

Las medidas de contingencia dictan el manejo de lo atravesable, programas maliciosos y emergencias.

3.2.11.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar las capacidades Anti-Troyano
- Evaluar las capacidades Anti-Virus
- Listar los recursos de contingencia

3.2.11.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Existencia de procedimientos de medidas de contingencia
- Existencia de medidas de contingencia para garantizar la continuidad de las operaciones en la red
- Contar con un plan de contingencia de los sistemas de información
- Existencia de medidas para asegurar la capacidad de los servidores (copias de seguridad)
- Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos están protegidos desde este subsistema
- Verificar las propiedades del sistema de contingencia
- Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos

3.2.11.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Definición de las capacidades Anti-Troyano
- Definición de las capacidades Anti-Virus
- Identificación de las Medidas de Contingencia de Escritorio
- Identificación de las Debilidades de Contingencia de Escritorio
- Lista de recursos de contingencia

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(11) Testeo de medidas de contingencia

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen procedimientos de medidas de contingencia?			
2. ¿Existen medidas de contingencia para garantizar la continuidad de las operaciones en la red?			
3. ¿Se tiene herramientas para la detección de intentos de acceso a los recursos protegidos?			
4. ¿Se cuenta con un plan de análisis de riesgos de sistemas?			
5. ¿Se tiene un periodo crítico de recuperación de los procesos?			
6. ¿Existe un análisis de aplicaciones críticas para establecer las prioridades del proceso?			
7. ¿Se cuenta con un plan de contingencia de los sistemas de información?			
8. ¿Existen medidas para asegurar la capacidad de las comunicaciones?			
9. ¿Existen medidas para asegurar la capacidad de los servidores (copias de seguridad)?			
10. ¿Existe procedimientos de siniestros analizados de información?			
11. ¿Existen procedimientos de recuperación de información?			
12. ¿Se tiene elaborado un manual de contingencias?			
13. ¿Los empleados tienen conocimiento sobre los planes de contingencia?			
14. ¿Existe procedimientos de las medidas de contingencia de Escritorio?			
15. ¿Existe procedimientos de las debilidades de contingencia de Escritorio?			

Tabla 3.13. CheckList Testeo de medidas de contingencia

FUENTE: [Machicado C, 2011]

3.2.12 Descifrado de contraseñas

El descifrado de contraseñas no debe ser confundido con el de recuperación de contraseñas vía escucha de texto por canales libres, es más sencillo de entender que un trastorno del sistema de seguridad, pero solo que tiene mecanismos de autenticación sin cifrar, nada de debilidades en contraseñas.

3.2.12.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Evaluar los ficheros de contraseñas descifrados o no descifrados
- Listar las cuentas, con usuario o contraseña de sistema
- Listar los sistemas vulnerables a ataques de descifrado de contraseñas
- Listar los archivos o documentos vulnerables a ataques de descifrado de contraseñas
- Listar los sistemas con usuario o cuenta de sistema que usan las mismas contraseñas

3.2.12.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Existencia de medidas de restablecimiento de contraseñas de las cuentas de usuario
- Existencia de medidas de cifrado de contraseñas
- Contar con mecanismos de control de almacenamiento de contraseñas
- Contar con un ocultamiento de ingreso de contraseña de circulación por la red

3.2.12.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Ficheros de Contraseñas descifrados o no descifrados
- Lista de cuentas, con usuario o contraseña de sistema
- Lista de sistemas vulnerables a ataques de descifrado de contraseñas

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(12) Descifrado de contraseñas

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen normas y políticas de contraseña?			
2. ¿El personal tiene conocimiento de políticas de contraseña?			
3. ¿Existen normas y política para el cambio de contraseñas cada cierto periodo?			
4. ¿Existen medidas de control para concientizar al usuario de usar contraseñas complejas?			
5. ¿Se tiene un listado de sistemas vulnerables a ataques por descifrado de contraseña?			
6. ¿Se tiene un listado de archivos o documentos vulnerables a ataques por descifrado de contraseña?			
7. ¿Se tiene un listado de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas?			
8. ¿Existe medida de registro de un ataque automatizado?			
9. ¿Existen medidas de control y prevención contra ataques de fuerza bruta?			
10. ¿Existen herramientas de generación de contraseñas?			
11. ¿Existen medidas de control para el tiempo de vida de las contraseñas?			
12. ¿Existen medidas de restablecimiento de contraseñas de las cuentas de usuario?			
13. ¿Existen medidas de cifrado de contraseñas?			
14. ¿Se cuenta con mecanismos de control de almacenamiento de contraseñas?			
15. ¿Se cuenta con un ocultamiento de ingreso de contraseña de circulación por la red?			

Tabla 3.14. CheckList Descifrado de contraseñas

FUENTE: [Machicado C, 2011]

3.2.13 Evaluación de políticas de seguridad

La política de seguridad resaltada aquí es el documento escrito legible que contiene las políticas que delinean la reducción de riesgos en una organización con la utilización de tipos específicos de tecnologías.

3.2.13.1. Objetivos de la evaluación

Los objetivos de la evaluación de seguridad de Internet en la DNTI son:

- Comparar la política de seguridad contra el estado actual de la presencia en Internet
- Aprobar la búsqueda de cualquier signo que revele que la política está aprobada por la gerencia
- Cerciorar que la documentación está adecuadamente almacenada
- Identificar los procedimientos de manejo de incidentes
- Verificar los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet

3.2.13.2. Alcances de la evaluación

Los alcances de la evaluación de seguridad de Internet en la DNTI son:

- Existencia de implementación de normas y políticas de seguridad
- Existencia de medidas para actualizar y mejorar las normas y políticas de seguridad
- Existencia de medidas para el cumplimiento de las normas y políticas de uso de internet
- Existencia de medidas para el cumplimiento de las normas y políticas de uso de servicios

3.2.13.3. Resultados de la evaluación

Los resultados de la evaluación de seguridad de Internet en la DNTI serían:

- Evaluar resultados de existencia de políticas de seguridad
- Cumplir las reglas que exigen la implementación de medidas de seguridad
- Debe existir una regla que indique que la administración remota
- Verificar que la política de seguridad establezca las medidas de contención

Para cumplir con los objetivos ya mencionados se realizara el siguiente Check List:

(13) Evaluación de políticas de seguridad

PREGUNTAS	*SI*	*NO*	*OBSERVACIONES*
1. ¿Existen implementados normas y políticas de seguridad?			
2. ¿Se cumple a cabalidad las normas y políticas de seguridad?			
3. ¿El personal tiene conocimiento de las normas y políticas de seguridad?			
4. ¿Existen medidas para garantizar el cumplimiento de las normas y políticas de seguridad?			
5. ¿Existen medidas para actualizar y mejorar las normas y políticas de seguridad?			
6. ¿Existe medidas para garantizar que la documentación de las políticas y normas de seguridad este adecuadamente almacenada?			
7. ¿Existe medidas de control para garantizar que la documentación de las normas y políticas de seguridad sea manipulada por el personal adecuado?			
8. ¿Existen procedimientos de manejo de incidentes?			
9. ¿Se tiene identificado los procedimientos de manejo de incidentes?			
10. ¿El personal que se encarga sobre la brecha de seguridad de la información está debidamente capacitada?			
11. ¿Existen medidas para el cumplimiento de las normas y políticas de uso de internet?			
12. ¿Existen medidas para el cumplimiento de las normas y políticas de uso de servicios?			
13. ¿Existen medidas para el cumplimiento de las normas y políticas de uso de servidores?			
14. ¿Existen medidas para el cumplimiento de las normas y políticas de acceso a la información?			
15. ¿Existen medidas para el cumplimiento de las normas y políticas de acceso físico?			

Tabla 3.15. CheckList Evaluación de políticas de seguridad

FUENTE: [Machicado C, 2011]

CAPÍTULO IV

EVALUACIÓN DE RESULTADOS

Los requisitos de cumplimiento
que imponen las medidas de protección
como un sustituto de la responsabilidad
también son un sustituto de la rendición de cuentas.

4.1 Análisis de resultados

Con el fin de lograr los objetivos planteados al inicio de este proyecto de grado, se vació la información obtenida mediante los Check List y para obtener el valor adecuado de cada uno de estos Check List se usó la ISO 27004 para realizar la medición correcta de cada uno de estos punto de seguridad tomados en el campo del Internet orientado en la Dirección Nacional de Tecnologías de la Información (DNTI).

A continuación se hará un detalle individual estadístico de los puntos tomados dentro de la evaluación en tecnologías de Internet de la OSSTM.

4.1 Logística y controles

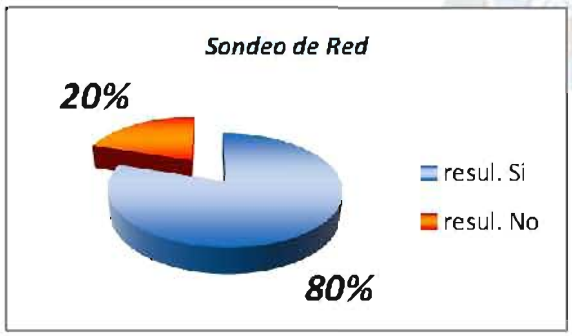
Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a logística y controles dentro la DNTI son:

Resultados Si	Resultados No
73,33 %	26,66 %

Figura 4.1. Resultado individual de la evaluacion en Logística y controles
FUENTE: [Machicado C, 2011]

4.2 Sondeo de red

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al sondeo de red dentro la DNTI son:



Resultados Si	Resultados No
80 %	20%

Figura 4.2. Resultado individual de la evaluacion en Sondeo de red
FUENTE: [Machicado C, 2011]

4.3 Identificación de los servicios de sistemas

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a la identificación de los servicios de sistemas dentro la DNTI son:

Resultados SI	Resultados No
26,66 %	73,33 %

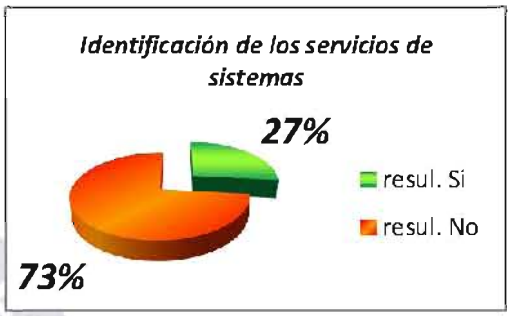
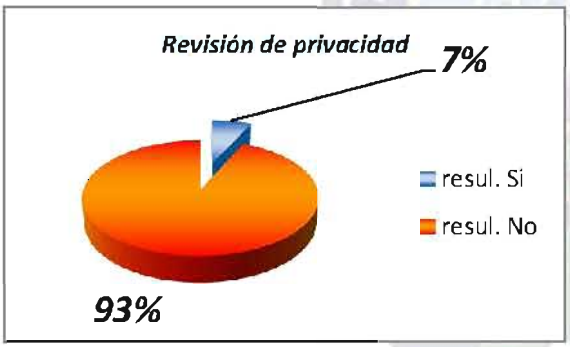


Figura 4.3. Resultado individual de la evaluacion en Identificación de los servicios de sistemas

FUENTE: [Machicado C, 2011]

4.4 Revisión de privacidad

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a la revisión de privacidad dentro la DNTI son:



Resultados SI	Resultados No
6,66 %	93,33 %

Figura 4.4. Resultado individual de la evaluacion en Revisión de privacidad

FUENTE: [Machicado C, 2011]

4.5 Obtención de documentos

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a la obtención de documentos dentro la DNTI son:

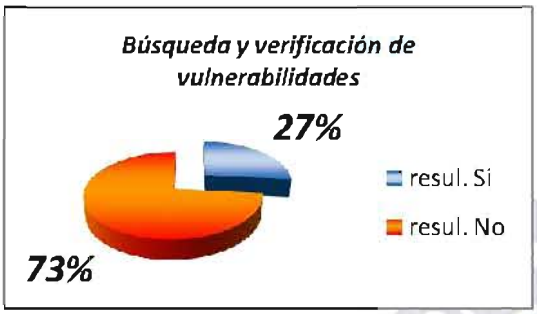
Resultados SI	Resultados No
93,33 %	6,66 %

Figura 4.5. Resultado individual de la evaluacion en Obtención de documentos

FUENTE: [Machicado C, 2011]

4.6 Búsqueda y verificación de vulnerabilidades

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a la búsqueda y verificación de vulnerabilidades dentro la DNTI son:



Resultados Si	Resultados No
26,66 %	73,33 %

Figura 4.6. Resultado individual de la evaluacion en Búsqueda y verificación de vulnerabilidades
FUENTE: [Machicado C, 2011]

4.7 Testeo de aplicaciones de Internet

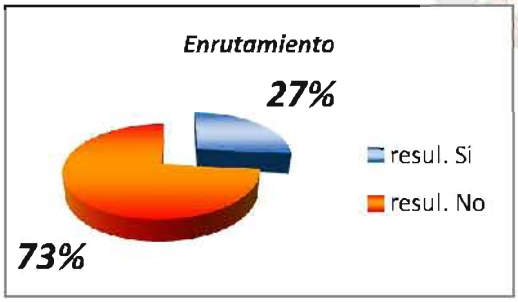
Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al testeo de aplicaciones de Internet dentro la DNTI son:

Resultados Si	Resultados No
13,33%	86,66 %

Figura 4.7. Resultado individual de la evaluacion en Testeo de aplicaciones de Internet
FUENTE: [Machicado C, 2011]

4.8 Enrutamiento

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al enrutamiento dentro la DNTI son:



Resultados Si	Resultados No
26,66 %	73,33 %

Figura 4.8. Resultado individual de la evaluacion en Enrutamiento
FUENTE: [Machicado C, 2011]

4.9 Testeo de control de acceso

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al testeo de control de acceso dentro la DNTI son:

Resultados SI	Resultados No
53,33 %	46,66 %

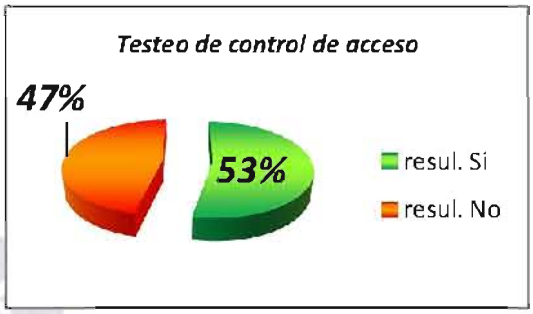
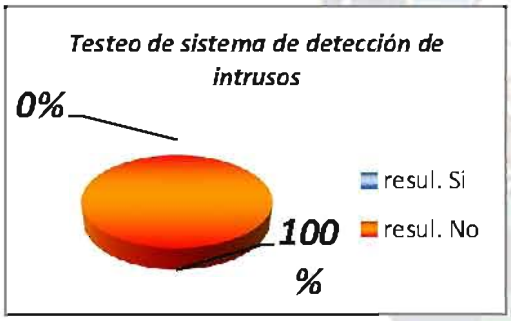


Figura 4.9. Resultado individual de la evaluacion en Testeo de control de acceso
FUENTE: [Machicado C, 2011]

4.10 Testeo de sistema de detección de intrusos

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al testeo de sistema de detección de intrusos dentro la DNTI son:



Resultados SI	Resultados No
0 %	100 %

Figura 4.10. Resultado individual de la evaluacion en Testeo de sistema de detección de intrusos
FUENTE: [Machicado C, 2011]

4.11 Testeo de medidas de contingencia

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al testeo de medidas de contingencia dentro la DNTI son:

Resultados SI	Resultados No
26,66 %	73,33 %

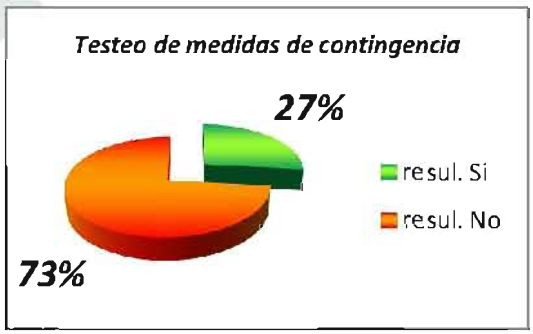
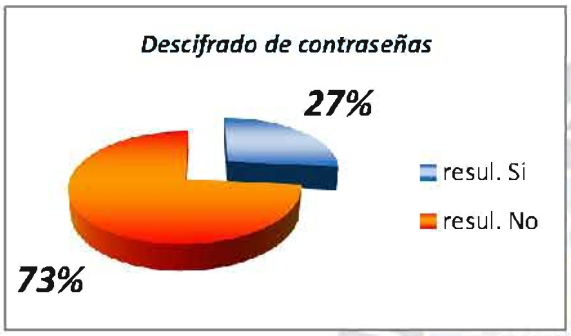


Figura 4.11. Resultado individual de la evaluacion en Testeo de medidas de contingencia
FUENTE: [Machicado C, 2011]

4.12 Descifrado de contraseñas

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo al descifrado de contraseñas dentro la DNTI son:



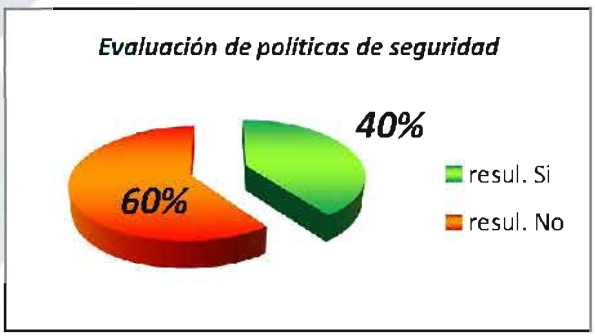
Resultados SI	Resultados No
73,33 %	26,66 %

Figura 4.12. Resultado individual de la evaluacion en Descifrado de contraseñas
FUENTE: [Machicado C, 2011]

4.13 Evaluación de políticas de seguridad

Los valores encontrados en la evaluación en la seguridad en las tecnologías de Internet de acuerdo a la evaluación de políticas de seguridad dentro la DNTI son:

Resultados SI	Resultados No
40%	60 %



4.2 Resultados de la evaluación

Los resultados encontrados están detallados en la siguiente tabla identificando los todos puntos en general en la evaluación que se realizó en la dirección DNTI.

	Excelente 100% - 90%	Buena 80% - 70%	Regular 60% - 50%	Mínimo 40% - 30%	No cumple 20% - 10%
Logística y Controles			46 %		
Sondeo de Red			60 %		
Identificación de los Servicios de Sistemas			46 %		
Revisión de Privacidad					19 %
Obtención de Documentos		77 %			
Búsqueda y Verificación de Vulnerabilidades				37 %	
Testeo de Aplicaciones de Internet				27 %	
Enrutamiento			46 %		
Testeo de Control de Acceso				35 %	
Testeo de Sistema de Detección de Intrusos					0 %
Testeo de Medidas de Contingencia			46 %		
Descifrado de Contraseña				35 %	
Evaluación de Políticas de Seguridad				30 %	

Tabla 4.1. Tabla de resultados en general en la evaluacion de tecnologias de Internet DNTI

FUENTE: [Machicado C, 2011]

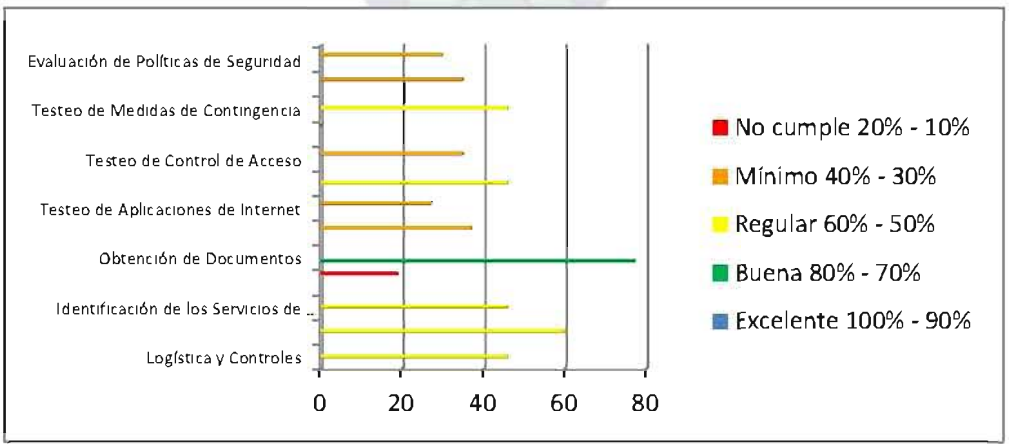


Figura 4.14. Resultado general de la evaluacion de tecnologias de Internet DNTI

FUENTE: [Machicado C, 2011]

4.3 Herramienta de evaluación Backtrack

A continuación se mostrara la utilización de la herramienta Backtrack que es un compilado de herramientas en una para realizar distintas pruebas de penetración en la seguridad en las tecnologías de Internet, dentro de la DNTI, formando parte de la evaluación del presente proyecto.

Como muestra de las pruebas que realiza este compilado de herramientas, se fijara un punto estratégico de ataque que será la aplicación Nmap que es utilizada para identificar el posible S.O de la máquina objetivo. Un atacante puede utilizar esta información para llevar a cabo ataques más elaborados. A diferencia de la herramienta Xprobe2 analizada en la sesión de identificación de banners, Nmap permite otra cantidad de opciones de encubrimiento de IP de la máquina atacante, que no son posibles realizar desde Xprobe2.

A continuación se detalla todos pasos a seguir para realizar la operación de ataque:

Procedimiento: Desde la shell de Linux (BackTrack) ejecutar la siguiente sintaxis:

nmap <opciones> (Dirección IP)

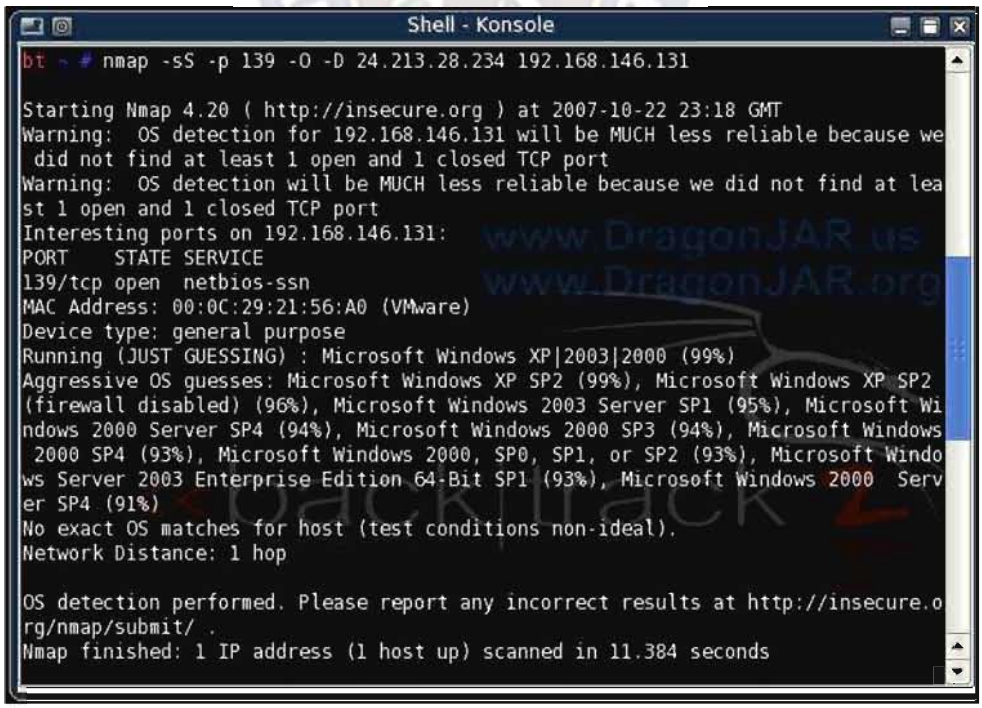


Figura 4.15. Procedimineto de seguridad herramienta Nmap

FUENTE: [Machicado C, 2011]

La demostración del potencial de la herramienta nmap. Se usó un sniffer en la máquina objetivo, para determinar en este caso desde donde viene la consulta y a que puerto en específico.

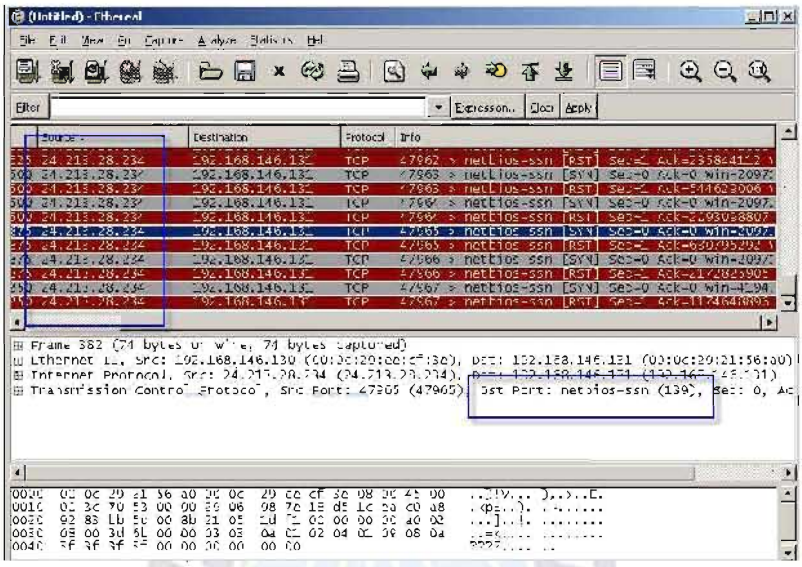


Figura 4.16. Demostración de la herramienta Nmap

FUENTE: [Machicado C, 2011]

Desde la shell de BackTrack se ejecuta ***nmapfe*** comando para ejecutar la herramienta. Escribimos la dirección IP de la máquina objetivo, para este caso 192.168.146.131.

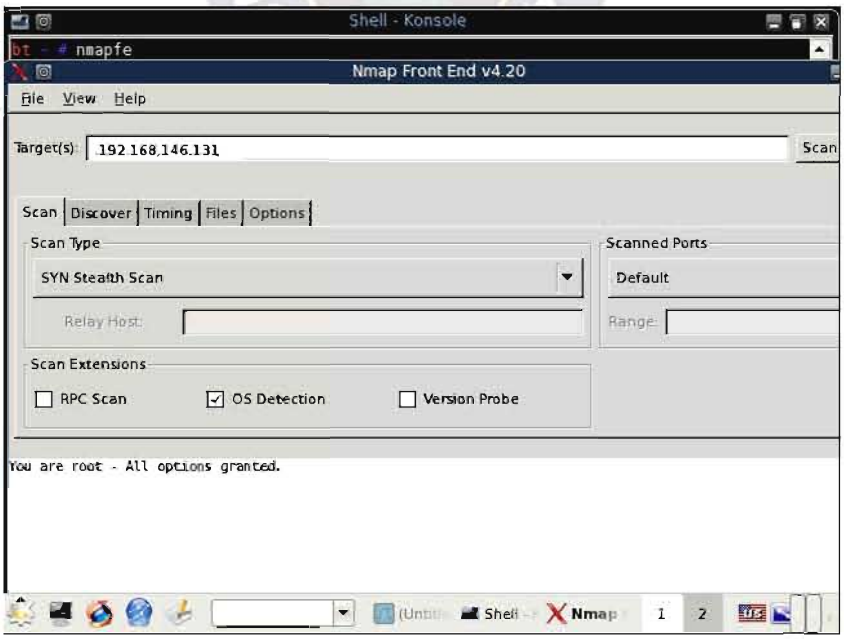


Figura 4.17. Ejecutando nmapfe de la herramienta Nmap

FUENTE: [Machicado C, 2011]

Verificar que la detección del Sistema Operativo este seleccionada.

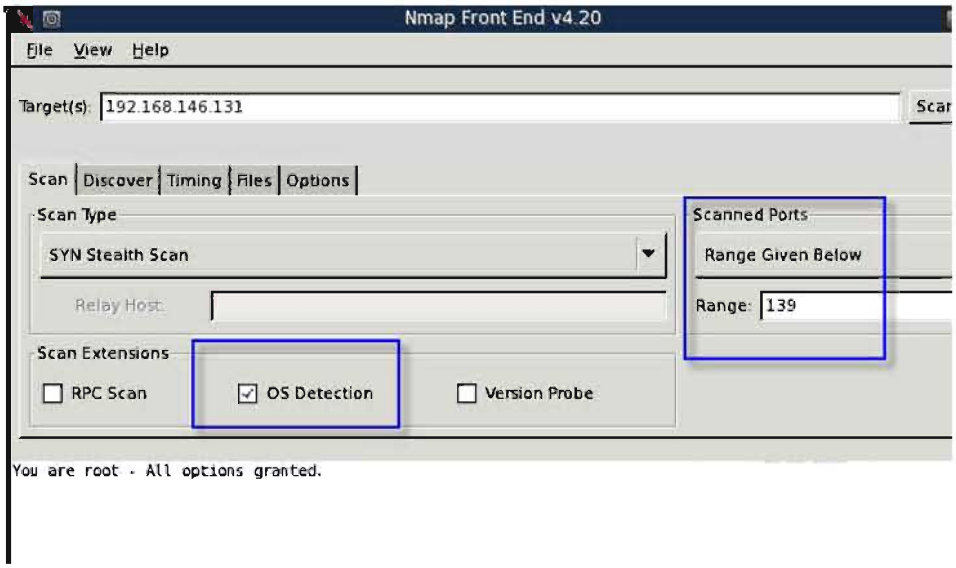


Figura 4.18. Verificacion de selección correcta del Sistema Operativo
FUENTE: [Machicado C, 2011]

Se elige la pestaña de opciones y allí seleccionamos la opción Decoy (la cual nos permite encubrir nuestra IP real), y entramos una IP falsa. Para este caso 24.213.28.234.

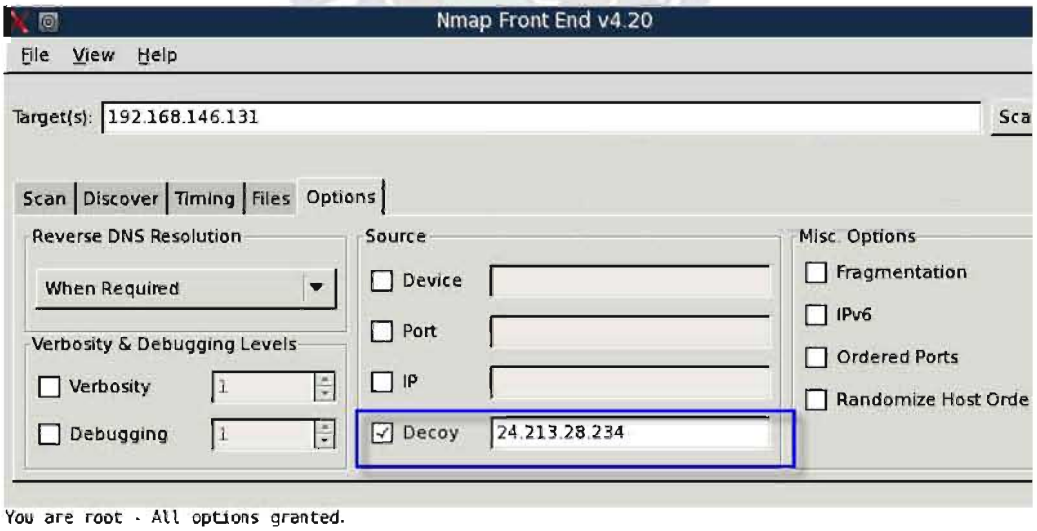


Figura 4.19. Usando la opcion Decoy
FUENTE: [Machicado C, 2011]

Por último clic en Scan y se espera los resultados del testeo.

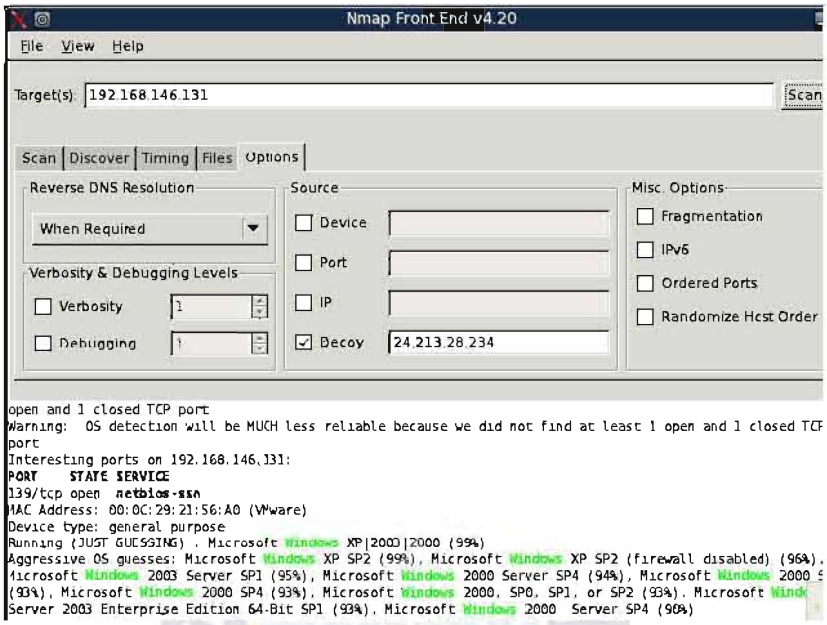


Figura 4.20. Espera de resultados

FUENTE: [Machicado C, 2011]

Al final vemos la identificación de varias máquinas conectadas con el Armitage:

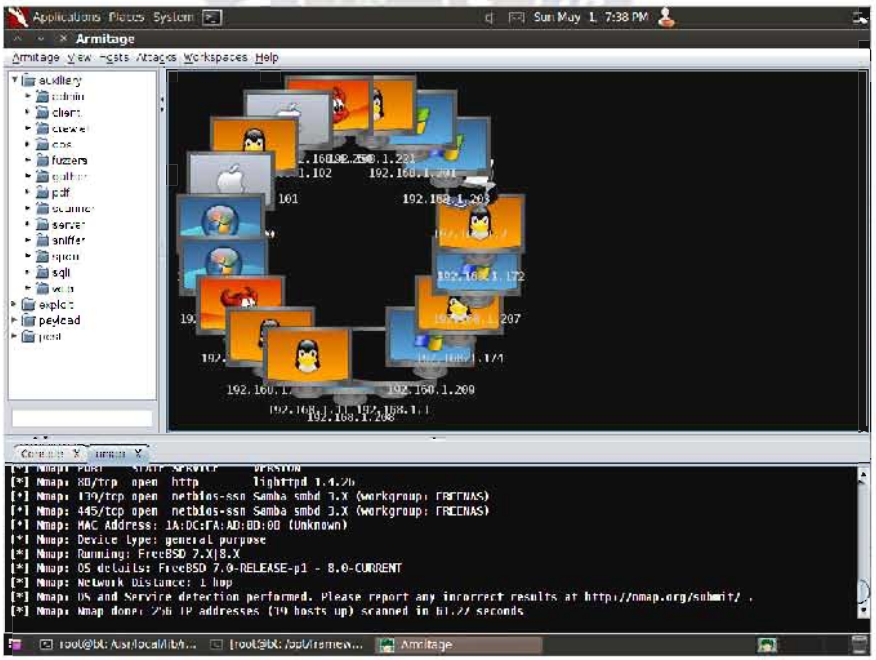


Figura 4.21. Identificación de maquinas conectadas con el Armitage

FUENTE: [Machicado C, 2011]

CAPÍTULO V
COSTOS Y BENEFICIOS

Concienciación sobre la seguridad
debe ser la práctica constante
de una habilidad y
no el recordatorio continuo de una amenaza.

5.1 Evaluación financiera

La rentabilidad está constituida por servicios de seguridad percibidos donde por lo que es conveniente realizar una evaluación con los siguientes indicadores:

5.1.1 Relación de Beneficio Costo (B/c)

Este indicador financiero expresa la rentabilidad en términos relativos. La interpretación de tales resultados es en centavos por cada "euro" ó "dólar" que se ha invertido.

La fórmula que se utiliza es:

Es el valor del dinero en el tiempo que se percibe:

Dónde: ***B/C*** = Relación Beneficio / Costo
B = Valor de la producción (beneficio bruto)
C = Egresos (i = 0, 2, 3,4...n)
ke = Tasa de descuento

El indicador financiero Beneficio Costo (B/c) se realizara de acuerdo a los servicios que se ofrecen al realizar la evaluación de seguridad, a la DNTI. Se tiene los siguientes datos:

TASA DE EXPECTATIVA DE GANACIA 15%

PRECIO POR CONSULTA 100000

PERIODOS	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
INGRESOS	0	0	0	0	0	100000	100000
GASTOS ADMINISTRATIVOS	5000	5000	5000	5000	5000	5000	60000
GASTOS OPERACIÓN	800	800	800	800	800	800	10800
TOTAL EGRESOS	5800	5800	5800	5800	5800	5800	70800
UTILIDAD BRUTA	-5800	-5800	-5800	-5800	-5800	44200	
IUE(25%)	-1450	-1450	-1450	-1450	-1450	11050	7300
UTILIDAD NETA	-4350	-4350	-4350	-4350	-4350	33150	21900

COSTO 63%
BENEFICIO

Tabla 5.1. Relación de Beneficio Costo (B/c)
FUENTE: [Machicado C, 2011]

En consecuencia al obtener un índice costo beneficio positivo mayor a cero, indica que el proyecto es aceptable.

5.1.2 Valor Actual Neto (VAN)

Consiste en actualizar a valor presente los flujos de caja futuros, que va a generar el proyecto, descontados a un cierto tipo de interés (la tasa de descuento), y compararlos con el importe inicial de la inversión. Como tasa de descuento se utiliza normalmente, el costo promedio ponderado del capital de la empresa que hace la inversión.

La fórmula que se utiliza es:

Es el valor del dinero en el tiempo que se percibe:

Dónde: ***ke (%)*** = expectativa de ganancia costo de oportunidad
ke (%) = i + o = costo financiero más riesgo
n = vida útil del proyecto
= Inversión inicial
Fn = flujo financiero de cada periodo

El indicador financiero Valor Actual Neto (VAN) se realizara de acuerdo a los servicios que se ofrecen al realizar la evaluación de seguridad, a la DNTI. Se tiene los siguientes datos:

TASA DE EXPECTATIVA DE GANACIA 15%

PRECIO POR CONSULTA 100000

PERIODOS	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
INGRESOS	0	0	0	0	0	100000	100000
GASTOS ADMINISTRATIVOS	5000	5000	5000	5000	5000	5000	60000
GASTOS OPERACIÓN	800	800	800	800	800	800	10800
TOTAL EGRESOS	5800	5800	5800	5800	5800	5800	70800
UTILIDAD BRUTA	-5800	-5800	-5800	-5800	-5800	44200	29200
IUE(25%)	-1450	-1450	-1450	-1450	-1450	11050	7300
UTILIDAD NETA	-4350	-4350	-4350	-4350	-4350	33150	21900

VAN Bs 7.303,58

Tabla 5.2. Valor Actual Neto (VAN)
FUENTE: [Machicado C, 2011]

En consecuencia al obtener el índice de valor actual neto es mayor a cero el proyecto es rentable.

5.1.3 Tasa Interna de Retorno (TIR)

Para aplicar la TIR, se buscará encontrar una tasa de actualización con la cual el valor actualizado de las entradas de un proyecto, se haga igual al valor actualizado de las salidas.

La ecuación de la TIR es la siguiente:

El indicador financiero Tasa Interna de Retorno (TIR) se realizara de acuerdo a los servicios que se ofrecen al realizar la evaluación de seguridad, a la DNTI. Se tiene los siguientes datos:

TASA DE EXPECTATIVA DE GANACIA	15%
PRECIO POR CONSULTA	100000

PERIODOS	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
INGRESOS	0	0	0	0	0	100000	100000
GASTOS ADMINISTRATIVOS	5000	5000	5000	5000	5000	5000	60000
GASTOS OPERACIÓN	800	800	800	800	800	800	10800
TOTAL EGRESOS	5800	5800	5800	5800	5800	5800	70800
UTILIDAD BRUTA	-5800	-5800	-5800	-5800	-5800	44200	29200
IUE(25%)	-1450	-1450	-1450	-1450	-1450	11050	7300
UTILIDAD NETA	-4350	-4350	-4350	-4350	-4350	33150	21900

TIR 96%

Tabla 5.3. Tasa Interna de Retorno (TIR)
FUENTE: [Machicado C, 2011]

En consecuencia al obtener el índice de tasa interna de retorno es mayor a la tasa de descuento esto indica que el proyecto es aceptable.

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

Cuanto más uno se aleja del concepto
de la seguridad de la prisión,
más necesaria es la cooperación
y las buenas intenciones de las personas
que se están asegurando.

6.1 Conclusiones

De acuerdo con los objetivos planteados y los resultados obtenidos durante el desarrollo de los capítulos anteriores del presente proyecto de titulación, se pueden establecer las siguientes conclusiones:

- Se pudo comprobar que es factible la utilización de la metodología OSSTMM en la DNTI, pues ha cubierto una gran parte de sus necesidades al momento de resguardar la información de la empresa YPFB.

- Una política de seguridad es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de comportamiento del personal, en relación con los recursos y servicios informáticos de la empresa y que en el caso de la DNTI se ve reflejado en la evaluación de políticas de seguridad.

- Las políticas de seguridad, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. De igual manera, deberán establecerse las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

- Al diagnosticar la situación actual de la DNTI, se identificó la falta de políticas de seguridad para vigilar el acceso a la red y a los sistemas informáticos, lo que genera aplicaciones o usos efectuados de manera indebida.

- Fue evidente también la falta de capacitación a los usuarios en cuanto al manejo de la infraestructura y el uso de herramientas de seguridad en el sistema, además Adoptar el plan de contingencias que impacta en la organización, en las funciones y en las responsabilidades, que se mantenga, se pruebe y se actualice periódicamente.

- El trabajo de investigación realizado en este proyecto de titulación, permitió confirmar que son deficientes por ahora las condiciones técnicas, operativas y políticas que facilitan la implementación de lineamientos que apunten hacia el logro de políticas de seguridad a los fines de alcanzar el mejor aprovechamiento del sistema.

6.2 Recomendaciones

Se define las siguientes recomendaciones respecto a la evaluación de seguridad que se realizó:

- Tomar en consideración la implementación de esta metodología para tener un buen manejo de la seguridad en todos aspectos tecnológicos dentro de la empresa, dirigidas dichas prácticas por la DNTI.

- Implementar un plan de contingencia para la seguridad informática, este será una herramienta imprescindible para la recuperación de información, este plan de contingencia debe contemplar tanto la seguridad física, como la seguridad lógica y estaría complementado con un plan de emergencia y con un plan de recuperación de la información.

- Documentar en lo posible las políticas de seguridad a implementar y comunicar a todo el personal involucrado, en el funcionamiento de la DNTI sobre las políticas adquiridas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Fortalecer los conocimientos de todo el personal, tanto administrativo como operativo, con cursos de formación y capacitación en el área de seguridad de la información.

- Definir claramente los permisos y accesos de cada funcionario de la empresa y de todos los usuarios y empleados del sistema de información de la organización.

- Las políticas de seguridad en la DNTI, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, rotación de funcionarios, desarrollo de nuevos servicios.

- Capacitar a los usuarios y empleados en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y a la seguridad física del área de trabajo.

- Crear un programa de educación y entrenamiento a los usuarios y empleados de la empresa en la DNTI que incluya: prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad, la integridad y el desempeño de las tareas de la información.

- Retroalimentar los diferentes planes diseñados para el sistema de información de la DNTI, con todos los incidentes de seguridad deben ser registrados, reportados, revisados y escalados apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas, esto significa que por lo menos cada año se deberá examinar las falencias o debilidades del plan para modificarlo o reforzar los puntos más propensos a desastres.

BIBLIOGRAFÍA

En el arte, el resultado final es una cosa de belleza,
mientras que en la ciencia,
el medio de alcanzar el resultado final es una cosa de belleza.
Cuando una prueba de seguridad
es un arte entonces el resultado es incomprobable
y esto mina el valor de una prueba.
Un modo de asegurar una prueba de seguridad
tiene el valor debe saber
que la prueba correctamente ha sido conducida.

Bibliografía

Se tiene las siguientes fuentes bibliográficas por orden de aparición:

[1] YPFB, Yacimientos Petrolíferos Fiscales Bolivianos [en línea]: documentación de fuentes electrónicas sobre la Internet.2011 [fecha de consulta: 22 de abril de 2011]. Disponible en: <http://ypfb.gob.bo/index.php?option=com_content&view=article&id=126&Itemid=126>

[3] ZENTENO Flores, Lorena Michele. "Guía de auditoría de seguridad de la información" [en línea]: documentación de fuentes académicas en biblioteca de la UMSA.2006 [fecha de consulta: 10 de mayo de 2011].

[4] GARRO, Ayala Máximo. "Método Científico" [en línea]: documentación de fuentes electrónicas sobre la Internet.2003 [fecha de consulta: 21 de mayo de 2011]. Disponible en: <http://www.slideshare.net/maxgarro/metodologia-de-la-investigacion-presentation-954512>

[5] BUNGE, Mario. "Metodología de la investigación científica" [en línea]: documentación de fuentes electrónicas sobre la Internet.2009 [fecha de consulta: 27 de mayo de 2011]. Disponible en: <http://www.slideshare.net/Estadistica22/la-ciencia-y-el-mtodo-cientifico>

[6] LACKERBAUER, Ingo. "Internet" [en línea]: documentación de fuentes electrónicas sobre la Internet.2001 [fecha de consulta: 23 de septiembre de 2011]. Disponible en: <http://books.google.es/books?id=stRFzoTzGrIC&printsec=frontcover&dq=internet&hl=es&ei=vD_WTpLvLo7EgAf-heWgAQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CEIQ6AEwAA#v=onepage&q&f=false>

[7] GARCÍA Fernández, Alfonso. "Nuevas tecnologías en Internet" [en línea]: documentación de fuentes electrónicas sobre la Internet.1999 [fecha de consulta: 23 de septiembre de 2011]. Disponible en: <http://books.google.es/books?id=L6U8cgAACAAJ&dq=TECNOLOGIAS+DE+internet&hl=es&ei=GkHWTsanEMi9gAf9tsy3AQ&sa=X&oi=book_result&ct=result&resnum=4&ved=0CEkQ>

[8] GARCÍA Codina, Carlos. "Seguridad en redes Wan e Internet" [en línea]: documentación de fuentes electrónicas sobre la Internet. 2009 [fecha de consulta: 30 de septiembre de 2011]. Disponible en: <http://www.bubok.es/libros/190290/SEGURIDAD-EN-REDES-WAN-E-INTERNET>

[9] MALDONADO. "Las vulnerabilidades más críticas en Internet" [en línea]: documentación de fuentes electrónicas sobre la Internet. 2009 [fecha de consulta: 30 de septiembre de 2011]. Disponible en: <http://www.vsantivirus.com/20vul.htm>

[10] CABALLERO Quezada, Alonso E. "Seguridad en las Tecnologías de Internet" [en línea]: documentación de fuentes electrónicas sobre la Internet. 2005 [fecha de consulta: 30 de septiembre de 2011]. Disponible en: <http://www.informatizate.net/articulos/seguridad_en_las_tecnologias_de_internet_parte_02_20050207.html>

[11] FRANCO Jiménez, Ma. del Rocío. "Metodología para la auditoría del uso adecuado de la tecnología" [en línea]: documentación de fuentes electrónicas sobre la Internet.2002 [fecha de consulta: 18 de septiembre de 2011]. Disponible en: <http://mario.elinos.org.mx/docencia/semiaud/auditusotecinfo.pdf>

[12] COITE, Angélica. ROMERO Hugo. "Auditoria de sistemas y políticas de seguridad informática"[en línea]: documentación de fuentes electrónicas sobre la Internet.2002 [fecha de consulta: 08 de septiembre de 2011]. Disponible en: <http://www.monografias.com/trabajos12/fichagr/fichagr.shtml>

[13] BAILEY E., Cristian E. R. "Aspectos para auditorias de sistemas de información y tecnologías informáticas e implementación de estándares de seguridad informática" [en línea]: documentación de fuentes electrónicas sobre la Internet.2001 [fecha de consulta: 09 de septiembre de 2011]. Disponible en: <http://www.monografias.com/trabajos32/auditoria-seguridad-informatica/auditoria-seguridad-informatica2.shtml>

[14] NAVARRO Solsol, Linda. "Metodologías de control interno, seguridad y auditoría informática "[en línea]: documentación de fuentes electrónicas sobre la Internet.2005 [fecha de consulta: 19 de septiembre de 2011]. Disponible en: <http://www.google.com.bo/url?sa=t&rct=j&q=metodologias%2Bde%2Bseguridad%2Binformatica%2Bmarion%2B&source=web&cd=6&ved=0CE4QFjAF&url=http%3A%2F%2Fwww.dspace.espol.edu.ec%2Fbitstream%2F123456789%2F5670%2F12%2F12.%2520Tesis.-%2520Cap%25C3%25ADtulo%25202.doc&ei=02m4TsTJOoLm0QGoxbXsBw&usg=AFQjCNGuoRKI8ZUIdGgbKGci8sVGNHVXoA&sig2=g7sAXdW3Fg9z6dCv3QYSmw>

[15] HERZOG Peter V., "OSSTMM Manual de Metodología Abierta de Testeo de Seguridad"[en línea]: documentación de fuentes electrónicas sobre la Internet.2009 [fecha de consulta: 29 de septiembre de 2011]. Disponible en: <http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf>