INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓNY COMUNICACIONES

INVESTIGACIÓN Y ANÁLISIS DE LA IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD EN TECNOLOGÍAS DE INFORMACIÓN BASADO EN EL ESTÁNDAR BS7799 PARA UNA EMPRESA DE MANUFACTURA

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN EN TECNOLOGÍAS DE INFORMACIÓN

POR:

ENRIQUE ORTIZ RAMON

MONTERREY , N.L. DICIEMBRE 2004

INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

PROGRAMAS DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

Los miembros del comité de tesis recomendamos que la presente tesis del Ing. Enrique Ortiz Ramón sea aceptada como requisito parcial para obtener el grado académico de Maestro en Administración de Tecnologías de Información.

Comité de tesis:

_____
Ricardo Morales González, MC.
Asesor

_____
Dr. Macedonio Alanis González
Sinodal

_____
Ernesto Uriel Rey Guillén, MC.
Sinodal

_____
David Alejandro Garza Salazar, PhD.
Director del Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.
Diciembre de 2004

INVESTIGACIÓN Y ANÁLISIS DE LA IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD EN TECNOLOGÍAS DE INFORMACIÓN BASADO EN EL ESTÁNDAR BS7799 PARA UNA EMPRESA DE MANUFACTURA

POR:

ENRIQUE ORTIZ RAMÓN

TESIS

Presentada al Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de Tecnologías de Información

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE 2004

Dedicatoria

A mi esposa Laura por todo su apoyo, amor y cariño incondicional que me inspira para seguir adelante en todos nuestros proyectos de vida

Gracias

Agradecimientos

A mi comité de tesis por el apoyo brindado para la realización de esta tesis.

A Dios, por guiarme por el mejor camino y darme fuerzas para salir adelante.

Gracias

Resumen

Desde el inicio de las redes de sistemas, la filosofía de la estructura de los ambientes interconectados era precisamente el de compartir la información entre varios dispositivos de red, sin tomar en cuenta ningún aspecto de seguridad, poco a poco se fueron dando cuenta que la seguridad en las tecnologías de información es un aspecto muy importante en los dispositivos de red que comparten información, hoy en día implementar un esquema de seguridad es imperativo en todos los aspectos para un correcto desarrollo tecnológico de las empresas.

El estándar británico BS7799 se ha vuelto uno de los principales estándares en la industria para la implementación de los esquemas de seguridad, este estándar es uno de los más completos ya que abarcan todo lo relacionado con los activos de información. Las empresas certificadas con el estándar británico cuentan con prestigio y reconocimiento internacional avalando los esquemas de administración de seguridad y riesgo que operan en esa empresa.

Esta tesis pretende mostrar un esquema de implementación de seguridad en las tecnologías de información enfocado a una empresa de manufactura, este esquema estará basado en el estándar BS7799 para su implementación, con el desarrollo del caso analizado se podrán dar una idea de como se puede implementar un esquema de seguridad de este tipo en una empresa de manufactura, cada empresa es única en su estructura de activos de información por lo que no se pretende establecer una guía estándar para todas las empresas sino sugerir una estructura de implementación para este tipo de empresas.

INDICE

LISTA DE GRÁFICAS

LISTA DE GRÁFICAS

LISTA DE TABLAS

CAPITULO 1

1. Introducción

1.1 Situación Problemática

El crecimiento de las computadoras y las tecnologías de información, ha sido explosivo. Nunca antes se había integrado en todas las actividades humanas la tecnología con tanta rapidez. Las computadoras han traído diversos beneficios a la humanidad como los estudios del genoma humano, exploración espacial, inteligencia artificial, y una amplia gama de aplicaciones para facilidad y mejora de la vida humana (Bosworth, Kabay, 2001).

Desafortunadamente, existe un lado obscuro de la computación: Son usadas para diseñar y crear armas de destrucción masiva así como aviones militares, submarinos nucleares, y estaciones espaciales de reconocimiento. El rol de la computación en formular armas químicas y biológicas y su desarrollo, es uno de sus usos menos prometedores (Bosworth, Kabay, 2001).

Herrmann(2002) afirma que es comúnmente dicho que "la seguridad es poder", esto es cierto por que la información correctamente integrada, analizada y sintetizada, conduce a conocimiento y decisiones fundamentadas. En la actualidad, la vasta mayoría de la información del mundo reside en, es derivada de, y es intercambiada entre sistemas automatizados. Decisiones críticas son hechas (generación de órdenes para comprar o vender acciones por ejemplo), y acciones críticas son hechas (para administrar la transfusión de algún tipo de sangre por ejemplo) basadas en información de estos sistemas. Para que la información se vuelva poder, debe ser precisa, correcta, a tiempo, ser presentada, manipulada, almacenada, recuperada e intercambiada de manera segura y confiable afirma la autora.

Urs y Kelly(2000) establecen; la ley trata de prevenir el daño de los intereses materiales e intelectuales de otros. Sin embargo en el mundo actual, una nueva raza de usuarios de computadoras ha emergido. El "hacker" es el que obtiene gozo descubriendo maneras de exceder actuales limitaciones. De esta manera, los hackers en el sentido original son referidos como exploradores que resuelven problemas y exceden los límites convencionales a través de prueba y error en situaciones las cuales no existen guías de modelos previos en cual se derivan. El comportamiento malicioso, incluyendo la intrusión maliciosa de las computadoras son encarnadas no solo por los hackers si no también por los "crakers". Consecuentemente, los crakers tratan de tomar información

y usar otro hardware y software sin derechos de usarlo y utilizándolo para dañar, destruir o capitalizarse con la información encontrada

Heather Goodell y Scott Meyers (2001), preguntan en su libro Maximum Security, ¿Por qué la seguridad de la información es un gran problema?, define si realmente la seguridad de su organización es valiosa. Información Personal, Números de Tarjetas de Crédito, Información de salario, listas de contactos de clientes y proveedores, estrategias de mercado, esfuerzos y estrategias de investigación y desarrollo, propiedad intelectual, reportes de ganancias, ¿Son estas de algún valor para alguien?
También afirma la importancia de los sistemas que dependen de las computadoras, estos son, por ejemplo:

- Sistemas de Transportación
- Registros financieros personales y corporativos
- Información de pacientes en Hospitales
- Sistemas de procesamiento de tarjetas de crédito
- Cajeros automáticos
- La red telefónica nacional
- Sistemas de control de tráfico aéreo
- Sistemas de potencia

Ahora digamos que un hacker puede atacar y comprometer cualquiera de estos sistemas. Que puede hacer?, bueno puede accesar los registros de salud de cualquier persona, robar dinero de cuentas bancarias, robar tarjetas de crédito, parar el sistema telefónico nacional o más severo, puede robar su identidad, obtener tarjetas de crédito con su nombre, bloquear el sistema aéreo y causar accidentes(Goodel y Meyers,2001).

Neuman (1995) denota: Muchas de las explotaciones de seguridad-vulnerabilidad resultan directamente por una ingeniería pobre de hardware y software.. Desafortunadamente, muchos esfuerzos pasados y existentes de desarrollo de software han fallado en tomar ventaja de una buena práctica de ingeniería; particularmente estos sistemas con requerimientos rigurosos de seguridad y confiabilidad.

Seymour Bosworth, Michel E. Kabay (2001), definen la seguridad como el estado libre de peligro y no expuesto al daño de accidentes o ataque, o puede ser definido como el proceso para lograr ese estado deseable. El objetivo de la seguridad en los sistemas de información es el optimizar el rendimiento de una organización con respecto a los riesgos a los que es expuesto. Riesgo es definido como la oportunidad de lesión, daño, o pérdida. De tal manera, el riesgo tiene dos elementos: 1, Oportunidad

Elemento de incertidumbre, y 2, Perdida o Daño. Excepto por la posibilidad de restitución, las acciones de seguridad en información de sistemas trabajan para reducir perdidas futuras. Por la incertidumbre sobre futuras pérdidas por riesgo, la seguridad perfecta, el cual implica *cero* pérdidas es indefinidamente caro. Por esta razón, los administradores de los sistemas de seguridad y riesgo se esfuerzan en optimizar la asignación de recursos minimizando el costo total de la seguridad en información de sistemas. Este proceso es comúnmente referenciado como la *administración del riesgo*. (Seymour Bosworth, Michel E. Kabay, 2001).

Los programas de estándares de sistemas de seguridad, guías y estrategias de implementación han sido, o están siendo desarrolladas por sectores públicos y privados en todo el mundo, estos esfuerzos están enfocados a dirigir muchos aspectos de la información en muchos niveles de detalle, el estándar BS7799 es uno de los estándares más completos en la actualidad relacionado con todos los aspectos de la seguridad en la información, (Ricardo Morales, Ricardo Pineda,2003).

1.2 Planteamiento del Problema

A continuación se describen los tipos de amenazas más importantes de acuerdo a (Gelurski, 2003):

Ataques de Denial of Service (Negación de Servicios)

Los ataques de Denial of Service fueron diseñados para parar una red empresarial o site de comercio electrónico inundando de gran cantidad de trafico, similar a millones de personas accesando un recurso repetidamente, inhabilitando el recurso, esto se genera mandando una gran cantidad de paquetes inservibles al sistema, (Gelurski, 2003).

Estadísticas de Denial of Service

Mas del 78% de los encuestados en la encuesta FBI/CSI (Richard Power,2003), reportaron ataques de Denial of Service.

Basado en un estudio conducido por el Nombre de Dominios Islándico, 25% de las páginas de web de las 1000 compañías "Fortune" son actualmente vulnerables a ataques de Denial of Service, (Gelurski 2003).

Los ataques de Denial of Services se han incrementado de 7.38% en el Q1-2002 a 13.24% en el Q3-2002, (Gelurski 2003)

Virus

Los Virus se replican solos en los sistemas de archivos. Para accionar una infección, el virus debe anexarse a un archivo que está siendo ejecutado. Por lo tanto depende de una intervención/interacción de un humano para que esto suceda. Una vez habilitado los virus se copian por si solos en archivos esenciales de sistema, haciéndolo difícil de eliminar. La mayoría de los virus residen en memoria y activamente intentan infectar otros programas. El objetivo del programador de virus es crear un daño en grán escala de propagación.
85% de los Virus se esparcen a través de correo electrónico (una escalación notoriamente significativa ya que anteriormente la única forma de esparcir los virus era a través de un disquete infectado), (Gelurski 2003)

	1996	*1997*	*1998*	*1999*	*2000*
Diskette	74%	88%	67%	39%	7%
Anexo e-mail	9%	26%	32%	56%	87%
Arch. Bajado	12%	18%	12%	13%	2%
Otro	15%	20%	11%	13%	4%

Tabla 1.2-1 Porcentajes de tipos de transmisión de virus informáticos

Worms(Gusanos)

Los Worms son programas de software que se propagan, por sí solos, a través de una red. A diferencia de los virus y trojanos, se ejecuta en un sistema sin intervención humana, y típicamente ejecuta una tarea en el que intenta encontrar otro sistema potencialmente vulnerable. Entra a un sistema explotando vulnerabilidades o características sobrepasadas en software que comúnmente corre en los sistemas, usando un acercamiento automatizado muy similar a esos efectuados por ataques humanos. Los Worms a menudo existen puramente en memoria, evitando el sistema de archivos y haciéndose invisible al software de antivirus que checa los sistemas de archivos, (Gelurski 2003).

Estadísticas de los Worms

Cuando surgió el ataque de Nimda* por el Internet el tráfico de paquetes se incremento de 1,500 a 60,000, dependiendo del segmento, de acuerdo a la revista Information Security Magazine (referenciado por Gelurski, 2003).

De acuerdo a la revista Information Security Magazine a pesar de que el 90% de las compañías que habían implementado algún sistema de seguridad, 88% aún reportaron infecciones de virus y worms durante el 2002,(referenciado por Gelurski, 2003).

Desde la liberación del Nimda* hace 9 meses, la actividad de este worm ha decrecido solo un 45%(Gelurski, 2003).

1.3 Estadísticas de Amenazas y Riesgos

(Higgins 2003) en el Reporte de Amenazas de Seguridad del Internet establece que los riesgos de Internet se han intensificado y evolucionado de muchas formas, excluyendo los worms y las amenazas combinadas, la medida de los volúmenes de ataques cibernéticos declinó ligeramente bajando un 6% del periodo semestral anterior a Feb 2003. A pesar de este decremento, muchas organizaciones, experimentaron un incremento agudo de volúmenes de ataques con relativa severidad en los ataques.

El volumen de los ataques por país nos demuestra que el 80% de los ataques fueron lanzados a través de sistemas localizados en solo 10 países* y México se encuentra en esta lista de países, lo cual nos demuestra que nos encontramos en un sitio de mucho riesgo a ataques directos.

(Higgins 2003) añade que a riesgos asociados con ataques cibernéticos, la taza de descubrimiento de vulnerabilidades de nuevos productos de TI se ha incrementado considerablemente en el último año. El número total de vulnerabilidades nuevas documentadas en 2002 fue 81.5% mayor que el 2001. Este incremento fue dirigido casi exclusivamente por vulnerabilidades calificadas como relativamente severas. Además, aproximadamente 60% de las vulnerabilidades documentadas eran fácilmente explotables ya sea por que herramientas sofisticadas eran fácilmente adquiridas en el Internet o por que no se requerían herramientas en lo absoluto para explotar esa vulnerabilidad, en un promedio de horas de liberación muchos de estas amenazas se esparcen rápidamente entre organizaciones conectadas al Internet, y en la actualidad algunas continúan infectando miles de sistemas a través del mundo.

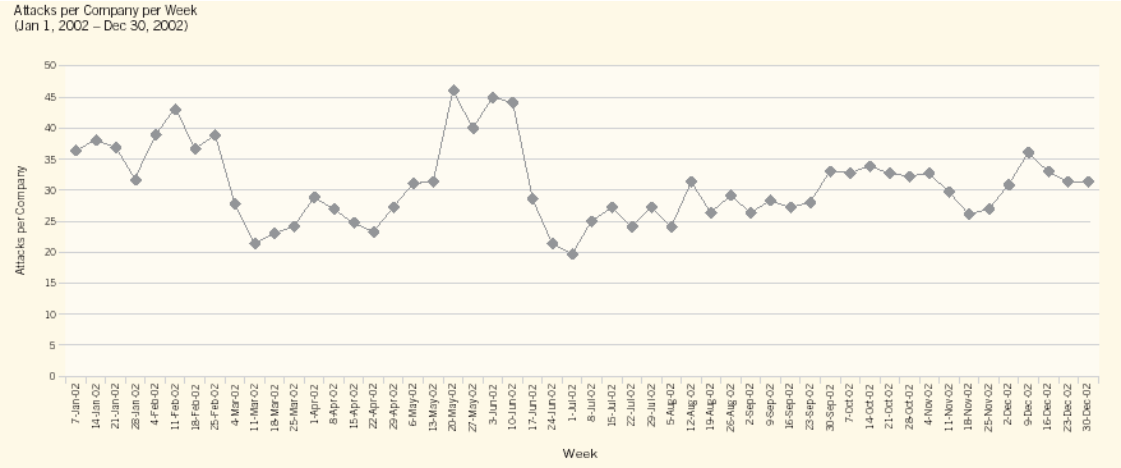
1.3.1 Tendencias de Amenazas

(Higgins, 2003), establece que para las compañías que no están haciendo uso de medidas en contra de los ataques, los riesgos se han incrementado considerablemente con el paso del tiempo, para establecer un análisis de esto podemos categorizar las tendencias en: Tendencias de

Ataque Cibernético, Tendencias de Vulnerabilidades, Tendencias de Código Malicioso, Tendencias de Abuso y Uso Indebido.

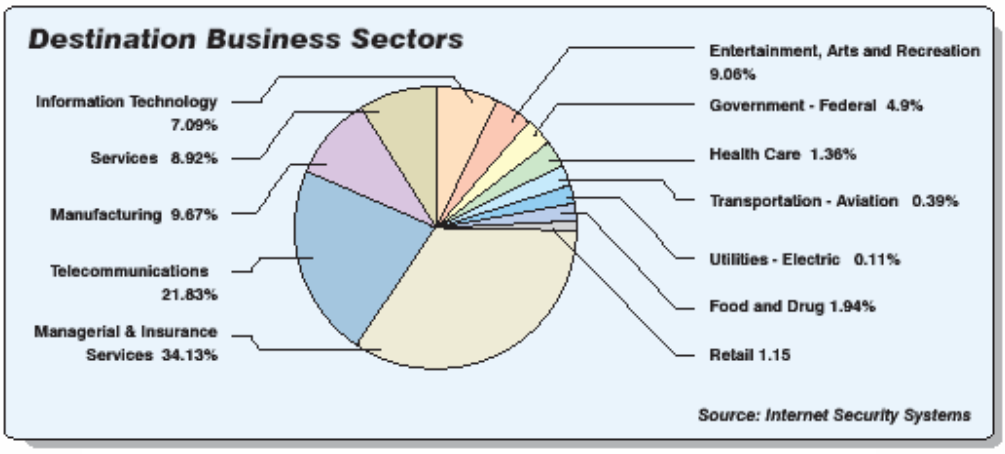
1.3.2 Tendencias de Ataque Cibernético

(Higgins, 2003), establece que en promedio, las compañías experimentaron 30 ataques por compañía por semana durante el último cuarto del 2002



Gráfica 1.3.2 -1: Ataques por Compañía por semana Fuente: Mark Higgins; Symantec Internet Security Threat Report; Feb 2003

En el Internet Risk Impact Summary White Paper elaborado por el ISS (2003), por sectores de la Industria podemos determinar que la industria de administración y aseguradores son los objetivos más comunes, le sigue telecomunicaciones y manufactura.



Gráfica 1.3.2 -2: Sectores de la Industria atacados Fuente: X-Force Global Threat Operations Center; Internet Security Systems

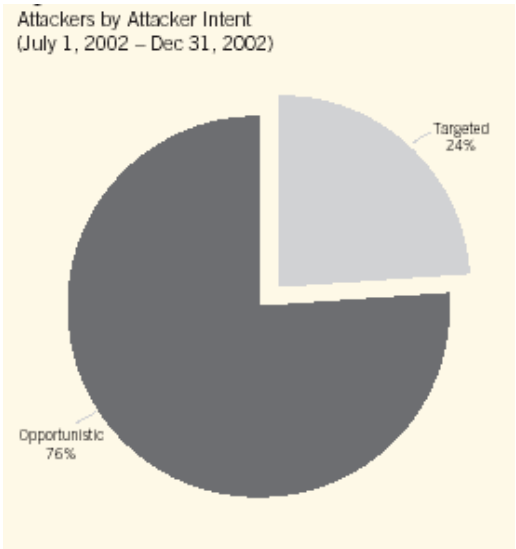
(Higgins 2003), establece que por país de origen de los ataques, los ataques del sur de corea se incrementaron por un 62%, estableciéndolo como la segunda fuente de más ataques entre los países posiblemente por el incremento en servicios de banda ancha de ese país, México se encuentra en octavo lugar.

Top Ten Attacking Countries per Internet Capita
(July 1, 2001 – Dec 31, 2002)

Ranking	Country	Attacks per 10,000 Internet users (July 1, 2001 – Dec 31, 2001)	Ranking in Period II (Jan 1, 2002 –Jun 30, 2002)	Ranking in Period I (July 1, 2001 – Dec 31, 2001)
1	South Korea	23.7	6	4
2	Poland	18.4	5	8
3	Czech Republic	14.2	11	NA
4	France	14.2	3	5
5	Taiwan	14.0	7	9
6	Hong Kong	13.9	2	2
7	Belgium	13.3	4	17
8	Mexico	11.8	13	14
9	China	10.8	10	11
10	Israel	10.1	1	1

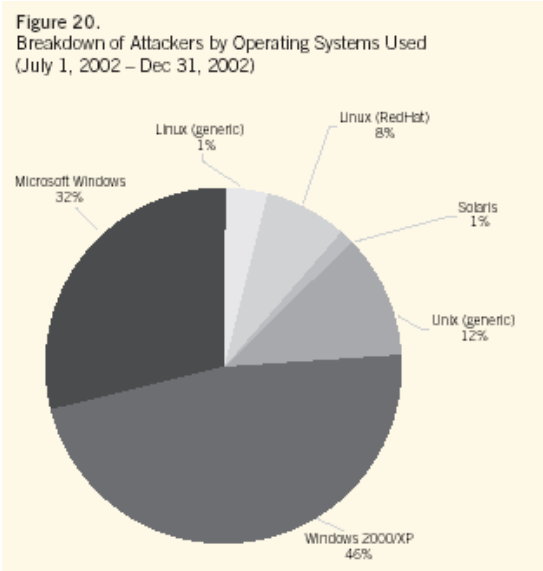
Gráfica 1.3.2 -3: 10 Países más atacados por Internet Capita: Fuente: Mark Higgins; Symantec Internet Security Threat Report; Feb 2003

(Higgins 2003), afirma que una de las preguntas más intrigantes es la de los intentos de ataque contra los ataques perpetrados, realmente un atacante tenía como objetivo una empresa o solamente estaba haciendo un escaneo en el Internet en busca de una oportunidad para explotar sistemas vulnerables. De todos los intentos de ataques perpetrados el 24% de éstos realmente fueron realizados.



Gráfica 1.3.2 -4: Atacantes por tipo de ataque: Fuente: Mark Higgins; Symantec Internet Security Threat Report; Feb 2003

(Higgins, 2003), establece que por sistema operativo usado para un ataque, tenemos que el Windows 2000/XP es el más usado, seguido por las demás plataformas Windows, Unix (Genérico) y Linux (RedHat) respectivamente.

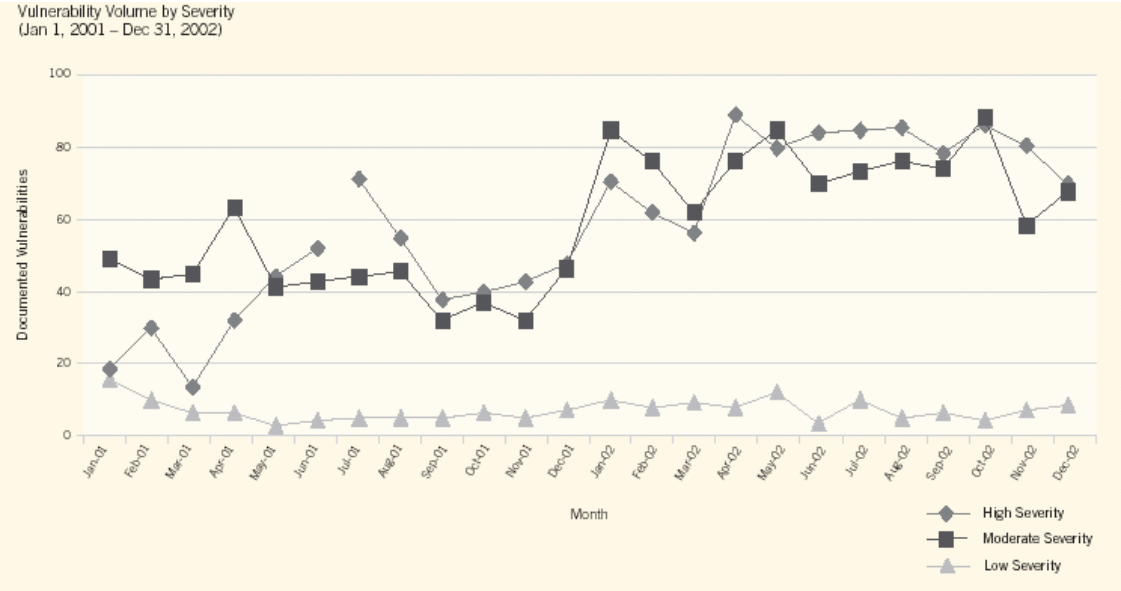


Gráfica 1.3.2 -5: Irrupciones de atacantes por sistema operativo: Fuente: Mark Higgins; Symantec Internet Security Threat Report; Feb 2003

1.3.3 Tendencias de Vulnerabilidades

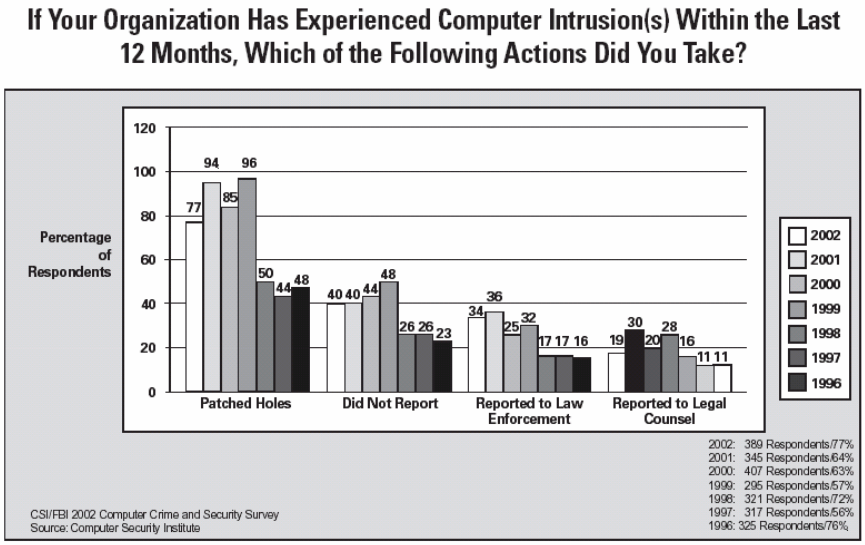
De acuerdo con (Higgins 2003) se documentaron 2,524 nuevas vulnerabilidades en el 2002, el cual elevó el porcentaje de vulnerabilidades anuales a 81.5% sobre el 2001. En promedio se generaron aproximadamente 7 vulnerabilidades por día, esto se puede deber a que existen diferentes herramientas y metodologías para explotar las vulnerabilidades y el aumento de la cobertura en los medios sobre vulnerabilidades.

Higgins afirma que el descubrimiento una nueva vulnerabilidad puede dejar los sistemas seguros en un momento, expuestos a ataques en el momento siguiente, con múltiples vulnerabilidades emergiendo diariamente, la efectividad relativa de una postura de seguridad en una organización es un constante estado de flujo.



Gráfica 1.3.3 -1:Volumen de vulnerabilidad por severidad: Fuente: Mark Higgins; Symantec Internet Security Threat Report; Feb 2003

(Power, 2003), establece en los resultados de su encuesta de crimen de computación y seguridad que el resultado de la mayoría de los ataques e intrusiones efectuadas en los últimos años se debe a parches de hoyos de seguridad y vulnerabilidades en su infraestructura de tecnología, lo cual establece que un origen importante de intrusiones se debe a este punto.



Gráfica 1.3.3 -2: Encuesta de Ataques a empresas: Fuente: Richard Power; Computer Crime and Security Survey

1.3.4 Tendencias de Código Malicioso

Según (Higgins, 2003), los ataques combinados representan el mayor riesgo en la comunidad del Internet, estos ataques representan el 80% de los ataques reportados en el segundo semestre del 2002, el código malicioso que roba información confidencial de los usuarios se ha incrementado substancialmente sobre el año pasado.

1.3.5 Tendencias de Abuso y Uso Indebido

(Higgins, 2003) afirma que más del 50% de los incidentes de seguridad reportados envuelven abuso o mal uso de los recursos por los empleados de la compañía. Adicionalmente, tal vez el aspecto más alarmante de estos incidentes es el hecho de la relativa facilidad con la que estos incidentes se efectuaron, la mayoría de los atacantes internos no tuvieron que "hackear" el sistema en términos de seguridad, la autorización de los recursos ya estaba dada como empleados.

1.4 Seguridad en las Tecnologías de Información

Junto con la evolución, nuevos desafíos en áreas de seguridad en la computación, administración del riesgo y continuidad del negocio han surgido. Mientras el Internet ha abierto un nuevo mundo de negocios, también ha introducido usuarios individuales y corporaciones al espectro siempre-creciente de riesgos incluyendo worms, virus, ataques de negación de servicios, abusos de empleados, robo e inclusive espionaje industrial; cada uno capaz de infligir millones de dólares en daños a corporaciones y lisiar la capacidad de competir de las compañías (Gelurski, 2003).

Las organizaciones que operan en la economía "en–linea" actual, afrontan una nueva misión, mantener el tiempo de operación mientras protegen la integridad y privacidad de la información almacenada en servidores, PCs, información almacenada y en tránsito. Ya sea secretos de comercio propietario, bases de datos de clientes, cadenas de proveedores en-línea, números de tarjetas de crédito, o interrupciones frecuentes de clientes, pérdidas financieras, obligaciones legales, y en mayor contexto, disminuir la habilidad de servir a los clientes y permanecer competitivos en el mercado(Gelurski, 2003).

1.5 Objetivo

Proponer un esquema integral de seguridad en las tecnologías de información, basado en el estándar Británico BS7799 enfocado a una empresa de manufactura.

CAPITULO 2

2. Marco Teórico

2.1 La Importancia de la Administración del Riesgo

(Debra S. Herrman, 2002) establece que la administración del riesgo es el proceso que permite a los administradores de Tecnologías de Información balancear los costos operacionales y económicos de medidas de seguridad para proteger los sistemas de Tecnologías de Información e información que soporta la misión de la empresa, este proceso no es único al ambiente de las tecnologías de información. Para que un proceso de administración de riesgo sea eficiente, es necesario que cubra todas las áreas de la empresa con procesos críticos y vitales para el buen funcionamiento de éste incluyendo activos de información y procesos operativos.

2.2 La importancia de Las políticas de Seguridad

(Goodhell y Meyers) establecen que en la computación y el ambiente de red de una organización son comúnmente los elementos que dibujan la línea entre el éxito y fracaso de una empresa. La confianza en las computadoras y el internet en nuestro trabajo diario requieren consideraciones de seguridad en diversas áreas. La seguridad de la red, servidores, equipos de escritorio es compleja pero no es el único factor que trae seguridad a la empresa. El trabajo hecho para apuntalar la seguridad de la red y los sistemas de cómputo pueden caer en la inutilidad si los usuarios no trabajan de una manera segura. Puede también generarse un esfuerzo inútil si la administración no lo mantiene. La seguridad también decrece si no se adapta al cambiante ambiente de trabajo. La seguridad es responsabilidad de cada persona dentro de la organización. Todas las administraciones de cómputo, usuarios e inclusive esos empleados que no usan equipo de cómputo en su práctica diaria comparten la responsabilidad global de la seguridad en la compañía.

2.3 Estándar BS7799

(Lillywhite 1999), comenta que en esta era comercial altamente competitiva, los ejecutivos de los negocios siempre enlistan la información como uno de los elementos más vitales de una estrategia corporativa exitosa. Desafortunadamente, mientras preocupa la importancia de las organizaciones comerciales, la información es también sujeta a una gran cantidad de riesgos. En años recientes, un número de medidas efectivas se han identificado y adoptado por algunas organizaciones comerciales y en 1993, el Departamento de Comercio e

Industria del Reino Unido junto con socios industriales, propusieron el código de práctica que se destinaría a la Administración de la Seguridad en la Información. Este código llamado BS7799, en 1995 terminó siendo el estándar de seguridad para las empresas ahora obteniendo la certificación por el British Standard International.

Objetivos Principales del BS7799
Proveer una base común para que las compañías desarrollen, implementen y midan sus prácticas de administración de seguridad.
Proveer confianza entre las compañías.

Componentes Principales del BS7799
Los componentes principales del estándar BS7799 son los siguientes:

Confidencialidad – Asegura que los activos de información sean accesados sólo por usuarios autorizados.

Integridad – Significa que los activos pueden ser modificados solo por personal autorizado o de formas autorizadas. En este contexto, la modificación incluye escritura, cambio de estatus, borrado, creado.

Disponibilidad – Establece que los activos sean accesados sólo por usuarios autorizados en el tiempo apropiado, en otras palabras, si el usuario tiene acceso legítimo a los recursos de información, este acceso no deberá ser interrumpido

La información de la compañía incluye toda la información existente no importa su formato, o a que tipo de negocio de la compañía esta relacionada. Los formatos mas comunes en los que se maneja la información son los siguientes: Texto, imágenes, sonido, conocimiento, cintas magnéticas, microfilmes, discos ópticos, fotografías, transparencias, etc.

Beneficios de la Integración del Estándar BS7799
Los beneficios más importantes de implementar un esquema de seguridad basado en el estándar BS7799 son los siguientes:

- Permite que la seguridad en la información sea administrada de manera comprensiva, realista y práctica.
- Establece una confianza mutua entre sitios enlazados y socios de negocios.
- Reafirma el aseguramiento de calidad
- Demuestra altos estándares de seguridad a clientes prospectos y actuales.
- Incrementa la capacidad de sobrevivir a un desastre.
- Asegura el cumplimiento de los requerimientos legales.

La seguridad de la información es lograda implementando un conjunto de controles que pueden ser políticas, prácticas, procedimientos, estructuras organizacionales. Estos controles necesitan establecerse para asegurar que los objetivos específicos de seguridad de la organización sean cumplidos.

CAPITULO 3

3. Método

El desarrollo del modelo de seguridad se compone de 3 fases:

Fase Estratégica:
El objetivo de esta fase es de definir el esquema de seguridad corporativo de la empresa y establecer el compromiso de los altos mandos corporativos.

Fase de Desarrollo:
El objetivo de esta fase es diseñar y desarrollar los controles de seguridad en la información que fueron definidos en la fase estratégica, establecer las normas y políticas que fundamentarán los lineamientos de los procesos y tecnologías requeridas para la aplicación del esquema de seguridad.

Fase de Implementación:
El objetivo de esta fase es el integrar el esquema de seguridad implementando las políticas y los procesos de seguridad de la información definidos en la fase de desarrollo, en esta tesis se mencionarán los aspectos clave para la correcta implementación de este esquema, está fuera del alcance de esta tesis desarrollar ampliamente la fase de implementación.

Una organización que use el BS7799 como su base de seguridad, se puede registrar en el BSI (British Estándar International) para obtener una certificación y demostrar a los inversionistas que se cumplen con los requerimientos de éste estándar, con el objetivo de generar certidumbre y confianza de que su inversión tiene una correcta administración de seguridad en las tecnologías de información.

3.1 Tipo de Investigación

Dado a que analizaremos un esquema de seguridad basado en el BS7799 que ha sido poco desarrollado en México, esta investigación será de tipo exploratoria, el cual Hernández Fernández y Baptista (2003) define como los estudios que se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes.

Este estudio se enfocará a establecer un modelo integral de seguridad sobre la base del estándar BS7799 que, este modelo protegerá los recursos de la compañía y administrará el riesgo de las empresas tomando en cuenta los esquemas de confiabilidad, seguridad y disponibilidad.

3.2 Población

El desarrollo de un esquema de seguridad en tecnologías de información debe ser integrado por un área específicamente dedicada a la seguridad de la información, este departamento idealmente debe de encontrarse en un nivel directivo y no dependiente del área de sistemas, sin embargo esta compañía no cuenta con un departamento específico para este rubro por lo que el área de sistemas será la encargada de implementar el esquema de seguridad contando con el apoyo directivo para esta implementación, por lo que la población estará enfocada al personal tanto directivo como al encargado de tecnologías de información.

3.3 Variables

Las variables a monitorear son las siguientes:

- Nivel de confiabilidad de la empresa.
- Nivel de Conocimientos de Seguridad de las TI de empresa.
- Tipos de esquemas de seguridad implementados en la empresa.
- Nivel de disponibilidad de la empresa en términos de operación constante al año.
- Tipos de Políticas y procedimientos de seguridad en la empresa.

3.4 Recolección de Información

Investigación: Se realizará una investigación bibliográfica en artículos actuales y libros referentes al tema de estudio. Esta investigación deberá abarcar los tópicos expuestos en la situación problemática para obtener un marco de referencia en el cual basar el análisis propuesto.

Encuestas: Uno de los aspectos más importantes para que un esquema de seguridad sea exitosamente implementado, es la aceptación y compromiso del personal que se verá afectado por ello, por lo que se considera importante analizar diferentes aspectos relacionados con esto como la percepción de la seguridad del personal en los diferentes niveles organizacionales, el valor que les puede dar el integrar un esquema de seguridad para su trabajo, el impacto que consideran tendrá en sus procesos, etc.

Entrevistas: Se realizarán entrevistas al personal de tecnologías de información para recopilar información sobre sus procesos, activos de información, niveles de impacto en caso de falla en sistemas etc.

Observación: Se observará el desarrollo del modelo de seguridad, su implementación y el comportamiento del personal de sistemas en relación con la implementación del modelo de seguridad.

CAPITULO 4

4. Modelo de seguridad basado en el estándar BS7799

4.1 Principios del Modelo de Análisis de Seguridad

La administración del riesgo es el proceso de identificar y analizar los riesgos de las Funciones ó los Procesos de la empresa, determinando la exposición de esa Función ó Proceso y pro activamente implementar controles que disminuyan el nivel de exposición y minimicen el riesgo. El objetivo de la administración del riesgo es asegurarse que el negoció o la organización asuma el correcto nivel de riesgo, ya que no todos los riesgos pueden ser totalmente eliminados o controlados

Un efectivo modelo de seguridad debe estar basado en los siguientes principios:

Orientado al Negocio – No orientado a la tecnología, la seguridad de la información debe ser orientada al negocio cubriendo todos los procesos y funciones que involucren flujo de información, tomando en cuenta los objetivos primordiales de la empresa con el fin de que las políticas y normas de seguridad vayan alineadas a estos objetivos.

Valuación del Riesgo – La valuación del riesgo de la seguridad de la información debe ser efectiva, objetiva y de costo razonable.

Los Activos de Información – Son principalmente propiedad de las áreas funcionales y es su responsabilidad protegerlas.

La Seguridad de la Información – Debe tener representación de todas las áreas organizacionales y debe ser considerada como un proceso integral de estas.

La Seguridad de la Información – Debe responder y ajustarse rápidamente a los cambios humanos, tecnológicos y de negocios.

Por que Administrar los Riesgos

La correcta administración de los riesgos llevará a la empresa a valorar y controlar y adecuadamente cualquier riesgo que sus activos de información estén expuestos, ningún esquema o modelo de seguridad es panacea de la seguridad y los riesgos, lo adecuado es administrar eficientemente esos riesgos para generar políticas y normas de mitigación y control de riesgos.

Las políticas, estándares y procedimientos para la seguridad de la Información son una serie de múltiples documentos que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones.

Las normas son documentos que establecen las bases de un determinado procedimiento, son los requerimientos que necesitan los procedimientos, estos están sustentados en los controles del BS7799.

4.2 Alcance del Proyecto

Para establecer un correcto modelo de seguridad, es necesario abarcar por completo todas las diferentes áreas de la empresa en donde intervienen sistemas de información, con el objetivo de poder analizar el esquema de seguridad de manera eficiente, este proyecto de tesis se enfocará a establecer y determinar el esquema de seguridad en el activo de información que más impacte a la empresa de manufactura que estamos analizando, y con esto se identificarán los requerimientos necesarios para establecer un correcto modelo de seguridad y partir de ahí para establecer un modelo de seguridad.

Como se menciona anteriormente no todos los modelos de seguridad son iguales, ya que dependiendo de los objetivos del negocio, algunos factores influirán más que otros, por eso se determina que el modelo de seguridad a analizar será enfocado a la empresa de manufactura, inclusive dentro de las mismas empresas de manufactura, los cambios entre una y otra pueden ser significativos, este documento establecerá una base para determinar el proceso de desarrollo de un modelo de seguridad en una empresa de manufactura y la importancia de basarlo en un estándar de seguridad, aún así cada caso deberá ser analizado individualmente

Por razones de confidencialidad la empresa de manufactura en la que se establecerá el modelo de seguridad la llamaremos Versa como empresa ficticia pero estará basada en un caso real.

Adicionalmente a esto, se establecerá el análisis de seguridad hasta el plan de acción que es el fundamento para la implementación de los controles normativos y controles técnicos, dado a que el objetivo principal de este proyecto es analizar el esquema de seguridad no implementar una solución en su totalidad, este documento pretende establecer los fundamentos y bases para una correcta implementación de un esquema de seguridad en las Tecnologías de Información, el modelo propuesto está

enfocado a establecer una base para un correcto modelo de seguridad y no describirlo con alto nivel de detalle.

4.3 Proceso de Análisis de Riesgo - Fase Estratégica

Para poder analizar los riesgos de los activos de información de una empresa, es necesario conocer los componentes principales de ésta, como sus procesos, activos de información, reglas de negocio, todo lo que ayude a identificar la estructura, procesos y objetivos del negocio. Esto nos permitirá poder clasificar los activos de información y valorar adecuadamente cada uno de ellos, la regla básica es empezar por el activo de información más crítico para la empresa y de ahí partir para hacer el análisis de riesgo hasta completar todos los activos de información de la empresa. Cuanta mayor información tengamos de la empresa más correctamente podremos evaluar sus activos de información.

La fase estratégica pretende recopilar la información relacionada con los activos de información más críticos, además de proveer información para la fase de desarrollo es necesario estructurar la documentación adecuada de estos activos.

Para contar con un adecuado proceso de análisis de riesgo es necesario contar con los siguientes elementos.

Reglas de Negocio
Describe como opera la compañía a evaluar, esto con el fin de identificar por niveles de criticidad cada proceso para poder ser evaluado de manera apropiada cada uno de ellos, identificando el recurso más crítico de Tecnologías de Información basado en términos de disponibilidad, integridad y confidencialidad y partiendo de esto para su análisis, en este caso nos enfocaremos al proceso de información más crítico de la compañía.

Flujos de Información
Habiendo determinado el activo más crítico, se procederá a establecer los flujos de información de ese activo en particular con el objetivo de entender mejor cómo interactúa el proceso con los distintos activos de información

Inventario de Activos
Permite identificar los activos en los que se encuentra estos recursos de información describiendo sus características principales.

Identificación y clasificación de información, Usuarios de Información

Se obtendrá información de los dueños de los componentes más críticos de información y obtener una clasificación de ésta, describiendo las diferentes categorías para conocer si la información puede ser restringida, abierta, de escritura o lectura, etc, también poder determinar que uso se le da a esta información, también relacionar que usuarios acceden a estos recursos de información.

Análisis de Impacto

Es necesario determinar el impacto adverso resultado de una amenaza satisfactoria derivada de una vulnerabilidad. Un análisis de impacto del negocio prioritiza en niveles de impacto asociados con la divulgación de la información crítica de una empresa basado en la valoración cualitativa y cuantitativa de la sensibilidad y criticidad de los activos de información. Esto generalmente es en términos de impacto financiero.

4.3.1 Reglas de Negocio de Versa

La empresa Versa, soporta sus operaciones con la mas alta tecnología para la manufactura de polímeros, esta empresa cuenta con sistemas de automatización, control, análisis de producción, manufactura y empaque de sus productos, los sistemas de información son un activo de alto valor para la producción, en el mercado en el que se encuentran, existen solo dos tipos de calidad en sus productos, primera y desperdicio, con este alto grado de nivel de calidad es necesario analizar, monitorear y coordinar todo lo relacionado con el proceso para poder generar ese nivel óptimo de producción.

Por estar automatizados en sus procesos de más de un 90% es de gran importancia establecer un modelo de seguridad en Tecnologías de Información basado en el estándar BS7799 en la compañía Versa con esto tendrán una administración de riesgos efectiva, y reducir al máximo cualquier riesgo de seguridad que implique un paro en sus operaciones que derivarán de pérdidas importantes o hasta el cierre total de la compañía.

La compañía tiene una operación en su área de producción continua 7 x 24, con un alto grado de disponibilidad y con metas de producción de un porcentaje no mayor al 12% de desperdicio. Por esto es necesario establecer cual de todos los activos de información es el que causa más impacto en su producción, y con esto establecer el modelo de análisis de riesgo de este activo de información.

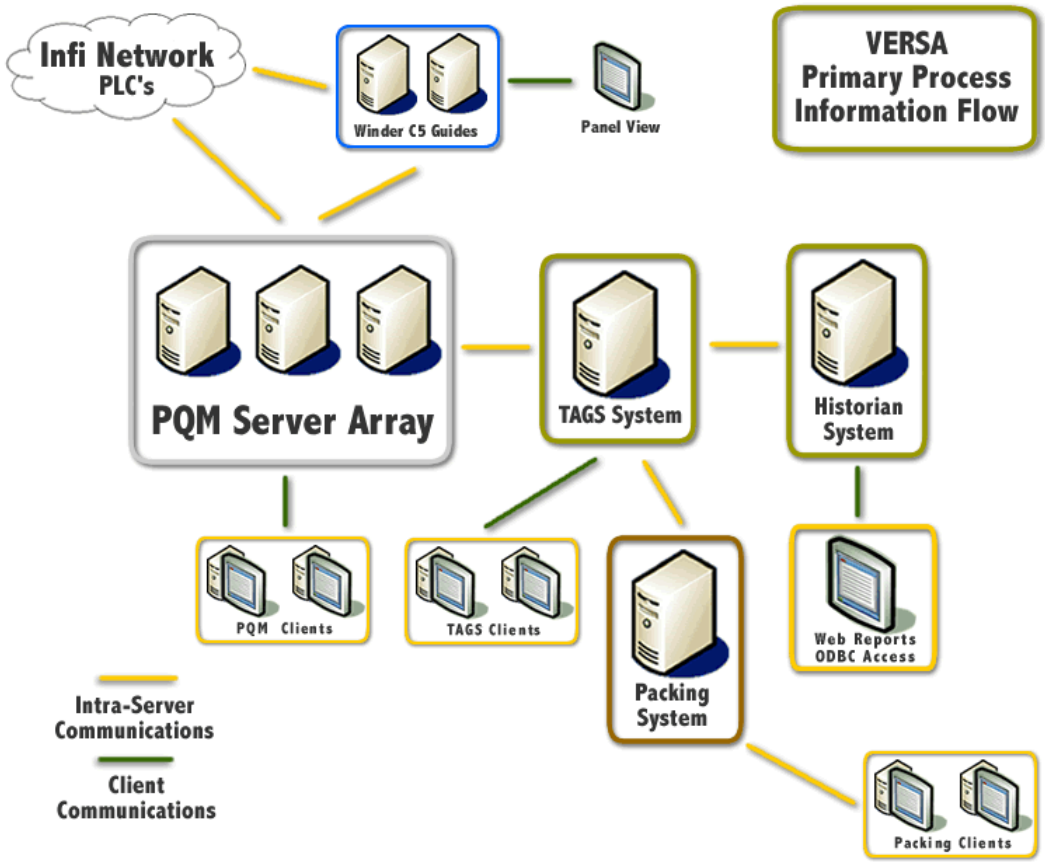
Identificación de Recursos Críticos de Tecnologías de Información

Por el análisis de la estructura de operación podemos establecer que la principal prioridad de la empresa se encuentra en términos de la Disponibilidad de la infraestructura de tecnología en base a la Disponibilidad, Integridad, Confidencialidad de las TI ya que sin esta la producción de la planta se ve degradada en su totalidad.

Para tener un mejor entendimiento de esto, es necesario analizar los flujos de información general describiendo cada uno de los activos que intervienen en todo el proceso, y poder analizar de manera adecuada todo el sistema entendiendo los puntos claves y más críticos de todo el sistema.

4.3.2 Flujos de Información General

A continuación se muestra la descripción del flujo de información que interactúa con el sistema PQM:



Gráfica 4.3.2-1: Versa Primary Process Information Flow

Red INFI PLC's

Todos los elementos que conforman la producción se encuentran monitoreados por elementos electrónicos llamados PLC's, estos elementos recaban información referente a presiones, temperaturas, funcionamiento de motores, calderas, etc, aquí es de donde se genera toda la información que permite determinar el estado de cada elemento crítico del proceso con el fin de determinar si el producto cuenta con las características adecuadas.

Sistema de Calidad PQM

La planta cuenta con dos sistemas de calidad, el sistema PQM Product Quality Management e IP21 de Aspentech, estos sistemas interactúan con la red de PLC's para recopilar información y monitorear los diferentes niveles del proceso, estos niveles cuando están dentro de los rangos especificados por los ingenieros de proceso, generan producto de calidad A, cualquier nivel fuera de rango manda el producto a clase F, desperdicio, si no se tienen datos sobre estos niveles, automáticamente el producto es calidad F.

Sistema de Seguimiento y Grado de Calidad TAGS

El sistema SSGC, es el que se encarga de procesar todas las reglas de negocio de la planta, en el se tiene información de todas las reglas de negocio y movimientos que involucran el proceso como segregaciones por fueras de estándar, tipos de producto, niveles de peso y dimensiones de las bobinas de hilo, etc, además de mantener y generar las etiquetas para la correcta identificación de cada tubo y bulk pack(caja con varios tubos o hilos producidos).

Sistema de Almacenamiento/Empacado

En el área de almacenamiento y empaque se cuenta con un sistema automatizado de empacado de bobinas Alemán Autefa GmBH. en todas las áreas de producción, este sistema cuenta con robots para transportación, almacenamiento, empaque en caja, peso y emplayado de las bobinas, todo este sistema esta soportado por una infraestructura de TI basada en Oracle con Windows NT Server junto con aplicaciones desarrolladas en lenguaje C++.

En caso de desastre se cuenta con un área limitada de empacado y pesado/emplayado, esta área puede mantener un promedio de producción de 8 horas, no existe un sistema de almacenamiento manual por lo que se tiene solamente un área de empacado temporal en el que puede almacenar este tiempo limitado de producción.

Sistema de Historial de Producción

En este sistema se encuentra recopilada el historial de producción de la planta, en el se puede sacar análisis de producción de meses atrás y ver las tendencias de producción de la planta, este sistema es necesario para el análisis y estadísticas de producción.

4.3.3 Matriz de Activos Críticos

Para poder determinar el grado de impacto de cada uno de los activos se genera una matriz de activos críticos, debido a que la falta de disponibilidad de algún activo de información derivará en pérdidas considerables dado a que la producción será desperdicio, basándonos en esto, la matriz de activos críticos analizará el impacto en caso de no contar con la disponibilidad de cada uno de ellos, evaluándolo en términos cronológicos, al determinar el tiempo permitido de paro al año, podemos darnos cuenta de la criticidad de cada uno de los sistemas.

A continuación se enlistan los sistemas más críticos de la empresa:

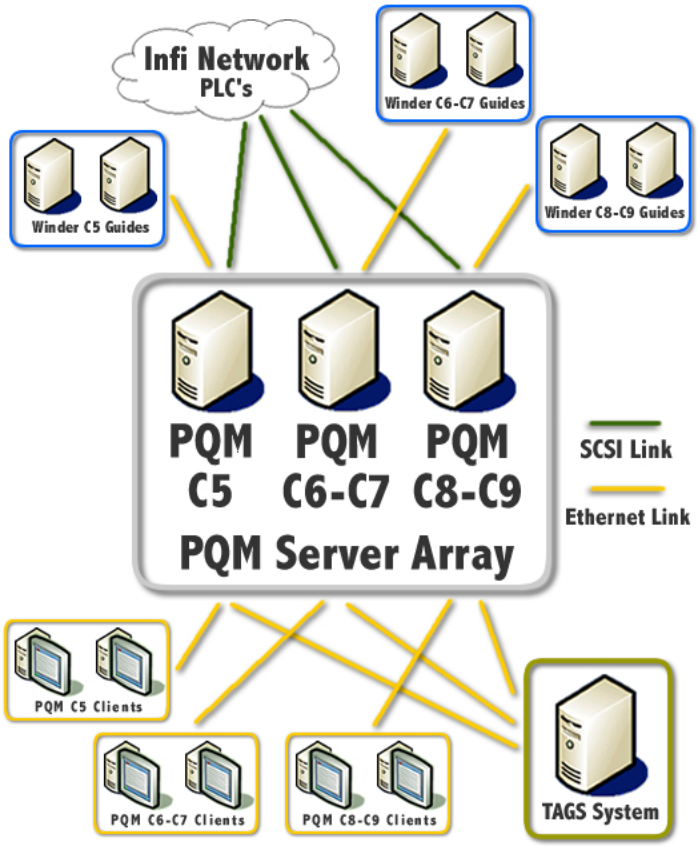
Recurso	Impacto en caso de Paro	Tiempo permitido de Paro/Año
Servidor de Dominio	Usuarios no se pueden autenticación al sistema de TAGS, y acceder archivos.	12 Hrs.
Servidores PQM	**No se pueden establecer los grados de producción impactando el grado producido degradándolo a desperdicio.**	**8 Hrs.**
Servidor Product Historian	No se puede analizar las estadísticas de producción.	5 Días
Sistema TAGS	No se puede modificar cambios en la producción como segregaciones, no se puede empacar por la interacción con SAP	24 Hrs.
Infraestructura de Red en Producción	No funcionaría el sistema de TAGS, PQM continuaría funcionando.	24 hrs.

Tabla 4.3.3-1: Matriz de Activos Críticos Basado en Disponibilidad de los Activos

Por todo esto, podemos establecer que el activo de información más importante es el sistema **PQM** ya que este establece la calidad del producto para ser vendido, sin éste, el producto estará determinado como desperdicio en su totalidad, por esta razón el activo que analizaremos como base será este.

4.3.4 Gráfica de Flujos de Información del Sistema PQM

A continuación se presenta la gráfica de flujos de información que entran y salen del arreglo de servidores PQM, en este se enlista tanto la información que fluye por ethernet como la que se transmite a través de un cable SCSI conectado a los PLC's de Bailey.



Gráfica 4.3.4-1: Gráfica de Flujos de Información del Activo PQM

4.3.5 Inventario de Activos

(Stoneburner, Goguen, Ferniga, 2001) establecen que en la evaluación de riesgos de un sistema de tecnología de información, el primer paso es establecer el alcance del esfuerzo. En este paso, se establecen las fronteras del sistema de Tecnología de información, junto con los recursos y la información que constituyen el sistema. A continuación se citan la lista de inventarios activos del sistema evaluado como de mayor impacto al negocio.

PQM Server Array	*Descripción*	*Características Principales*
PQM 90	**Servidor para Planta C5**	**Establece los grados de producción**
Hardware	Servidor Compaq PROLIANT 5500	2 procesadores Pentium III 400Mhz
Sistema Operativo	Windows NT Server 4.0	Service Pack 6a
Middleware	Microsoft Message Queue V1.0	Intercambio de mensajes de datos entre servidores
Aplicaciones	ABB Tenore NT Versión 1.1	Service Pack 5
PQM 200 C6-C7	**Servidor para Planta C5**	**Establece los grados de producción**
Hardware	Servidor Compaq PROLIANT 5500	2 procesadores Pentium III 400Mhz, 1 GB RAM, 100GB RAID 5 Storage
Sistema Operativo	Windows NT Server 4.0	Service Pack 6a
Middleware	Microsoft Message Queue V1.0	Intercambio de mensajes de datos entre servidores
Aplicaciones	ABB Tenore NT Versión 1.1	Service Pack 5
PQM 2000 C8-C9	**Servidor para Planta C6-C7**	**Establece los grados de producción**
Hardware	Servidor Compaq PROLIANT 570	2 procesadores Pentium III XEON 700Mhz, 1GB RAM, 100GB RAID5 Storage
Sistema Operativo	Windows NT Server 4.0	Service Pack 6a
Middleware	Microsoft Message Queue V1.0	Intercambio de mensajes de datos entre servidores
Aplicaciones	ABB Tenore NT Versión 1.1	Service Pack 5

Tabla 4.3.5-1 Matriz de Inventario de Activos Sistema PQM

Es necesario contar con esta matriz ya que nos servirá para tener documentado todos los activos en donde está sustentado el sistema PQM y poder determinar cuales son las características de cada uno de ellos para su posterior análisis.

4.3.6 Activos de Información, Identificación y Clasificación de Información, y Usuarios de la Información

En esta parte será necesario generar una matriz de todos los activos que intervienen en la aplicación, sus características de hardware, que uso se le da a ese activo, para que se utiliza, que tipo de restricción tiene la información que maneja, que usuarios y permisos utilizan este activo y que impacto generaría la no disponibilidad del activo de información, esto nos dará una perspectiva más clara de cada uno de los activos que involucran a cada uno de los sistemas.

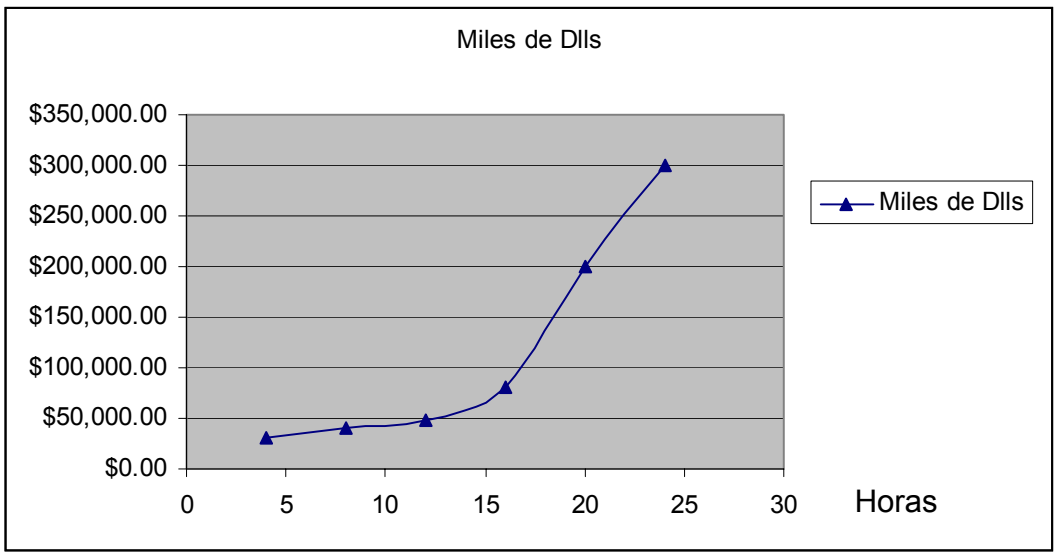
Activo	*Descripción*	*Uso*	*Identificación de la información*	*Clasificación de la información*	*Usuarios*	*Permisos*	*Impacto en caso de Paro*
PQM 90 C5	Servidor Compaq Proliant 5500 PII/Xeon 400 dual, 1GB RAM, 100GB Storage	Sistema de Calidad de producto en base a grados de producción de planta C5	-Establecimiento de grados de calidad en base a valores de producción -Degradaciones automáticas por fueras de rango en valores de producción.	-Restringida -Restringida	-Ing. de Proceso -Operadores	-Escritura -Lectura	No se pueden establecer los grados de producción impactando el grado producido a desperdicio
PQM 2000 C6-C7	Servidor Compaq Proliant 5500 PII/Xeon 400 dual, 1GB RAM, 100GB Storage	Sistema de Calidad de producto en base a grados de producción de planta C5	-Establecimiento de grados de calidad en base a valores de producción -Degradaciones automáticas por fueras de rango en valores de producción.	-Restringida -Restringida	-Ing. de Proceso -Operadores	-Escritura -Lectura	No se pueden establecer los grados de producción impactando el grado producido a desperdicio
PQM 2000 C8-C9	Servidor Compaq Proliant 5500 PII/Xeon 400 dual, 1GB RAM, 100GB Storage	Sistema de Calidad de producto en base a grados de producción de planta C5	-Establecimiento de grados de calidad en base a valores de producción -Degradaciones automáticas por fueras de rango en valores de producción.	-Restringida -Restringida	-Ing. de Proceso -Operadores	-Escritura -Lectura	No se pueden establecer los grados de producción impactando el grado producido a desperdicio

Tabla 4.3.6-1: 5.3.6 Activos de Información, Identificación y Clasificación de Información, y Usuarios de la Información

4.3.7 Análisis de Impacto

(Stoneburner, Goguen, Ferniga, 2001) establecen que es necesario determinar el impacto adverso resultado de una amenaza satisfactoria derivada de una vulnerabilidad. Un análisis de impacto del negocio prioritiza en niveles de impacto asociados con la divulgación de la información de una empresa basado en la valoración cualitativa y cuantitativa de la sensibilidad y criticidad de los activos de información como hardware, software, sistemas, servicios y activos relacionados con tecnología que soportan a la operación crítica de la empresa.

Se analizará el impacto financiero basándose en cifras estimadas de producción, total neto producido en un día $253,000 Dlls Clase A y $48,000 Dlls clase F. La gráfica describe la pérdida financiera en caso de que el sistema PQM esté abajo en un promedio de un día.



Gráfica 4.3.7-1: Gráfica de Análisis de Impacto en Pérdidas Monetarias

4.4 Proceso de Análisis de Riesgo - Fase Desarrollo

Una vez obtenido todos los datos de la empresa y habiendo evaluado cada uno de los activos, determinado el impacto en caso de una vulnerabilidad y habiendo identificado el activo de información más crítico para la empresa, procedemos a analizar este activo de información en términos de determinar las amenazas que pueden impactar a este activo, los riesgos potenciales que tiene este activo y los controles del BS 7799 que mitigan estos riesgos para finalmente establecer un plan de acción que determinará el desarrollo de la fase de implementación del modelo de seguridad.

4.4.1 Selección de Amenazas

(Stoneburner, Goguen, Ferniga, 2001) establecen que una amenaza es el potencial de una fuente de riesgo de ejercitar satisfactoriamente una vulnerabilidad en particular. Una vulnerabilidad es una debilidad que puede iniciarse accidentalmente o ser explotada intencionalmente.

Los activos están sujetos a muchos tipos de amenazas que derivan en daños a la empresa, estos daños pueden ocurrir de un ataque directo o indirecto a la información de la empresa como destrucción, acceso, modificación, corrompimiento, no disponibilidad o pérdida de la información, las amenazas se pueden originar de fuentes deliberadas o no intencionales, una amenaza necesitará explotar una vulnerabilidad del sistema, aplicación o servicio usado en la organización para causar daño a estos activos

El activo de información más crítico de la empresa Versa es el del sistema PQM a continuación se presentan las amenazas más relevantes que afectan directamente a este sistema, estas amenazas fueron las que se consideraron las más impactantes en este activo de información.

Amenaza	Descripción
3.6	Malicious Code
3.8.8	Denial of Services
3.5.6	Unauthorized Access to information
3.4.2	Unauthorized Changes

Tabla 4.4.1-1: Selección de Amenazas

4.4.2 Matriz de Riesgo

Valoración de Niveles de Riesgos

Para poder determinar una correcta evaluación de los riesgos de el activo de información a evaluar es necesario identificar una escala para esta valoración que sea adecuada a la metodología aplicada, esta escala puede establecerse en tres simples niveles, determinando su impacto en perdida financiera. Adicionalmente a esto tenemos la facilidad de Riesgo que es una descripción general del conjunto de elementos que se requieren para que este riesgo sea concretado.

Nivel de Riesgo	Impacto	Facilidad de Riesgo
ALTO	• Mayor de $300,000 Dlls	• Contiene prácticas administrativas claramente deficientes(configuraciones de fábrica, no firewall, no existe administración de políticas) • Contiene conocimiento no detallado de la configuración del sistema
MEDIO	• Entre $80,000 Dlls y $299,000 Dlls	• Contiene errores administrativos comunes (demasiados puertos abiertos, procesos con privilegios mayores de los que necesita, ciclos intermitentes de parcheo) • Depende de configuraciones de fábrica y estructuras conocidas para soportar el ataque • Soporta un ataque por script pero no una propagación automatizada
BAJO	• Entre $25,000 Dlls y $79,000 Dlls	• Efectivo cuando son aceptadas las mejores prácticas de seguridad(configuración de firewall, administración de las configuraciones, privilegios de cuentas, ciclos de parcheo continuos) • Contiene conocimientos específicos de opciones de configuración que no son de fábrica • Contiene multiples vulnerabilidades para ser activos y efectivos

Tabla 4.4.2-1: Valoración de Niveles de Riesgos

Amenazas y Riesgos del Sistema PQM

Una vez habiendo determinado los niveles de riesgo procedemos a relacionar las diferentes amenazas que se relacionan con este activo de información determinando el nivel de impacto y la facilidad de que ocurra este riesgo esto con el fin de poder valorar la pérdida financiera que ocurriría en caso de un desastre, con el nivel de impacto y la facilidad de riesgo se saca un promedio general y se determina el Nivel de Riesgo promedio general de cada una de las amenazas.

Amenazas y Riesgos del Sistema PQM					
No. Sec. Req	Descripción	Nivel de Impacto	Facilidad del Riesgo	Nivel de Riesgo	Descripción de la Amenaza
3.6	Malicious Code	Alto	Bajo	Medio	Partes de código que pueden ser ejecutados remotamente para propósitos destructivos
3.8.8	Denial of Services	Alto	Alto	Alto	Negación de servicios que conlleva a la caída de la aplicación
3.5.6	Unauthorized Access to Information	Alto	Bajo	Medio	Acceso no autorizado a los sistemas por cualquier medio

Tabla 4.4.2-2: Amenazas y Riesgos del Sistema PQM

Estos niveles de riesgo nos permitirán evaluar cada uno de los diferentes riesgos y su impacto en el activo analizado, se pondrá especial atención a los activos en donde el nivel de riesgo es elevado.

4.4.3 Análisis de Controles

Uno de los aspectos más importantes es el desarrollo de los controles del BS7799, estos establecen la relación de las amenazas con los controles del BS7799 que mitigan estas amenazas, en esta matriz se establecen los controles generales y luego los controles específicos, posterior a esto se desarrollará cada uno de los controles específicos para generar normas que establezcan las bases de las acciones que deben seguir para mitigar cada una de estas amenazas.

Num.	Amenaza	Num.	Controles Generales	Num.	Controles Específicos
3.5.6	Unauthorized access to information	7.3	General controls	7.3.2	Removal of Property
		9.5	Operating system access control	9.5.1	Automatic terminal identification
				9.5.3	User identification and authentication
				9.5.4	Password management system
				9.5.5	Use of system utilities
				9.5.7	Terminal time-out
		10.5	Security in development and support processes	10.5.1	Change control procedures
3.6	Malicious code	8.1	Operational Procedures and Responsibilities	8.1.4	Segregation of Duties
		8.3	Protection against malicious software	8.3.1	Controls against malicious software
		8.4	Housekeeping	8.4.1	Information back-up
				8.4.3	Operator Logs and Fault Logging
		9.7	Monitoring system access and use	9.7.3	Clock Synchronization
		10.5	Security in development and support processes	10.5.4	Covert channels and Trojan code
3.8.8	Denial of Services	8.5	Network management	8.5.1	Network controls
		11.1	Business Continuity Management	11.1.1	Business Continuity Management Process and Impact Analysis
				11.1.3	Writing and Implementing Continuity Plans
				11.1.4	Business Continuity Plan Framework
				11.1.5	Testing, Maintaining and Re-assessing Business Continuity Plans

Tabla 4.4.3-1 Matriz de Amenazas contra Controles BS7799

4.5 Análisis de Controles Específicos

Una vez teniendo la matriz de amenazas contra controles procedemos a desarrollar estos controles originados del BS7799, primeramente se hace una descripción del control según el BS7799, después los requerimientos en la empresa basados en ese control, después las normas que deben de implementarse basados en ese control y por último el diseño o desarrollo de ese control, que son las acciones que se deben de hacer para cumplir con las normas establecidas en cada uno de los controles.

BS7799: [7.3.2] Removal of Property

El equipo, información o software que pertenece a la organización no debe ser removido sin la autorización de la administración.
El tener la capacidad de poder remover el software sin una previa autorización puede derivar en la no-disponibilidad de la aplicación así como el hardware donde se ejecutan estas aplicaciones.

Requerimientos

Es necesario implementar controles de seguridad que impidan que tanto el hardware como el software no pueda ser removido, resguardando y restringiendo el acceso a personal no autorizado, se deberán generar políticas de utilización de software y asignar a el personal que puede tener la facultad de hacer algún cambio de equipo o aplicaciones especificando claramente las responsabilidades directas e indirectas de cada activo de información y físico.

Normas

- Se deberá contar con el inventario de hardware y software instalado.
- Se deberá contar con un documento que establezca las asignaciones de los responsables de los movimientos de hardware y software.
- Deberá existir una bitácora de movimientos de hardware y software detallando la fecha de movimiento, razón del movimiento, responsable.
- Se deberá contar con la autorización del encargado de Tecnologías de Información para cualquier movimiento de hardware o software.
- Se deberá contar con un proceso de autorización de cambios, salidas de equipos y dispositivos.

Diseño

- Deberá contarse con un procedimiento establecido para cualquier movimiento de equipo o actualización de hardware.
- Se deberá generar un checklist de actualización que establezca el cumplimiento de cada uno de los puntos necesarios para hacer dicha

actualización como avisos de baja de sistema, autorización del cambio por IT, por los responsables del sistema, por el área de operaciones.
- Se deberá llenar la bitácora de actualizaciones cada vez que se lleven a cabo registrando la duración de la baja de sistema.

BS7799: [9.5.1] Automatic Terminal Identification

La identificación automática de terminales deberá ser considerado para autentificar las conexiones a ubicaciones específicas, el acceso a los servicios de información deben utilizar un proceso de autentificación segura.

Requerimientos

Para validar la identidad del personal que acceda a los recursos de información es necesario implementar un proceso de autentificación segura, las terminales deberán tener este proceso de autentificación segura tanto por sistema operativo como algún tipo de autentificación por niveles o jerarquías dependiendo del grado de modificación o acceso a la información que se requiera.

Normas

- Deberá contar con controles de seguridad para la identificación automática de los usuarios
- Deberá contar con métodos de encrypción para el envío de los datos de autentificación para que la seguridad en esos datos no se vea comprometida

Diseño

- El sistema PQM está sustentado en la plataforma Windows NT que cuenta con recursos de autentificación automáticos, la aplicación PQM cuenta con un sistema de autentificación adicional dividido por niveles que permiten establecer el grado configuración y cambio de valores de la aplicación, esto asegura que el personal adecuado tenga los privilegios adecuados para el trabajo que desempeña.
- El sistema de identificación automática deberá ser implementado de manera adecuada para los diferentes roles que el personal desempeña para ejecutar sus funciones, estableciendo e identificando los diferentes roles que el personal ejercerá sobre la aplicación documentando todo esto de manera adecuada.

BS7799: [9.5.3] User Identification and Authentication

Todos los usuarios deben tener un identificador único para uso personal para que las actividades puedan ser identificadas al individuo

responsable. Una técnica de autentificación debe ser escogida para reconocer la identidad de cada usuario.

Requerimientos
Se debe contar con una política de acceso a los recursos que describa el uso de usuarios y contraseñas individuales para cada persona que accede los recursos de información.
Se deberá contar con políticas de cambio de passwords, longitud, y fortaleza.

Normas
- Se deberá generar un documento en el que especifique cada rol y responsables de la aplicación para establecer los niveles jerárquicos en los que puedan acceder cada usuario, este documento deberá estar autorizado por el gerente de la planta
- Es necesario establecer una política de cambio de passwords recurrente
- Se deberá establecer la longitud y fortaleza de las contraseñas.
- Se deberá generar un proceso que en el que en determinado tiempo establecido requiera que se cambie el password.

Diseño
- Se establecerán políticas de acceso tanto al sistema operativo como a la aplicación estableciendo los usuarios que requieren acceder y los niveles de acceso requeridos para escritura, lectura, configuración, sistema, etc.
- Utilizar la autentificación de Windows NT para asegurar la identidad de los usuarios que utilizan el sistema y establecer niveles jerárquicos a los usuarios a nivel sistema operativo.
- Utilizar la autentificación del sistema PQM para asegurar la identidad de los usuarios que utilizan el sistema y además poder tener la capacidad de establecer niveles jerárquicos a nivel aplicación controlado por contraseñas para poder identificar a los usuarios que requieren un nivel de configuración más profundo de los que requieren sólo ver los datos y no modificarle a la configuración de la aplicación.

BS7799: [9.5.4] Password Management System
Los sistemas de administración de passwords deberán proveer un recurso efectivo, interactivo y que asegure la calidad de los passwords.

Requerimientos
Se requiere contar con una política de passwords para asegurar la intergridad y confiabilidad de los mismos.

Es necesario contar con una correcta administración de passwords para poder asegurar la calidad de los passwords como son la longitud, historia de passwords similares.

Normas
Establecer un esquema de control de password para asegurar la integridad de los mismos.
Deberá asegurarse que la aplicación cuente con mecanismos de control de usuarios para protección a diferentes niveles de la aplicación, ya sean de solo lectura, lectura-escritura, y Administración general.

Diseño
- Se deberá establecer una política de asignación de contraseñas para asegurar la calidad de las contraseñas, especificando longitud, tipo de caracteres y tiempo de expiración.
-
- Implementar el esquema de aseguramiento de contraseñas del sistema operativo windows NT y del sistema PQM.

BS7799: [9.5.5] Use of System Utilites

El uso de las utilerías de sistema debe ser restringido y altamente controlado.

Requerimientos
Es necesario controlar los accesos a las herramientas de sistema para evitar cualquier mal uso de ellos, asignando responsables de estos sistemas permitiéndose acceso sólo a ellos.

Normas
- El acceso a las herramientas de sistema como las herramientas de sistema operativo, instaladores de la aplicación, etc. deberán ser estrictamente controlados asignando y documentando al personal que deberá tener la capacidad y responsabilidad de hacerlo.
- Deberá contarse con una bitácora de cambios para llevar un control de cualquier cambio o acceso que deba ser ejecutado o modificado.

Diseño
- Deberá asignarse el personal que deberá contar con privilegios para acceder las utilerías de sistema.
- Los administradores deberán registrar cualquier necesidad de uso de las herramientas de sistema para llevar un registro de los movimientos ejecutados por los administradores, llenando las bitácoras específicas al uso de las herramientas de sistema.

BS7799: [9.5.7] Terminal Time-Out

Terminales inactivas en ubicaciones de alto riesgo sirviendo sistemas de alto riesgo deberán apagarse o bloquearse después de un periodo definido de inactividad para prevenir el acceso de personas no autorizadas.

Requerimientos

Cualquier terminal que esté desatendida es vulnerable a mal uso de personal no autorizado deberá asignarse una política para establecer al tiempo de inactividad que debe transcurrir para que la terminal de acceso al sistema PQM deberá ser automáticamente bloqueado.
Aunque las terminales del sistema PQM se encuentran dentro de la planta, las ubicaciones de estas no pueden estar en sitios restringidos ya que se encuentran a lo largo de la producción este ambiente puede generar la situación adecuada para que personal no autorizado pueda acceder estos recursos.

Normas

- Deberá contarse con una política de bloqueo de terminales en el que especifique el tiempo en el que esta deberá ser bloqueada por inactividad.
- Deberá implementarse un esquema de bloqueo de contraseñas automático que en determinado tiempo bloquee la terminal por inactividad.

Diseño

- La política que establece el tiempo de bloqueo por inactividad de las terminales PQM, será de 5 minutos como tiempo máximo de inactividad para bloquear los equipos, al transcurrir este tiempo será necesario introducir la contraseña de acceso.
- Deberá implementarse en todas las terminales la política de tiempo de bloqueo por inactividad.

BS7799: [10.5.1] Change Control Procedures

La implementación de los cambios debe ser estrictamente controlada por el uso de procedimientos de cambios formales.

Requerimientos

Tanto el sistema PQM como el sistema operativo debe ser actualizado de manera periódica, es necesario implementar un sistema de control de

cambios generando documentos de control de cambios y procedimientos de actualización para registrar y controlar de manera más adecuada cada una de estas actualizaciones.

Normas
- Es necesario establecer documentación donde se lleve el control de cambios y actualizaciones del sistema, este documento debe ser registrado por la persona responsable de la actualización y validado por el encargado del sistema.

Diseño
- la bitácora de actualizaciones deberá contener fecha de actualización, componentes actualizados, firma de autorización, impacto del cambio y tiempo de actualización.

BS7799: [8.1.4] Segregation of Duties

Las acciones y áreas de responsabilidad deben ser segregadas esto para reducir el riesgo de modificación o mal uso de la información o los servicios.

Requerimientos
Unas de las principales fallas de la aplicación es debido a la falta de conocimiento o delegación de responsabilidades en el uso del sistema PQM por lo que es necesario implementar un estricto control generando políticas de acceso y asignación de roles, aunado con un programa de capacitación adecuada para asegurar la correcta operación de las aplicaciones.

Normas
- Es necesario establecer explícitamente las responsabilidades de cada uno de los usuarios del sistema PQM esto para reducir la vulnerabilidad de la aplicación por mal uso o modificación indebida por falta de conocimiento o negligencia.
- Es necesario implementar un esquema de capacitación del sistema para el personal que lo utiliza, teniendo control del personal que haya tomado el plan de capacitación.

Diseño
- Con el control de usuarios deberá asignarse el tipo de acceso que cada uno de los usuarios necesita y al momento de asignarle ese usuario, integrarlo en el grupo de usuarios del que requiere acceso, estos tipos de acceso pueden ser de lectura, lectura-escritura, modificación a configuración, modificación a parámetros, administrador.

- Implementar un programa de capacitación de uso de sistema PQM, llevando control del personal que haya tomado la capacitación y bloqueando a los usuarios que no hayan tomado los cursos o que no se hayan actualizado en la capacitación que requieran.

BS7799: [8.3.1] Controls Against Malicious Software

Los controles para la detección y prevención para proteger contra software malicioso y es necesario la implementación de procedimientos de capacitación para el conocimiento de los usuarios al respecto.

Requerimientos

Para asegurar la continuidad de la operación, el sistema PQM así como todos los demás está susceptible de ataques de software malicioso por lo que es necesario implementar distintos tipos de bloqueo de este tipo de software.

Normas

- Establecer un perímetro adecuado para la operación del sistema que limite cualquier acceso no autorizado al sistema.
- Establecer un bloqueo a nivel aplicación estableciendo zonas de operación.
- Se deberá contar con una política de parcheo en el que determine la periodicidad, verificación e implementación de los parches que salgan para la aplicación y sistema operativo, para poder eliminar cualquier vulnerabilidad de sistema.
- Implementar un sistema de antivirus eficiente y multi-capas, que además tenga la capacidad de actualizarse automáticamente, que tenga la capacidad de parar cualquier worm o programa malicioso proveniente de cualquier medio, que remueva los virus y worms automáticamente, además que mantenga una bitácora de los virus y worms detectados y que avise de cualquier virus encontrado a los administradores del sistema.

Diseño

- El perímetro de trabajo y de seguridad en la red será implementado a través de firewalls y VLAN’s, los accesos deberán ser especificados a través de listas de acceso.
- Se establecerá una política de uso de la aplicación para restringir los usuarios que tienen privilegios de acceso al sistema y bloqueando todos los que no requieren acceso, este bloqueo puede ser por segmentos de red o por puertos del sistema.
- La política de actualizaciones de parches de sistema y aplicación deberá establecer que se debe actualizar mínimo cada 30 días las actualizaciones del sistema y la aplicación analizando cada

actualización y validando su necesidad de implementación, será necesario hacer pruebas de implementación antes de actualizar el sistema en producción.

- Se implementará el sistema de Antivirus que cuente con las siguientes características:
  - Protección de worms y virus
  - Auto Scan que actualiza la lista de virus de manera automática
  - Validación de archivos en tiempo real para que verifique cada archivo que sea ejecutado en el sistema
  - Bitácoras de control en el que se mantenga registro de cada virus o worm detectado
  - Aviso de cualquier virus detectado al administrador

BS7799: [8.4.1] Information Backup

Los respaldos de información esencial para el negocio deben ejecutarse y probarse con regularidad.

Requerimientos

Es necesario implementar un sistema de respaldos eficiente para poder contar con la información en caso de un desastre, aunque la mayoría de la información del sistema PQM es en línea, algunos cambios toman cargo en un tiempo considerable y que en caso de algún desastre como falla en el sistema deberá ser necesario recuperar, las acciones necesarias para cumplir con este control son las siguientes.

Normas

- Deberán existir procedimientos específicos de respaldo y restauración de información de la aplicación PQM
- Deberá especificarse que parte de la aplicación requiere respaldo, recurrencia de este respaldo, cual respaldo debe estar en sitio, fuera de sitio.
- Se deberá contar con una bitácora e inventario de respaldos efectuados donde se especifique fecha, archivos respaldados, tiempo de respaldo, bytes respaldados, tipo de respaldo (incremental, diferencial).
- Los medios de respaldo deberán ser probados a intervalos regulares para asegurar su utilidad, contando con un registro de estas pruebas.
- Deberá contarse con un esquema de replicación de datos para asegurar la consistencia de los datos en caso de una falla de hardware.

Diseño

- Se implementarán procedimientos de respaldo y restauración especificando los pasos que son necesarios para efectuar dichas acciones, así como los responsables de la ejecución de estos procesos,

dichos procedimientos contarán con checklists de validación para cada procedimiento.
- La documentación de los respaldos debe contener la parte de la aplicación que debe ser respaldada, la periodicidad, que parte de los respaldos deben estar en sitio y fuera de sitio, el tiempo que estos respaldos deben de estar almacenados y todo esto debe estar autorizado por el responsable de la aplicación y el encargado de sistemas, esta documentación servirá para que ambas partes estén de acuerdo en el esquema de respaldos implementado para el sistema PQM.
- El operador o sistema de respaldos deberá llenar la bitácora de los respaldos efectuados especificando fecha, archivos respaldados, tiempo de respaldo, bytes respaldados, tipo de respaldo (incremental, diferencial), esta bitácora deberá almacenarse en un lugar adecuado para ser utilizada en caso de un desastre.
- Dentro de los procedimientos normales de respaldo deberá integrarse un esquema de pruebas de respaldos, este esquema determinará la periodicidad de las pruebas que será de cada 30 días, validará el checklist utilizado para la restauración en caso de un desastre y se generará un reporte con los resultados obtenidos de las pruebas.
- Se implementará un esquema de arreglo de discos de hardware para que en caso de falla se tenga la capacidad de reducir el mal funcionamiento debido a esto y asegurar la continuidad de la operación.

BS7799: [8.4.3] Operator Logs and Fault Logging

El equipo de operaciones deberá mantener un log de sus actividades, Los logs de operaciones deberán estar sujetos a verificaciones regulares, cualquier falla deberá ser reportada y deberá ser tomada una acción correctiva.

Requerimientos

Los logs de operaciones son importantes para proveer seguridad a través del monitoreo de la integridad de la operación en los sistemas, además de ser útiles en ayudar en caso de investigación por algún incidente.

Normas

- Deberán implementarse esquemas de logeo automático tanto de las aplicaciones como del sistema operativo.
- Estos logs deberán ser retenidos por un periodo considerable de tiempo y deben estar sujetos a verificaciones frecuentes.

- El área operativa deberá validar que los logs estén en buenas condiciones así como validar cualquier problema que se registre en los logs de manera periódica.

Diseño
- Deberá configurarse los logs de la aplicación y sistema operativo para que registren los eventos importantes de estos, tanto los avisos informativos como las alertas y los avisos de precaución.
- El tiempo que será necesario retener los logs de información será de 30 días mínimo, tanto en aplicación como en sistema operativo.
- Se implementarán procedimientos de verificación de logs periódicos para su correcta validación.
- Se asignarán responsables del mantenimiento, pruebas e implementación de los logs de información.

BS7799: [9.7.3] Clock Synchronization

Las computadoras deben ser sincronizadas en los relojes para una grabación correcta.

Requerimientos
El sistema PQM depende mucho de la sincronización de los sistemas ya que depende del registro del tiempo para determinar los niveles de producción, además de tener la capacidad de analizar los logs de información entre activos de información de manera adecuada y cronológicamente sincronizada.

Normas
- Implementar un sistema de sincronización de relojes entre sistemas, manteniendo una misma hora en todos los activos de información.
- Implementar un sistema de validación de relojes para asegurarse que la sincronización es adecuada.
- Generar procedimientos de cambio de horario cuando este sea necesario como en el inicio y término del horario de verano.

Diseño
- Se implementará un esquema de sincronización de relojes de sistema a través de las herramientas de sistema operativo, ya que el sistema PQM se encuentra en una red de dominio Windows NT y esta proporciona herramientas de sincronización de relojes además que la aplicación PQM se sincroniza con la red INFI para contar con la misma hora de producción.
- Se generará un procedimiento de validación automática de la hora en el que registre cualquier diferencia de horas entre equipos, mandando un aviso a los administradores en caso de cualquier diferencia.

- Se llevarán a cabo los procedimientos de cambio de horario cuando cambie el horario de verano, al inicio y al final.

BS7799: [10.5.4] Covert Channels and Trojan Code

La compra, uso y modificación de software debe ser controlado y verificado para proteger contra código secreto o código troyano.

Requerimientos
Los activos de información PQM son muy críticos para la empresa por lo que el uso de cualquier otro software fuera del requerido por el sistema deberá ser estrictamente controlado para evitar cualquier código secreto o troyano,

Normas
- Se deberá contar con una política de instalación de software para la aplicación de PQM en el que establezca el software necesario que debe de estar instalado en este sistema.
- Se deberá contar con un inventario de software necesario para la aplicación PQM así como los responsables de ese software.
- Asegurar que no sea instalado cualquier otro software que no cumpla con los requerimientos del sistema PQM.

Diseño
- Implementar una política de instalación de software restrictiva para todo el personal que no sea los responsables de instalarlos.
- Generar documentación de los activos de software que deben de ser instalados para el correcto funcionamiento del sistema PQM y no permitir la integración de otro software que no se encentre en esta documentación.
- Implementar un programa de validación de aplicaciones para asegurarse que no se haya instalado ningún otro software adicional al requerido por personal no autorizado.

BS7799: [8.5.1] Network Controls
Un rango de controles debe ser implementado para lograr y mantener la seguridad en las redes.

Requerimientos
Las redes son especialmente vulnerables a abuso y mal uso así como fallas no intencionadas de la tecnología, la única forma de reducir estos riesgos es implementar controles de administración y seguridad junto con procedimientos adecuados de operación y control de cambios.

Normas
- Contar con la documentación completa de la infraestructura de red.
- Administrar y controlar los accesos a los recursos de red.
- Establecer perímetros de operación para segmentar las redes si es posible por aplicación
- Establecer lista de controles de acceso
- Implementar esquemas de encripción
- Implementar monitoreos de ancho de banda y de análisis de paquetes para la detección de ataques y análisis de tráfico

Diseño
- Se contará con un inventario, estructura de operación y diseño detallado de la infraestructura de red que interactúa con el sistema PQM.
- Los accesos de red estarán controlados de manera individual y bajo esquemas de acceso controlado.
- Cualquier acceso o transferencia de datos en el que el medio sea considerado de alto riesgo, se implementará un esquema de encripción para asegurar ese canal de comunicación.
- Toda la red será monitoreada por los administradores analizando anchos de banda consumida, tiempos pico, errores en paquetes e intentos de accesos no autorizados.

BS7799: [11.1.1] Business Continuity Management Process and Impact Analysis

Deberá haber un proceso administrado para desarrollar y mantener la continuidad del negocio.

Requerimientos
- Cualquier organización puede estar involucrada en un desastre o interrupción de sus procesos, cada organización es vulnerable a las consecuencias de formar parte de estas eventualidades, por lo que es necesario establecer una administración de continuidad del negocio comúnmente llamado Business Continuity Plan e Impact Analysis. Los resultados de este análisis de impacto serán utilizados para desarrollar el Business Continuity Plan.

Normas
- Se deberá implementar un esquema de Business Continuity Plan e Impact Análisis determinado y valorando cada uno de los activos de información relacionados con el sistema PQM.
- Deberá generarse una valoración de riesgos de los activos para proveer niveles de protección y administración de riesgos.

- Estos análisis permitirán que se implementen planes de contingencia en caso de desastre y estar preparados en caso de cualquier eventualidad.

Diseño
- Se establecerá un equipo de auditores y responsables de la valoración de los activos de información para implementar un análisis de impacto en caso de desastre, este equipo estará constituido de personal de sistemas y personal responsable del sistema PQM.
- El equipo de auditores determinará el impacto en caso de desastre de cada uno de los activos de información relacionados con el sistema PQM.
- Este análisis será basado en los riesgos e impactos relacionados con interrupción del negocio y lo que se compromete derivado de esto.
- El resultado de este análisis será firmado por el departamento de administración para la validación de su conocimiento.

BS7799: [11.1.3] Writing and Implementing Continuity Plans
Un plan de continuidad será implementado para mantener o restaurar las operaciones del negocio de una manera pronta después de una interrupción por falla o interrupción de los procesos.

Requerimientos
El plan de continuidad del negocio deben incluir acciones detalladas que deben ser tomadas en caso de emergencia o interrupción y quien es el responsable de las acciones que se deberán efectuar para mitigar esa interrupción, todas estas acciones deberán estar acordadas a lo largo de toda la organización.

Normas
- Deberán especificarse cada uno de los responsables que formarán parte del Business Continuity Plan.
- Cada uno de los responsables deberá tener pleno conocimiento de las acciones y responsabilidades que deberá tomar en caso de un desastre.
- Todos los procedimientos que se deberán efectuar en caso de un desastre deberán estar plenamente establecidos y autorizados por la administración.
- Los procedimientos deberán ser probados periódicamente.

Diseño
- Se generará un documento basado en el Business Continuity Plan e Impact Análisis para determinar los responsables de cada una de las acciones que deben ser realizadas en caso de desastre.

- Se generarán checklists de procesos que deben ser realizados cuando suceda un desastre junto con los responsables de cada uno de estos procesos.
- Se implementará un esquema de pruebas del plan de contingencia para asegurar su vigencia y efectividad.

BS7799: [11.1.4] Business Continuity Plan Framework

Un solo esquema de Business Continuity Plan deberá ser mantenido en la organización para asegurarse que los planes sean consistentes, y para identificar prioridades de pruebas y mantenimiento.

Requerimientos

Por su naturaleza un Business Continuity Plan es susceptible a generarse distintos planes, cada uno provisto por una parte específica de la organización por lo que es necesario generar un enlace entre cada uno de estos planes para que tengan una consistencia y no sea susceptible a fallas por estas diferencias.

Normas

- Establecer una base de desarrollo para los Buisness Continuity Plan que se implementen en la corporación, y que sea el estándar para todos los departamentos
- Que exista una interacción e intercambio de información entre departamentos para que exista una consistencia en cada uno de estos planes.

Diseño

- Se implementará un estándar del formato del Buisiness Continuity Plan para que todos los diferentes departamentos que cuenten con uno tenga consistencia y correlación entre ellos.
- Cada equipo que se genere para implementar el Buisiness Continuity Plan deberá ser responsable de hacer llegar información a los demás equipos que se conformen para elaborar estos planes, además se asegurarán que exista congruencia entre planes para que no existan diferencias que lleven a un plan a su falla.

BS7799: [11.1.5] Testing, Maintaining and Re-assesing Business Continuity Plans

Los Business Continuity Plans deberán ser probados regularmente y deberán ser revisados para asegurar que están al día y que son efectivos.

Requerimientos

La organización pudiera haber desarrollado planes de contingencia pero al no ser probados pueden ser más vulnerables a desastres. Los constantes

cambios en la organización pueden generar diferencias en la información contenida en estos planes y la información real, pruebas regulares y mantenimientos a estos planes son necesarios para evitar estos problemas.

Normas

- Establecer políticas que determinen los planes necesarios para hacer pruebas a los Business Continuity Plans, su registro y periodicidad.
- Establecer responsables de los cambios que se deben efectuar para mantener los Business Continuity Plans al día.

Diseño

- Se establecerían políticas en las que se determine que pruebas a los Business Continuity Plans deberán de ser efectuadas con una periodicidad de 3 meses, los resultados obtenidos serán evaluados para efectuar los cambios correspondientes.
- Se asignarán los responsables de hacer los cambios que sean necesarios a los Business Continuity Plans registrando cada actualización efectuada con responsable, fecha, cambios efectuados.

4.6 Plan de Acción - Fase de Implementación

Una vez obtenido todos los elementos que se requieren para analizar el activo de información, habiendo determinado sus amenazas y riesgos y habiendo generado una matriz de controles para mitigar esas amenazas, se procede a la integración de los procesos con los controles que el BS nos arrojó, se generará un plan de acción, estableciendo los tiempos de ejecución, responsables, etc. A través de un Plan de Trabajo podremos establecer métricas, objetivos y alcances tomando en consideración los factores externos que intervienen en el proceso de la integración de la seguridad en un activo de información.

Una de las partes más importantes es la generación e implantación de políticas de seguridad de la información, estas políticas generalmente existen dificultades de implementar en una empresa, una forma de mitigar esta dificultad es asignando a un responsable de la seguridad en las tecnologías de información en la empresa, para que se encargue de coordinar e implementar las políticas de seguridad de manera eficiente, para asegurar que el resultado final satisfaga las necesidades de la empresa y sea aceptada como parte normal de las operaciones de la compañía por parte de las personas a quien aplica esta política ya que inicialmente existirá un alto grado de resistencia a la integración de políticas en su operación diaria.

Las políticas de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y la cultura que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentación los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

Una vez completado el proceso de implementación se procede a monitorear continuamente que los controles sean aplicadas de manera adecuada además de las actualizaciones que el BS 7799 tiene, todo esto debido a las constantes vulnerabilidades que continuamente se descubren en los sistemas de información.

CAPITULO 5

5. Estudio de Campo

5.1 Distribución de la muestra

La encuesta que se elaboró tiene el objetivo de observar la situación actual de la seguridad en las tecnologías de información en México, cual es la postura del personal de tecnologías de información relacionado con este concepto y cual es la percepción de la seguridad en las TI en este sentido.

La encuesta se elaboró con un total de 30 personas que están directamente relacionadas con las tecnologías de información, se seleccionaron personal de diferentes niveles organizacionales desde directivos, gerentes, personal de soporte y desarrollo esto para tener una esquema más integral de la percepción de las tecnologías de información en el área de informática.

5.2 Recolección de Datos

Se les pidió a estas personas que contestaran una encuesta relacionada con la seguridad en las TI, el nivel de seguridad actual en sus empresas y el conocimiento del estándar BS7799, se aplicó esta encuesta a diferentes niveles organizacionales para analizar la diferente percepción que tienen de la seguridad en cada uno de estos.

5.3 Hipótesis

H1. El uso de estándares de seguridad como el BS7799 ayuda a definir un esquema común de niveles de seguridad entre las empresas garantizando los niveles de integridad, confidencialidad, disponibilidad de las empresas.

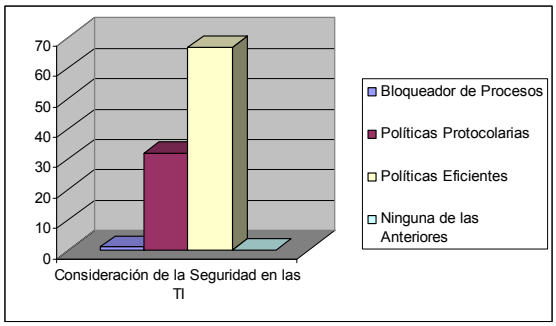
H2. La implementación de un esquema de seguridad ayuda a valorar, administrar y reducir los riesgos de una manera más organizada y estructurada.

H3. La implementación de un esquema de seguridad ayuda al personal a generar importancia y conciencia acerca de los diferentes riesgos que los activos de información pueden tener.

5.4 Resultados

La encuesta fue aplicada en el departamento de tecnologías de información de la empresa de manufactura, a especialistas del área de tecnologías de información. Los resultados obtenidos fueron analizados y de acuerdo a los datos generados obtuvimos los siguientes resultados:

Para poder determinar la percepción de la seguridad en las TI del personal, se planteó como consideran la seguridad en las TI desde el aspecto de ser un bloqueador de procesos a un conjunto de políticas para salvaguardar la información de manera eficiente, las respuestas fueron muy impactantes ya que aunque la mayoría de los encuestados determinó que es un conjunto de políticas eficientes, una cuarta parte piensa que son sólo un conjunto de políticas protocolarias y no cumplen los objetivos establecidos.

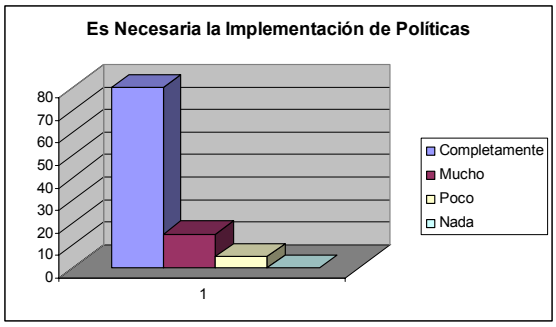


Gráfica 5.4-1 Consideración de la Seguridad en las TI

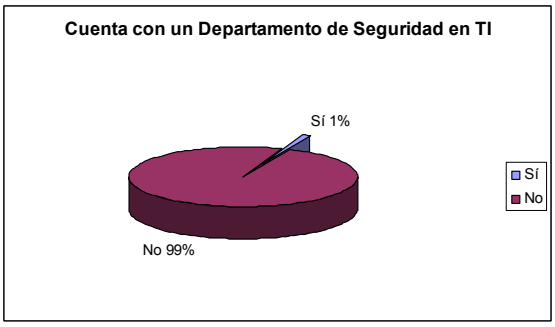
Gráfica 5.4-2 Existencia de Políticas en la Empresa

En el siguiente cuestionamiento se planteó si existía algún tipo de políticas y procedimientos de control de seguridad, para establecer el grado de integración de la seguridad en la empresa, el resultado fue que la mayoría de los encuestados determinó que si cuentan con algún tipo de política de seguridad en su empresa, lo cual indica que tienen cierto control de seguridad implementando políticas de seguridad en sus empresas.

A continuación quisimos establecer el grado de importancia para implementar políticas de seguridad in las TI en la empresa, para poder determinar el grado de interés en la implementación de una estructura de seguridad adecuada, el resultado fue que la mayoría de las personas piensan que sí es necesaria la implementación de políticas en las empresas.



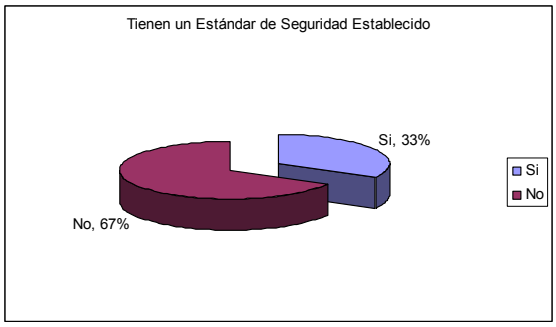
Gráfica 5.4-3 Necesidad de Implementación de Políticas

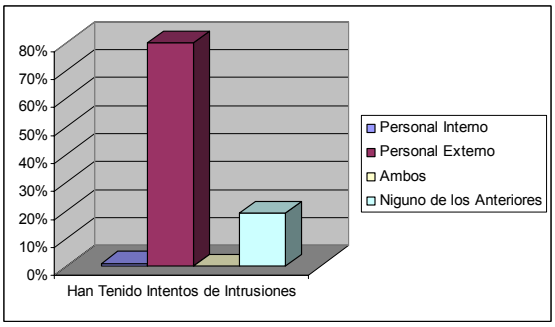


Gráfica 5.4-4 Se cuenta con departamento de TI

La importancia de establecer un departamento de seguridad en las TI es cada vez más importante para las empresas, la necesidad de implementar una correcta estructura operativa soportada en seguridad es imperante, por eso la necesidad de conocer si en las empresas cuentan con un departamento formalmente establecido para estructurar e implementar las políticas y procedimientos de seguridad implementando un departamento de seguridad en las tecnologías de información. El resultado fue que en la mayoría de las empresas no cuenta con un departamento establecido sólo para resguardar la seguridad en la información, esto puede deberse a varios factores, por ejemplo el tamaño de la empresa, el rubro de la empresa en la que se esté ubicado, y en muchas ocasiones que otros departamentos absorben las responsabilidades de seguridad en cada una de las empresas efectuando múltiples ocupaciones al mismo tiempo

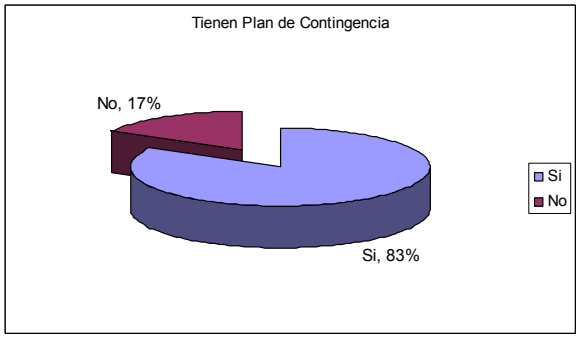
La evolución constante de las amenazas y las constantes actualizaciones en cuestiones de seguridad que son necesarias para salvaguardar la información sin contar las políticas y procedimientos bien definidos que son necesarias para integrar conceptualmente un modelo de seguridad en las tecnologías de información requiere de algún plan de contingencia en caso de desastres primero analizando si la empresa ha tenido intentos de intrusiones y si cuentan con un plan de contingencia en caso de desastres, el resultado arrojó que la mayoría no cuenta con un estándar de seguridad establecido puede ser por falta de conocimiento de los estándares de seguridad o que no cuentan con la infraestructura para desarrollarlo, de los intentos de intrusión podemos observar que la mayoría de estos han sido efectuados por personal externo o no han tenido ninguno intento por lo que podemos afirmar que los ataques internos en nuestra comunidad no son muy frecuentes aunque no se debe descartar que ocurran.





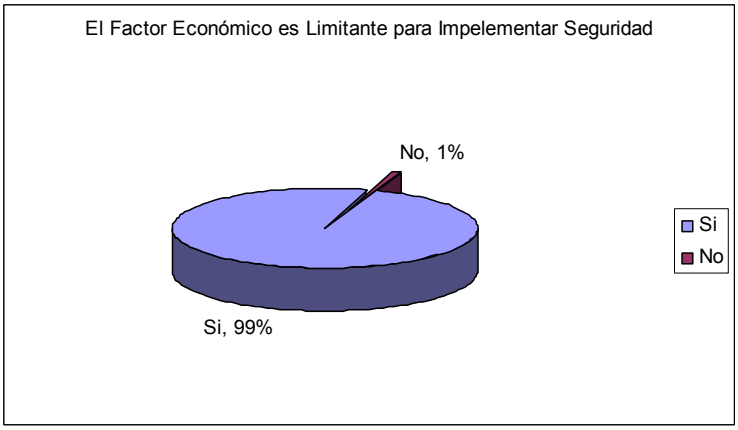
Gráfica 5.4-5 Estándar de Seguridad Establecido

Gráfica 5.4-6 Intentos de Intrusiones



Gráfica 5.4-7 Plan de Contingencia

Por último, se vio la necesidad de analizar la influencia del aspecto económico para implementar un correcto modelo de seguridad en las TI, noventa y nueve por ciento reconoció que existe un déficit en inversiones que se requiere para implementar este modelo.



Gráfica 5.4-8 Factor Económico para Implementación de Seguridad

6. CONCLUSIONES

La implementación de un modelo de seguridad será un estándar en un futuro cercano, las empresas requerirán certificaciones de seguridad para hacer negocios así como en la actualidad son los estándares de calidad, inclusive las certificaciones de calidad pueden tener un nivel mayor en importancia que las certificaciones de calidad, debido a que el impacto de no tener un esquema de seguridad integrado en las empresas puede repercutir en gran medida si llegan a tener algún incidente o eventualidad.

Posiblemente la carrera de los hackers contra las corporaciones nunca terminará solamente administrando y valorando de manera eficiente los riesgos de los activos de información podremos sobrellevar y reducir el riesgo de un ataque que pueda llevar a una corporación al cierre total de sus operaciones.

Esperemos que con el modelo aquí propuesto surjan varias iniciativas para implementar este modelo de seguridad como base con este estándar o con otro diferente como el SAS 70 que es muy similar al BS7799 por lo que su implementación también puede ser muy similar.

ANEXOS

TESIS DE SEGURIDAD
EN LAS TECNOLOGÍAS DE INFORMACIÓN

Por favor contesta las siguientes preguntas, son relacionadas con la seguridad en tecnologías de información en su empresa.

NOMBRE:
CARGO QUE OCUPA:

Marque con una X la opción elegida.

1. ¿En un aspecto general cómo considera la Seguridad en las Tecnologías de información (seleccione el que más considere que aplique)?

   Un bloqueador de procesos ☐
   Un conjunto de políticas protocolarias ☐
   Un conjunto de políticas para salvaguardar la información de manera eficiente ☐
   Ninguna de las anteriores ☐

2. ¿Existen en su empresa políticas y procedimientos de control de seguridad en las tecnologías de información?

   Si ☐ No ☐

3. ¿Considera necesaria la implementación de políticas de seguridad que haga que sus empleados estén capacitados en el área de seguridad en las TI?

   Completamente ☐ Mucho ☐ Poco ☐ Nada ☐

4. ¿Se tienen bien definidas y establecidas las políticas de seguridad de información en la empresa?

   Si ☐ No ☐

5. ¿Existe un área o personal dedicado a la seguridad en tecnologías de información en su empresa?

   Si ☐ No ☐

   En caso de que su respuesta sea No, pase a la pregunta 10

6. ¿El área de seguridad de la información apoya o soporta las estrategias de negocio y la misión de su empresa?

   Si ☐ No ☐

7. ¿Prevalece en toda la empresa una cultura de seguridad de la información?

   Si ☐ No ☐

8. ¿El personal encargado de la seguridad de la información es suficiente para cubrir las necesidades de la empresa?

Si ☐ No ☐

9. ¿La Alta Dirección apoya y se encuentra involucrada con el área o personal de sistemas para la seguridad de la información de la empresa?

   Si ☐ No ☐ No Se ☐

10. ¿Utiliza algún estándar de seguridad de información como referencia para poder implementar mecanismos y/o procesos de seguridad en su empresa?. *Ejemplo: Estándar Británico BS7799.*

   Si ☐ No ☐

11. ¿Sus clientes han expresado la necesidad de implementar un estándar de seguridad en las TI en su empresa?

   Si ☐ No ☐

12. ¿Se cuenta con un plan de contingencia escrito en caso de posibles ataques informáticos?. *Ejemplo: Disaster Recovery Plan, Buisness Continuity Plan*

   Si ☐ No ☐ No Se ☐

13. ¿Se ha detectado algún intento de *¨Hackeo¨* a la organización en los últimos tres años, ya sea por personal interno o externo?

   Por Personal Interno ☐
   Por Personal Externo ☐
   Ambos ☐
   Ninguno de los dos ☐

14. ¿Utiliza algún método (tecnológico y/o de procedimientos) para garantizar la seguridad de la información en su empresa?

   Si ☐ No ☐

15. ¿Considera el factor económico como una limitante importante en la empresa para poder brindar un nivel de seguridad de información de la empresa?

   Si ☐ No ☐

   Muchas Gracias

BIBLIOGRAFÍA

Ricardo Morales, Ricardo Pineda; Curso de Administración de la Seguridad en las Tecnologías de Información; EGADE, MTI, Instituto Tecnológico y de Estudios Superiores de Monterrey; 2003

Mark Higgins; Symantec Internet Security Threat Report Volume III Feb. 2003; Symantec Managed Security Services; EU 1993

[2] X-Force Global Threat Operations Center; Internet Risk Impact Summary; Internet Security Systems; EU 2003

[3] David Gerulski; "Are you Vulnerable?" inernational event summary report; Internet Security Systems; EU 1993

Seymour Bosworth, Michel E. Kabay, Computer Security Handbook; EU 2001

Debrah S. Herrman, Security Engineering and Information Assurance, A practical Guide, Auerbach Publications; EU 2002

Neuman P., Computer Related Risks, Addison-Wesley, 1995

Urs E. Gattiker and Hellen Kelly, Centre for Technology Studies, The University of Lethbridge, Canada 2000

Richard Power; CSI7FBI Computer Crime and Security Survey; Computer Security Institute; EU 2003

Heather Goodell, Scott Meyers; Maximum Security Third Edition; Sams Publishing; EU 2001

James W. Meritt, CISSP, Security: What is it and how much do I need?, Wang Global, EU 1999

Tom Lillywhite; How to Protect your information – an Introduction to BS7799; UK 1999

Humphreys, Plate; Prepairing for BS7799 Certification; BSI, UK 2000