UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

Tema:

"POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010"

Trabajo de Investigación

Previa a la obtención del Grado Académico de
MAGÍSTER EN REDES Y TELECOMUNICACIONES

Autor:

Ing. José Fabián Enríquez Miranda

Director:

Ing. Mg. Clay Fernando Aldás Flores

Ambato - Ecuador

2011

Al consejo de Posgrado de la UTA:

El tribunal receptor de la defensa del trabajo de investigación con el tema: "POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010", presentado por el Ing. José Fabián Enríquez Miranda y conformado por el Ing. Mg. Julio Enrique Cuji Rodriguez, Ing. M.Sc. Franklin Oswaldo Mayorga Mayorga e Ing. Mg. Jaime Bolívar Ruíz Banda, Miembros del Tribunal, Ing. Mg. Clay Fernando Aldás Flores, Director del trabajo de investigación y presidido por el Ing. Mg. Oswaldo Paredes Ochoa, Presidente del Tribunal; Ing. Mg. Juan Garcés Chávez Director del CEPOS – UTA, una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de investigación para uso y custodia en las bibliotecas de la UTA.

Ing. Mg. Oswaldo Paredes Ochoa
Presidente del Tribunal de Defensa

Ing. Mg. Juan Garcés Chávez
Director CEPOS

Ing. Mg. Clay Fernando Aldás Flores
Director de Trabajo de Investigación

Ing. Mg. Julio Enrique Cuji Rodríguez
Director de Tesis

Ing. Mg Franklin Oswaldo Mayorga Mayorga
Miembro del Tribunal

Ing. Mg. Jaime Bolívar Ruíz Banda
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema "POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010", nos corresponde exclusivamente a Ing. José Fabián Enríquez Miranda Autor y de Ing. Mg. Clay Fernando Aldás Flores, Director del trabajo de investigación; y el patrimonio intelectual del mismo a la Universidad Técnica de Ambato.

Ing. José Fabián Enríquez Miranda	Ing. Mg. Clay Fernando Aldás Flores
Autor	Director

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este trabajo de investigación o parte de él un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución

Cedo los Derechos de mi trabajo de investigación, con fines de difusión pública, además apruebo la reproducción de esta, dentro de las regularizaciones de la Universidad.

_____

Ing. José Fabián Enríquez Miranda

DEDICATORIA

Dedico este trabajo a Jesucristo mi Señor y Salvador, quien gracias a su inspiración divina, ha sabido llevar mi vida por el sendero del bien y ha hecho de cada actividad por mi emprendida, un verdadero milagro, a mi novia Paulina pues ella con su amor incondicional le ha dado sentido a cada uno de mis esfuerzos y actividades emprendidas, a mi familia por su constante apoyo y a mi Amigo David, propietario de la empresa Turbotech, por su confianza, amistad y gran capacidad de superación.

.

.

José Fabián

AGRADECIMIENTO

Agradezco infinitamente al Ing. Clay Aldás Msc. por su profesionalismo en el asesoramiento de la elaboración de este trabajo investigativo, a la empresa Turbotech donde se plasmó este trabajo de investigación, puesto que gracias a la confianza que sus directivos han puesto en mi esta proyecto se ha convertido en una realidad.

.

José Fabián

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE ESTUDIOS DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES

"POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010**"**

Autores: Enríquez Miranda José Fabián
Tutor: Ing. Mg. Clay Fernado Aldás Flores

RESUMEN EJECUTIVO

La investigación sobre "POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010", tiene como objetivo general reflexionar sobre las políticas de seguridad que las empresas privadas deben implementar para precautelar su información confidencial de ataques externos.

La Norma ISO 27001 hace una clara referencia a la seguridad de la información, donde se muestran los parámetros que se deben seguir para conseguir que el activo más importante de las organizaciones sea debidamente protegido.

La Seguridad como lo determina la norma no solo se enfoca a una Seguridad lógica de la información donde se enfatiza la creación de usuarios, protección de acceso a Servidores, etc, sino también hace referencia al área física donde reside la misma.

La Tesis que pongo en consideración ha reflejado la propuesta de implementación de Seguridad Física en la infraestructura del Área de Servidores de la empresa Turbotech, también esquematiza los parámetros de Seguridad Lógica del Servidor Web que almacena los aplicativos Web de la organización, así como las diferentes

Herramientas de software para el control de Intrusos y reducción de las vulnerabilidades a los que está expuesto el Servidor Web.

Además se incluye la implementación de las seguridades y configuraciones externas para controlar el acceso a la red virtual de Turbotech solo a aquellos usuarios debidamente definidos y con sus respectivos roles.

INTRODUCCIÓN

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

Debemos comprender que para que la información se considere segura debe contar con las siguientes características:

Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.

Confidencialidad: La información sólo debe ser legible para los autorizados.

Disponibilidad: Debe estar disponible cuando se necesita.

Irrefutabilidad: El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Es por esto que el presente tema de investigación tiene como importancia fundamental implementar las políticas de seguridad en una institución que por su proyección de crecimiento en el país, Colombia y Panamá, requiere que su información publicada en un sistema web tenga las garantías necesarias para evitar un acceso no autorizado a su información confidencial, considerando que su conexión remota debería presentarse como un recurso de seguridad.

CAPITULO I
EL PROBLEMA

Planteamiento del Problema

Contextualización

Actualmente según matermagazine en su publicación de Febrero 15 del 2009, indica que las empresas tecnológicamente hablando están enfocando sus plataformas de sistemas informáticos para el manejo de su información confidencial a sistemas web, donde asp.net, php y otros lenguajes hacen que el desarrollo e implementación de los mismos sea práctico, fácil y de gran alcance a nivel mundial, donde un gerente puede revisar el movimiento de sus ventas en cualquier lugar del mundo y a cualquier hora, sin embargo los piratas informáticos están al acecho de estas entidades para robar el activo más importante, su información.

Las estadísticas tomadas del Washington Post en la publicación de ciencia y tecnología de Diciembre del 2007, indican que el 36% de las intrusiones denominadas pishing, son las más comunes a nivel mundial en los sitios Web.

En el Ecuador las plataformas web son proyectos que apenas se están desarrollando, puesto que las entidades aún le apuestan a los sistemas cliente-servidor, sin embargo la entidades que han apostado por desarrollas sus sistemas en web forms, apenas están comenzando con análisis de invasiones exteriores que podrían provocar el colapso de sus instituciones, conforme lo indica el Comercio en su redacción titulada “La seguridad Informática no es asunto de parches”, en la columna de tecnología del Domingo 1 de Enero del 2006.

Turbotech al ser una empresa en franco crecimiento y expansión ve la necesidad de migrar sus sistemas informáticos a plataformas web que obviamente predispongan a la empresa a un estándar internacional que permita su desarrollo en Ecuador y Colombia, por lo tanto se hace imprescindible la planificación y posterior desarrollo del software de control de los procesos administrativos y de costos de esta pyme, por lo tanto al gestionar estos nuevos procedimientos se hace necesaria la implementación de políticas de seguridad en los sistemas informáticos al considerar que la administración de la empresa no solo se la va a llevar en diversas ciudades del Ecuador sino que la expansión a Colombia obliga a que dichas plataformas sean seguras para salvaguardad los datos de la organización y hacer que los sistemas sean altamente confiables.

Análisis Crítico

Diagrama Causa Efecto

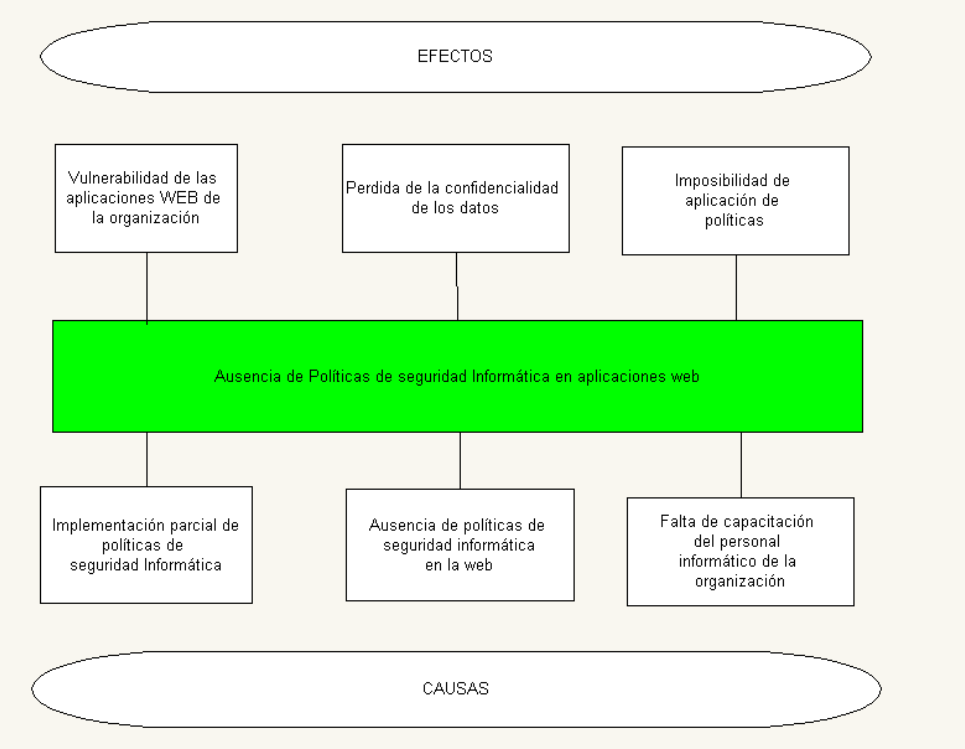


Grafico 1. Diagrama Causa Efecto.

Prognosis

En este contexto de la investigación el no realizarla provocaría que esta importante empresa no tenga las seguridades informáticas correspondientes y por lo tanto su información se convertiría en vulnerable para los hackers informáticos, que le daría mal uso, inclusive se podría llegar a la caída de los servicios informáticos de esta empresa.

Formulación del Problema

¿Cómo afectan las las políticas de seguridad en la vulnerabilidades de los entornos web en la empresa TurboTech?

Interrogantes de la Investigación

¿Cuáles son las políticas de seguridad que se aplican en la empresa TurboTech?
¿A qué vulnerabilidades están expuestos los entornos web de la empresa TurboTech?
¿Existen alternativas de solución al problema de la ausencia de políticas de seguridad en entornos web de la empresa TurboTech?

Delimitación de la Investigación

Campo: Ingeniera
Área: Seguridad de redes
Aspecto: Políticas de Seguridad y Vulnerabilidad de los Entornos WEB
Delimitación Espacial: La investigación se desarrollará en la empresa TurboTech de la ciudad de Ambato
Delimitación Temporal: El estudio se realizará en el primer trimestre del año 2010

Unidad de Observación

- Gerente y Subgerente
- Jefe de Sistemas
- Personal Administrativo

Justificación

La **importancia** de la investigación radica en determinar políticas de seguridad informática en las aplicaciones web para reducir la vulnerabilidad del ataque de piratas informáticos.

El proyecto investigativo es **factible** en la organización ya que se cuenta con la colaboración de los jefes departamentales, de gerencia y subgerencia, así como se cuenta con la suficiente bibliografía para la realización del proyecto. Además la empresa tiene asignado un presupuesto para la realización de la investigación.

Los beneficiarios de la presente investigación serán los mandos medios y los altos directivos, puesto que ellos manejan las transacciones comerciales vulnerables a los ataques.

Objetivos

Objetivo General

Establecer las políticas de seguridad informática para reducir la vulnerabilidad de los entornos web en la empresa TurboTech

Objetivos Específicos

- Determinar las políticas de seguridad que se aplican en la empresa TurboTech
- Cuantificar las vulnerabilidades que están expuestos los entornos web de la empresa TurboTech

- Proponer una alternativa de solución al problema de la ausencia de políticas de seguridad en entornos web de la empresa TurboTech

CAPITULO II
MARCO TEORICO

Antecedentes de Investigación

El trabajo presentado a continuación se basa en investigaciones realizadas por especialistas en los temas a tratar, donde se consideran los aspectos fundamentales del problema tratado y se da una amplia explicación de los temas a tratar.

La presente bibliografía de los proyectos de investigación que abordan los temas del presente proyecto, son :

Con referencia a las políticas de seguridad:

Alexandra Elizabeth Espín Meléndez, “Diseño, Desarrollo e Implementación de un sitio Busines (B2B) para Comercio Electrónico a través de Internet en la empresa Ciudadandina”, 2002,

Conclusión:

- Las webs de negocios varían de acuerdo a su contenido. Estas pueden ser desde simples páginas informativas sobre la empresa y sus actividades hasta páginas que permitan realizar transacciones comerciales o financieras.
- La falta de una ley para reglamentar el comercio en Internet, limita las potencialidades del comercio electrónico en el país. Esta ley regularía la eficiencia y el valor jurídico de los documentos electrónicos, así como también la **protección a los usuarios de este comercio**

Con referencia a la vulnerabilidad de los entornos web

Osorio Bastidas Mónica Jeaneth, “Aplicaciones Web Utilizando la Tecnología XML”,2004,

- **Conclusión:**

  Para el análisis diseño e implementación de esta aplicación prototipo, se opto por el proceso “Proceso software basado en UML para aplicaciones de gestión en la web”, que es simple y útil para el tipo de proyecto planeado; utiliza UML y WAE(Extensión de UML para aplicaciones Web) para la construcción de los modelos, conforme a su seguridad.

Fundamentaciones

Fundamentación Filosófica

En el presente trabajo **s**e considera el paradigma critico – propositivo, porque el problema y el objeto de estudio se encuentran en constante evolución. Enfocado a la investigación con una fundamentación metodológica porque está vinculada a la práctica social, esencialmente dirigida a contribuir al cambio y al mejoramiento del desarrollo organizacional.

La fundamentación de esta investigación aplica su accionar en la búsqueda de las causas que provocan los problemas en el campo mismo donde se provocan, sintetizando las posibles soluciones aplicables en la empresa.

Fundamentación Sociológica

El trabajo de investigación se sustenta en la necesidad de la sociedad de evolucionar al cambio tecnológico, pero considerando la seguridades que todo ámbito de la humanidad en estos últimos tiempos requiere.

Fundamentación Legal

Turbotech es una empresa que se rige a las normas ecuatorianas, en lo relacionado a políticas de impuestos con el SRI.

En lo relacionado a normativas de funcionamiento empresarial esta relacionado a la Cámara de la pequeña Industria de Tungurahua.

El problema a resolver basa su accionar en los principios de la norma **ISO 27001** que constituyen los "Sistemas de Gestión de la seguridad de la información.".
(véase Anexo 4).

Fundamentación teórica

NORMAS DE CALIDAD INFORMÁTICA

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática

debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón las normativas de calidad abarcadas por la ISO (Organización Internacional de Normalización) para la definición de las políticas de seguridad en un entorno web, determinan los siguientes aspectos a considerarse para la implementación:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

LA ISO 27001 SEGURIDAD DE INFORMACION

ISO/IEC 27001 es para certificación, ISO/IEC(Comisión Electrotécnica Internacional) 27002 es para implantar mediante especificaciones técnicas en materia de gestión para la seguridad de informática y los medios por donde fluye la información - ISO/IEC 27001 es "Especificación para Sistemas de Gestión en Seguridad Informática". Estas normativas internacionales compilan guías - fundamentos para implantar mejores prácticas en seguridad de la información.

Especifica los requisitos para implantar, operar, vigilar, mantener, evaluar un sistema de seguridad informática explícitamente "ISMS". Sobre ISO/IEC 27001 permite

auditar un sistema bajo lineamientos ISO/IEC 27001 para certificar ISMS(Sistema de Gestión de la seguridad de la Información).

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido.

POLITICAS DE SEGURIDAD INFORMATICA

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa Turbotech

Objetivos de la seguridad informática

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos

Entorno de seguridad web

La Web se ha desarrollado muy rápidamente y en parte como resultado de este ha habido muchos casos bien conocidos los problemas de seguridad con el navegador web y software de servidor. Incluso comercialmente desarrollado un software Web ha sido propenso a problemas de seguridad graves.

Políticas de Seguridad en entornos web

Otro aspecto que está cobrando especial importancia es la seguridad de la información que se intercambia en el Web. La explotación comercial de Internet exige disponer de sistemas de comunicación seguros, capaces de adaptarse a las

necesidades de los nuevos servicios, como la compra electrónica o la banca a distancia. En estos servicios, se manejan dos conceptos fundamentales, la autentificación (garantizar que tanto el usuario de un cliente Web como un determinado servidor de información son quienes dicen ser) y la confidencialidad (hacer que la información intercambiada no pueda ser interceptada por terceros).

Con los sistemas de comunicación actualmente en uso, es técnicamente posible dar clic un enlace de comunicaciones e interceptar el contenido de las comunicaciones TCP/IP (familia de protocolos de Internet) que por él se transmiten. Cuando se envía información privada, por ejemplo un número de tarjeta de crédito en un formulario de compra, es vital garantizar que la información sea recibida exclusivamente por su destinatario, y que la identidad es la esperada.

Control de acceso a la información

Se utiliza para limitar el acceso a determinados documentos de un servidor Web, en función del origen y tipo de petición. La forma de hacerlo varía con el entorno en el que se publican las páginas (sistema operativo y servidor HTTP, principalmente); en general, todas las soluciones pasan por definir un fichero que contiene las diferentes limitaciones de acceso, en un formato característico del servidor HTTP (Hypertext Transfer Protocol). En algunos casos se utiliza un fichero global con las restricciones de acceso o bien un fichero por cada directorio al que se quiere limitar el acceso.

Cuando un cliente Web accede a un fichero protegido, el servidor devuelve un código de error asociado a la falta de permisos para realizar la operación (código 401). Si el acceso se realiza desde un dominio o dirección IP prohibida, no será posible acceder a la información desde ese sistema. Cuando la protección se basa en nombres y claves de acceso, el browser solicitará estos datos y los enviará al servidor para que sean verificados. Las claves de acceso se envían al servidor por diferentes sistemas, sin codificar (sencillo pero inseguro) o codificadas (DES o Kerberos, por ejemplo). Será el propio servidor HTTP el que informe sobre la manera en que se deben enviar estas claves de acceso.

Para conocer cómo se especifican estas listas de control de acceso, se puede emplear la documentación de los respectivos servidores HTTP.

Existen tres tipos de servidores y controles de acceso:

Control de acceso en un servidor CERN(Organización Europea para la Investigación Nuclear)

La versión 3.0 del servidor desarrollado por el CERN permite limitar el acceso a documentos o grupos de documentos, en función de nombres de usuario o direcciones de origen. El control de acceso se puede realizar para todo el servidor, modificando los ficheros globales de configuración o para un directorio concreto. Como este método está disponible para cualquier usuario, sin necesidad de tener privilegios de administración, será el comentado aquí.

El control de acceso al contenido de un directorio se realiza creando un fichero de nombre .www_acl, en el mismo directorio que los ficheros cuyo acceso se quiere controlar. Un ejemplo aclarará más el formato de este fichero:

secret*.html : GET,POST : trusted_people minutes*.html : GET,POST : secretaries *.html : GET : willy,kenny

Está formado por líneas, cada una de ellas fijando una limitación de acceso diferente. Para cada especificación de ficheros, se indica los comandos HTTP permitidos y los usuarios o grupos de usuarios que pueden acceder. Cuando se añade un control de acceso, automáticamente se deshabilita el acceso para los usuarios o grupos no incluidos. Se utiliza el mecanismo de autentificación básica, en la cual las claves de acceso son transferidas por la red sin codificar.

Se pueden crear usuarios o grupos de usuarios con la aplicación htadm, a través de la cual se generan nuevos usuarios y se les asigna claves de acceso. Además, a través de la configuración global del servidor, es posible fijar permisos de acceso por defecto, o restringir el uso del servidor a determinadas direcciones (o rangos de direcciones) IP

Control de acceso en un servidor NCSA

El servidor HTTP de la NCSA (esto se aplica también a Apache, desarrollado a partir de él) permite limitar el acceso en función de direcciones de origen o nombres de usuario. El procedimiento es similar al del servidor del CERN. Se debe crear un fichero de nombre .htaccess en cada directorio cuyos ficheros requieran protección.

Control de acceso en un servidor Microsoft

El servidor HTTP de Microsoft puede limitar el acceso a máquinas o grupos de máquinas, a través de la utilidad de configuración del servidor (el Administrador de Servicios Internet). Para ello, se agrega la máscara de red de aquellos sistemas a los que se concede (o niega) el acceso al servidor.

Además, es posible controlar de forma individual el acceso a cualquier documento o directorio del servidor, sirviéndose de los permisos de acceso a ficheros y la base de usuarios del servidor NT. Para poder utilizar este tipo de control de acceso, es necesario que el sistema de ficheros en que residen los documentos Web tenga formato NTFS, el único que permite asignar permisos de acceso a ficheros.

Seguridad de Internet

Intentar comunicar un secreto en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la Seguridad en Internet no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red

Aspectos Claves

- **Gestión de claves** (incluyendo negociación de claves y su almacenamiento): Antes de que el tráfico sea enviado/recibido, cada router/cortafuegos/servidor (elemento activo de la red) debe ser capaz de verificar la identidad de su interlocutor.
- **Confidencialidad**: La información debe ser manipulada de tal forma que ningún atacante pueda leerla. Este servicio es generalmente prestado gracias al cifrado de la información mediante claves conocidas sólo por los interlocutores.
- **Imposibilidad de repudio**: Ésta es una forma de garantizar que el emisor de un mensaje no podrá posteriormente negar haberlo enviado, mientras que el receptor no podrá negar haberlo recibido.
- **Integridad**: La autenticación valida la integridad del flujo de información garantizando que no ha sido modificado en el tránsito emisor-receptor.
- **Autenticación**: Confirma el origen/destino de la información -corrobora que los interlocutores son quienes dicen ser.

- **Autorización**: La autorización se da normalmente en un contexto de autenticación previa. Se trata un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

Dependiendo de qué capa de la pila de protocolos OSI se implemente la seguridad, es posible prestar todos o sólo algunos de los servicios mostrados anteriormente. En algunos casos tiene sentido proveer algunos de ellos en una capa y otros en otra diferente.

Seguridad en el Nivel de Red

Implementar la seguridad en el nivel de red tiene muchas ventajas. La primera de todas es que las cabeceras impuestas por los distintos protocolos son menores ya que todos los protocolos de transporte y de aplicación pueden compartir la infraestructura de gestión de claves provista por esta capa. La segunda sería que pocas aplicaciones necesitarían cambios para utilizar la infrastructura de seguridad, mientras que si la seguridad se implementara en capas superiores cada aplicación o protocolo debería diseñar su propia infraestructura. Esto resultaría en una multiplicación de esfuerzos, además de incrementar la probabilidad de existencia de fallos de seguridad en su diseño y codificación.

La desventaja principal de implementar la seguridad en la capa de red es la dificultad de resolver problemas como el de la imposibilidad de repudio o la autorización del usuario, ciertos mecanismos de seguridad extremo a extremo -en los routers intermedios no existe el concepto de "usuario", por lo que este problema no podría darse.

Requisitos y Amenazas de la Seguridad

Para comprender los tipos de amenazas a la seguridad que existen, daremos algunos conceptos de los requisitos en seguridad. La seguridad en computadores y en redes implica tres exigencias:

- Secreto*:* requiere que la información en una computadora sea accesible para lectura sólo a usuarios autorizados. Este tipo de acceso incluye la impresión, mostrar en pantalla y otras formas que incluyan cualquier método de dar a conocer la existencia de un objeto.

- Integridad: requiere que los recursos de un computador sean modificados solamente por usuarios autorizados. La modificación incluye escribir, cambiar de estado, suprimir y crear.

- Disponibilidad*:* requiere que los recursos de un computador estén disponibles a los usuarios autorizados.

Los tipos de agresión a la seguridad de un sistema de computadores o de redes se caracterizan mejor observando la función del sistema como proveedor de información. En general, existe un flujo de información desde un origen, como puede ser un fichero o una región de memoria principal, a un destino, como otro fichero o un usuario.

Hay cuatro tipos de agresión:

Interrupción: un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Ésta es una agresión de disponibilidad. Ejemplos de esto son la destrucción de un elemento hardware (un disco duro), la ruptura de una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción: un ente no autorizado consigue acceder a un recurso. Ésta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un computador. Ejemplos de agresiones a la confidencialidad son las

intervenciones de las líneas para capturar datos y la copia ilícita de ficheros o programas.

Modificación: un ente no autorizado no solamente gana acceso si no que deteriora el recurso. Ésta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos, alterando un programa para que funcione de una forma diferente, y modificando el contenido de los mensajes que se transmiten en una red.

Fabricación: una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad. Un ejemplo sería la incorporación de registros a un fichero.

Ataques Pasivos

Las agresiones pasivas son el tipo de las escuchas o monitorizaciones ocultas de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones: divulgación del contenido de un mensaje o análisis del tráfico.

La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico o un fichero transferido pueden contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.

El segundo tipo de agresión pasiva, el análisis del tráfico, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la

identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se está realizando.

Las agresiones pasivas con muy difíciles de detectar ya que no implican la alteración de los datos. Sin embargo, es factible impedir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones está en la prevención antes que la detección.

Ataques Activos

La segunda categoría de agresiones es la de las agresiones activas. Estas agresiones suponen la modificación del flujo de datos o la creación de flujos falsos y se subdivide en 4 categorías: enmascaramiento, repetición, modificación de mensajes y denegación de un servicio.

Un **enmascaramiento** tiene lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo, se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La **repetición** supone la captura pasiva de unidades de datos y su retransmisión subsiguiente para producir un efecto no autorizado.

La **modificación de mensajes** significa sencillamente que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado.

La **denegación de un servicio** impide o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras que una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es bastante difícil prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. Por consiguiente, la meta es detectarlos y recuperarse de cualquier

REDES

Una **red de computadoras**, también llamada **red de ordenadores** o **red informática**, es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc. incrementando la eficiencia y productividad de las personas.

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, cable de fibra óptica, etc.).

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI (Modelo de interconexión de sistemas abiertos) por la ISO,

el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

Concepto de Internet como Red mundial

Una red interna específica, esta basada en una interconexión mundial de las redes gubernamentales, académicas, públicas, y privadas basadas sobre el Advanced Research Projects Agency Network (ARPANET) desarrollado por WARRA del departamento de la defensa de los EE.UU. también al World Wide Web (WWW) y designando el "Internet" con una "I" mayúscula para distinguirlo de otros internetworks genéricos.

Intranet y extranet

Una red interna que se limitan en alcance a una sola organización o entidad y que utilicen el TCP/IP Protocol Suite, el HTTP, el FTP (Protocolo de Transferencia de Archivos), y los otros protocolos y software de red de uso general en el Internet. Nota: Intranets se puede también categorizar como el LAN, CAN, MAN, WAN.

Una configuración común de una LAN es una intranet. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la infraestructura de una empresa sin los permisos y las contraseñas adecuadas. En una intranet, los servidores web están instalados en la red y la tecnología de navegador se utiliza como frontal común para acceder a información de tipo financiero o datos basados en texto o gráficos almacenados en esos servidores.

Una extranet es una intranet parcialmente accesible para los foráneos autorizados. Mientras que una intranet reside dentro de un firewall y es accesible solo para las personas que son miembros de la misma empresa u organización, una extranet

proporciona varios niveles de accesibilidad a los foráneos. Puede acceder a una extranet sólo si dispone de un nombre de usuario y contraseña validos y de acuerdo a esta información, se decide que partes de la intranet puede ver. Las extranets ayudan a extender el alcance de las aplicaciones y los servicios basados en intranet, asegurando el acceso a empresas y usuarios externos.

Las extranets enlazan clientes, proveedores, socios o comunidades de interés a una intranet corporativa sobre una infraestructura compartida utilizando conexiones dedicadas

De este documento puedo destacar

ATAQUES INFORMÁTICOS

Eavesdropping Y Packet Sniffing

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde estan instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación. Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Ooping Y Downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora. El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron : el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor. Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal. Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para

download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos). La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que estan siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad estan seguramente siendo atacado por un insider, o por un estudiante a miles de km de distancia, pero que ha tomado la identidad de otros. El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en

nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina (163 estudiantes.).

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

Ingeniería Social

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Computo los administradores son amigos o conocidos.

Caballos de Troya

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (P.ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

Difusión de Virus

Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables

(.exe, .com, .bat, etc) y los sectores de boot-particion de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.

Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza. El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

Obtención de Passwords, Códigos y Claves

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta. Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se estan cambiando?)

No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?

VULNERABILIDAD DE APLICACIONES WEB

El desarrollo de aplicaciones web seguras se está convirtiendo en una tarea cada vez más difícil debido a la creciente complejidad y variedad de servicios ofrecidos a través de Internet. La seguridad de las aplicaciones web no es sólo responsabilidad del administrador de sistemas, encargado de la infraestructura y redes, sino también del desarrollador. ASP.NET y .NET Framework ofrecen una gran variedad y riqueza de funcionalidades de seguridad, como la seguridad de acceso a código y la seguridad basada en roles, soporte nativo para autenticación basada en formularios, herramientas para creación de servicios web seguros, acceso seguro a bases de datos.

Introducción a la seguridad en los entornos Web.

La plataforma .NET proporciona como una de sus características más destacadas una robusta infraestructura de seguridad que facilita tanto a los desarrolladores, como administradores y usuarios finales, un mayor control sobre el código que se ejecuta en sus sistemas. Para la seguridad se deben conocer los fundamentos de la seguridad en

el acceso a código (CAS), basada en la identidad de código, en oposición a la identidad de usuario.

Acceso Seguro a datos en ASP .net

La mayor parte de aplicaciones web hoy en día necesitan acceder a bases de datos para obtener información sobre productos, servicios, clientes, etc., y presentar a partir de ella páginas dinámicas. En este módulo aprenderá cómo configurar el servidor web (IIS y ASP.NET) y utilizar ADO.NET para acceder a los datos de forma segura. Se explica además cómo almacenar y acceder a secretos de forma segura.

Autenticación mediante formularios en ASP.NET

La autenticación y autorización resultan fundamentales en toda aplicación web en la que se desee restringir lo que los usuarios pueden hacer. La autenticación permite conocer la identidad de quienes se conectan al servidor. La autorización permite verificar qué privilegios tiene asignados cada usuario y saber así qué acciones le están permitidas. Una vez detectada la necesidad de autenticar y autorizar a los usuarios, surge la importante cuestión de decidir cómo se llevan a cabo. ASP.NET incluye todo un conjunto de nuevas funcionalidades para simplificar la creación de aplicaciones que autentican a sus usuarios mediante formularios.

Autentificación mediante Windows en ASP.NET

La autenticación y autorización mediante Windows resulta mucho más segura que mediante formularios. En los casos en los que se puede utilizar, es de gran importancia en las aplicaciones ASP.NET.

Ataques de Entrada de Usuario

Uno de los medios de ataque más utilizados y eficaces consiste en enviar parámetros inesperados a una página ASP.NET, de manera que no pueda procesarlos y entre en un estado inestable o bien ejecute acciones indeseadas, como cambiar el precio a productos, borrar tablas de una base de datos o acceder a datos confidenciales de otros usuarios. El ejemplo más explotado en ASP.NET consiste en la manipulación de formularios. En este módulo se repasan algunos de los ataques más comunes y peligrosos y la manera de protegerse ante ellos.

Hipótesis

La aplicación de políticas de seguridad informática minimizaran la vulnerabilidad de los entornos web en la empresa Turbotech.

Señalamiento de variables

Variable Independiente

Políticas de seguridad

Variable Dependiente

Vunerabilidad de los entornos web

CAPITULO III
METODOLOGIA

Enfoque

Modalidad de Investigación

Para este trabajo investigativo se ha considerado la modalidad cuanti- cualitativa con énfasis en la argumentación de variables y marco teórico que los sustente .
Además se consideró en el marco de desarrollo factible en el marco de la propuesta.

Tipos de Investigación

Para el presente proyecto se ha determinado la utilización de los siguientes tipos de investigación:

Investigación exploratoria. Recibe este nombre la investigación que se realiza con el propósito de destacar los aspectos fundamentales de una problemática determinada y encontrar los procedimientos adecuados para elaborar una investigación posterior. Es útil desarrollar este tipo de investigación porque, al contar con sus resultados, se simplifica abrir líneas de investigación y proceder a su consecuente comprobación.

Investigación descriptiva. Mediante este tipo de investigación, que utiliza el método de análisis, se logra caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades. Combinada con ciertos criterios de clasificación sirve para ordenar, agrupar o sistematizar los objetos involucrados en el trabajo indagatorio. Al igual que la investigación que hemos descrito anteriormente, puede servir de base para investigaciones que requieran un mayor nivel de profundidad.

Población y muestra

La investigación contará con las siguientes personas:

Personas	**Numero**
Gerente	**1**
Subgerente	**1**
Jefe de Sistemas	**1**
Jefe de Compras	**1**
Jefe de Importaciones	**1**
Jefe de Ventas	**1**
Auxiliar Contable	**1**
Cajera	**1**

Facturador	**1**
Jefe de Mantenimiento	**1**
Jefe de Contabilidad	**1**
Auxiliares de diversas áreas	**4**
TOTAL	**15**

Tabla 3.1. Población y Muestra

Operacionalización de variables

Variable independiente

Políticas de Seguridad Informática.

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS BASICOS	TECNICAS E INSTRUMENTOS
Consiste en asegurar que los **recursos del sistema de información (material informático o programas)** de una organización sean utilizados de la manera que se decidió y que el **acceso a la información** allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su **autorización**	**MATERIAL INFORMÁTICO Y PROGRAMAS**	**HARDWARE**	¿Existen filtros y estabilizadores eléctricos en la red eléctrica de suministro a los equipos? ¿Tienen instaladas fuentes de alimentación redundantes? ¿Tienen instalados sistemas de alimentación eléctrica ininterrumpida para los equipos? ¿Los servidores cuentan con UPS's?	**ENCUESTA JEFE DEL DEPARTAMENTO DE SISTEMAS, GERENTE, SUBGERENTE, GEFES DE AREA, AUXILIARES DE AREA**
		SOFTWARE Y DATOS	¿Se realizan copias de los datos?, con que periodicidad? ¿Existe un procedimiento de copia de seguridad del software y los datos? ¿Se almacena alguna copia del software y datos fuera e los locales de la empresa? ¿Los respaldos de la información se la realizan en discos duros externos? ¿Existen implementado un servidor espejo como backup? ¿El servidor cuenta con un disco espejo para la redundancia de la información?	

Tabla 3.2. Variable Independiente

	ACCESO A LA INFORMACION	**NIVELES DE ACCESO**	¿Existen controles de acceso a los usuarios? ¿El área de servidores está expuesta a usuarios no autorizados? ¿Se crea un nuevo Nombre de usuario y contraseña por cada empleado que ingresa a la empresa? ¿Con que periodicidad se realizan el cambio de contraseñas?	
		POLÍTICAS DE ACCESO	¿Se establecen grupos de usuarios para el acceso a los recursos de los servidores? ¿Existen políticas de grupo aplicables para el acceso a la información?	
	AUTORIZACIÓN	**ROLES DE USUARIO**	¿De qué depende la asignación de los roles de usuario al crear uno nuevo? ¿Cuándo un usuario nuevo es creado tiene acceso a todos los recursos del servidor? ¿Cuándo un usuario se va de la empresa se elimina el usuario asignado a éste en el servidor?	**ENCUESTA AL JEFE DEL DEPARTAMENTO DE SISTEMAS**
		REGISTRO DE TRANSACCIONES	¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos? ¿Existe un procedimiento de identificación y autentificación?	

Variable dependiente

Vulnerabilidad de los entornos web

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS BASICOS	TECNICAS E INSTRUMENTOS
La vulnerabilidad de los entornos web, son los riesgos a los que estan expuestas los **web sites** publicadas en internet, cuyos **servidores** están alojados en lugares remotos y cuyo **nivel de acceso** para la realización de transacciones debe estar limitado a usuarios restringidos	**WEB SITES**	**PUBLICACION**	¿Dispone de web site empresarial? ¿Se ha contratado el hosting a una empresa externa? ¿Se realiza el mantenimiento por personal de la propia empresa? ¿Está alojado en la red empresarial esl servidor Web? ¿Se ha contratado personal informático para que diseñe las aplicaciones?	**ENCUESTA AL JEFE DEL DEPARTAMENTO DE SISTEMAS , GERENTE GENERAL Y SUBGERENTE**
	SERVIDORES	**SEGURIDAD**	¿Se dispone de cortafuegos? ¿Dispone de herramientas que auditen intentos de accesos externos? ¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?	
	NIVELES DE ACCESO	**NIVELES DE ACCESO**	¿Están los servidores protegidos en cuanto a inicios de sesión y acceso a través de la red? ¿Cuentan Turbotech con niveles de acceso a usuarios?	**ENCUESTA AL JEFE DEL DEPARTAMENTO DE SISTEMAS**

Tabla 3.3.Variable Dependiente

Técnicas e Instrumentos

Las técnicas de investigación aplicadas son la encuesta y la observación.

Plan para recolección de Información

La recolección de información se realizó de la siguiente manera, utilizando las siguiente técnicas:

La observación:

Es el registro visual de lo ocurre es una situacional real, clasificando y consignando los acontecimientos pertinentes de acuerdo con algún esquema previsto y según el problema que se estudia

La encuesta:

Este método consiste en obtener información de los sujetos de estudio, proporcionada por ellos mismos, sobre opiniones, actitudes o sugerencias. Hay dos maneras de obtener información con este método: la entrevista y el cuestionario. En el caso de la presente investigación se realizó una encuesta, con preguntas de carácter cerrado para obtener de una manera precisa los resultados base de la investigación.

Plan de procesamiento de información

Una vez aplicada las encuestas se realizará la respectiva tabulación de acuerdo a los resultados que se obtendrán

Análisis e interpretación de resultados

El procedimiento para el procesamiento de los datos y presentarlos de manera tal de realizar los análisis correspondientes, será el siguiente:

1. Calificación y tabulación de los datos.

a. Tabulación de la información mediante tablas de resumen de resultados, donde se determinan los casos que encajan en las distintas preguntas.

2. Análisis e integración de los datos.

a. Se relacionará y se comparará los contenidos documentales obtenidos e integrarlos en forma holística.

b. Los procedimientos utilizados para realizar la tabulación, análisis y la interpretación de los datos recopilados serán realizados a través de encuestas, motivo por el cual se recurrió a la asesoría de un profesional, experto en el área de investigación.

Este método permitirá clasificar y reclasificar el material recogido desde diferentes puntos de vista. El análisis permitirá la reducción y sintetización de los datos, se considera entonces la distribución de los mismos.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Encuesta dirigida al personal administrativo de la empresa TURBOTECHT

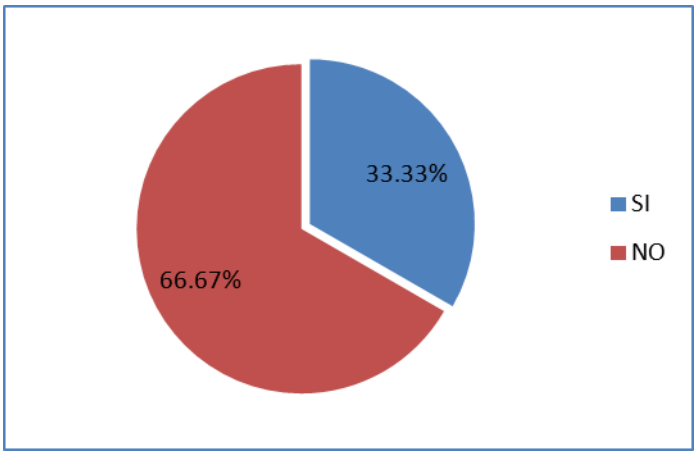
Tabla de frecuencia

Pregunta Nº 1

Tabla N. 1 HARDWARE : ¿Existen filtros y estabilizadores en la red eléctrica de suministros de los equipos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	5	33.33%	33.33%	33.33%
NO	10	66.67%	66.67%	100.00%
TOTAL	15	100.00%	100.00%	

Gráfico Nº 4.1.



Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la primer pregunta que tiene que ver el Hardware de la empresa precisamente si los usuarios y servidores de la empresa cuentan con estabilizadores eléctricos se

determinó que el 66.67% no cuentan con estos equipos de estabilización, mientras que el 33.33% si lo hacen.

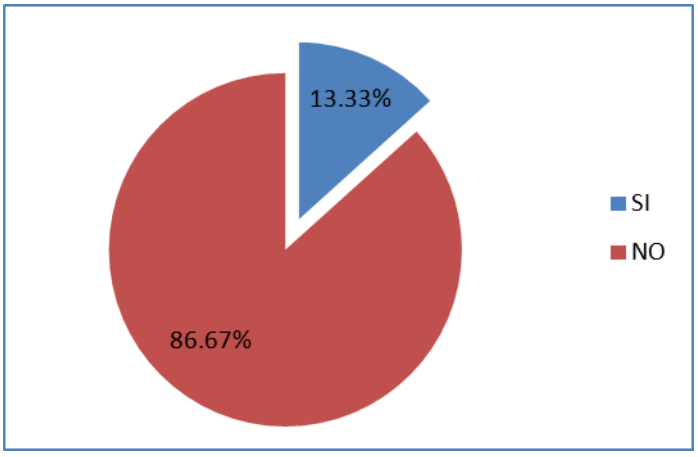
Esto traduce que solo el área de servidores cuenta con estabilizadores de voltaje mientras que los equipos de los usuarios no, esto es muy común pero no se debe descuidar los mismos puesto que el costo de los activos es muy alto.

Pregunta Nº2

Tabla N. 2 HARDWARE : ¿Tienen instaladas fuentes de alimentación redundantes?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	2	13.33%	13.33%	13.33%
NO	13	86.67%	86.67%	100.00%
TOTAL	15	100.00%	100.00%	

Gráfico Nº 4.2.



Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la segunda pregunta que tiene que ver el Hardware de la empresa igual que la pregunta anterior el 86.67% de los usuarios no poseen fuentes de alimentación redundantes mientras que el 13.33% si las poseen.

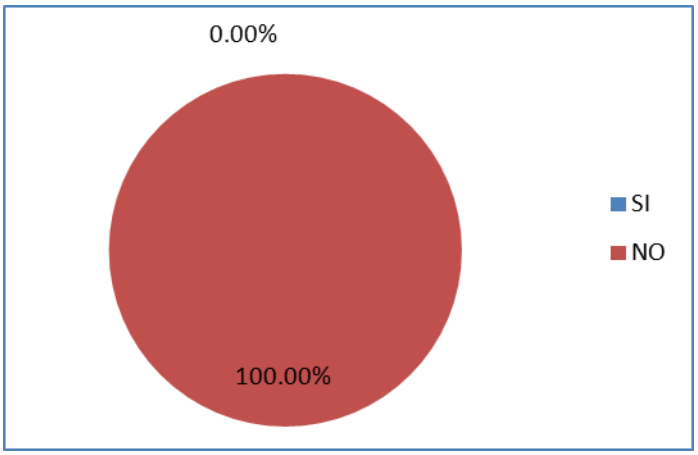
Esto traduce que solo el área de servidores cuenta con fuentes de alimentación redundantes

Pregunta Nº 3

Tabla N. 3 HARDWARE : ¿Tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

Gráfico Nº 4.3.



Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

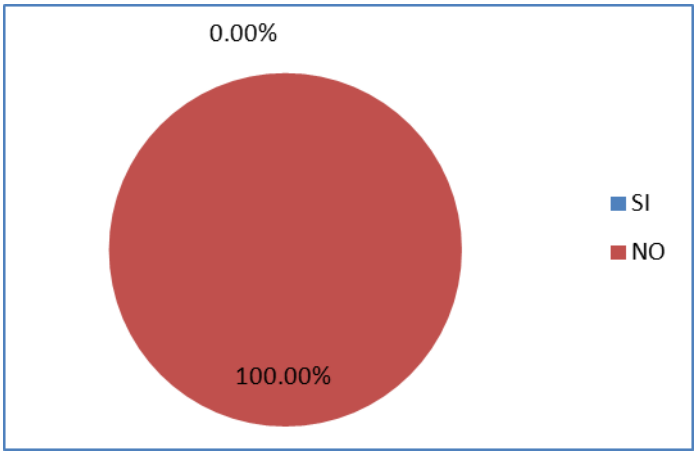
En la tercera pregunta que tiene que ver el Hardware ningún usuario ni servidor de la empresa cuenta con fuentes de alimentación eléctrica instaladas en sus equipos.

Pregunta Nº 4

Tabla N. 4 HARDWARE : ¿Los servidores cuentan con UPS's?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

Gráfico Nº 4.4.



Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la cuarta pregunta que tiene que ver el Hardware nadie del área administrativa cuenta con ups.

La empresa debería contar con estos equipos para proteger sus activos informáticos.

Pregunta Nº 5

Tabla N. 5 SOFTWARE Y DATOS : ¿Se realizan copias de los datos con periodicidad?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

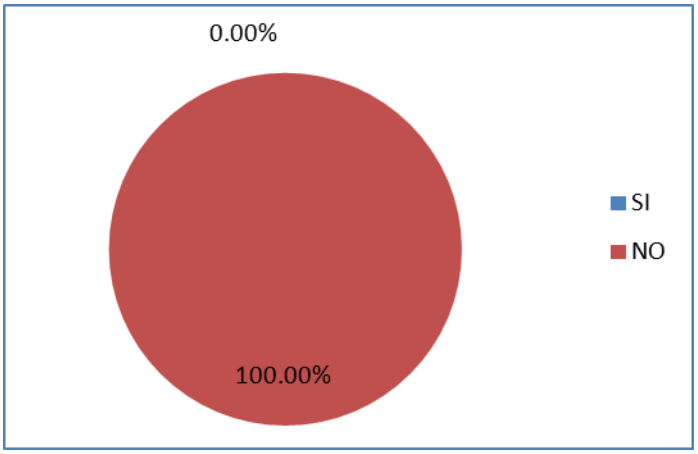


Gráfico Nº 4.5.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la quinta pregunta que tiene que ver el Software y datos, se evidenció según el 100% de las respuestas, que las copias de los datos no se realizan con periodicidad, sino que en tiempos no determinados.

La empresa debería contar con un procedimiento escrito de la política de respaldos de los servidores, puesto que la información es el activo mas importante de la organización.

Pregunta Nº 6

Tabla N. 6 NIVELES DE ACCESO :¿El área de servidores está expuesta a usuarios no autorizados?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	15	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	15	100.00%	100.00%	

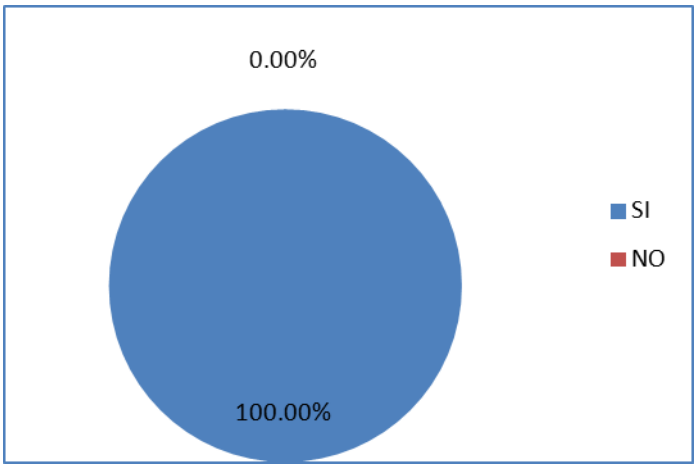


Gráfico Nº 4.6.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la sexta pregunta que tiene que ver el Niveles de Acceso, se evidenció según el 100% de las respuestas, indican que los servidores están expuestos a usuarios no autorizados.

Se debería contar con un identificado DATACENTER o por lo menos especificar seguridad de contraseñas a nivel de los servidores

Pregunta Nº 7

Tabla N. 7 NIVELES DE ACCESO :¿Se crea un nuevo nombre de usuario y contraseña por cada empleado que ingrese a la empresa?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	15	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	15	100.00%	100.00%	

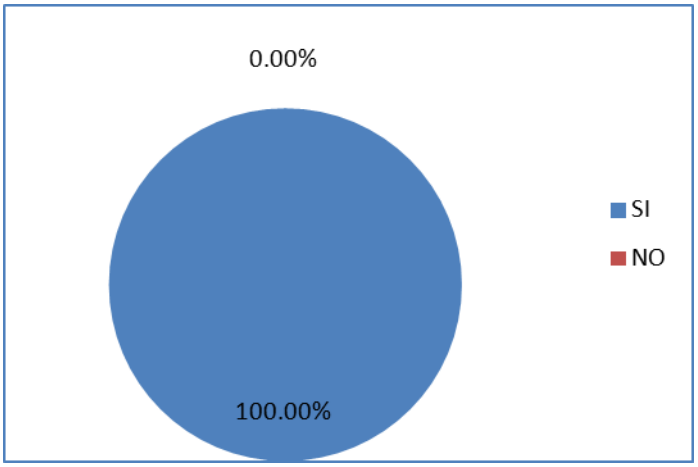


Gráfico Nº 4.7.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la séptima pregunta que tiene que ver con Niveles de Acceso, se evidenció según el 100% de las respuestas, indican que por cada nuevo usuario se crea un nuevo usuario.

Para tener mas certeza se debería especificar un procedimiento de creación de usuarios por cada empleado.

Pregunta Nº 8

Tabla N. 8 NIVELES DE ACCESO :¿Se realiza con periodicidad el cambio de contraseñas?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

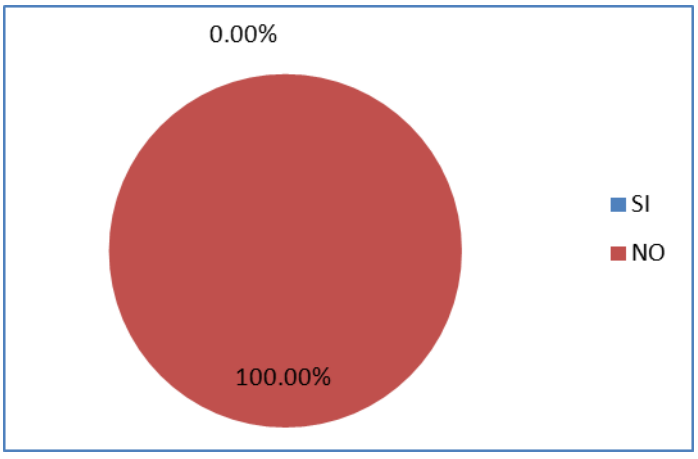


Gráfico Nº 4.8

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la octava pregunta que tiene que ver con Niveles de Acceso, se evidenció según el 100% de las respuestas, que nunca se cambian las contraseñas de los usuarios una vez creados.

Se debería plantear una política de cambio de contraseñas cada cierto tiempo para evitar suplantaciones en los equipos.

Pregunta N. 9

Tabla N. 9 POLITICAS DE ACCESO : ¿Se establecen grupos de usuarios para el acceso a los recursos de los servidores?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	3	20.00%	20.00%	20.00%
NO	12	80.00%	80.00%	100.00%
TOTAL	15	100.00%	100.00%	

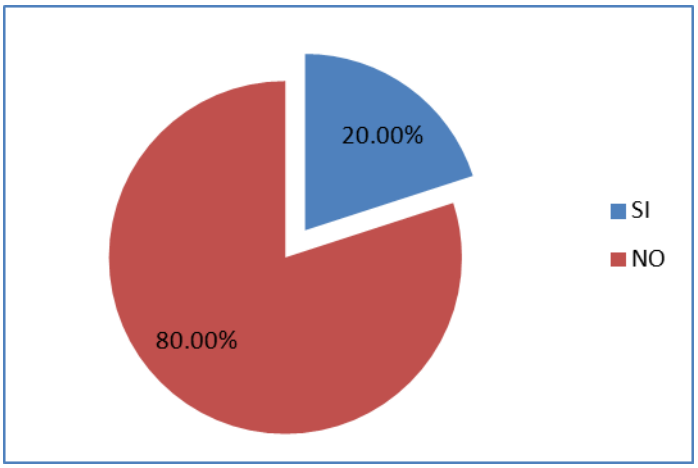


Gráfico Nº 4.9

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

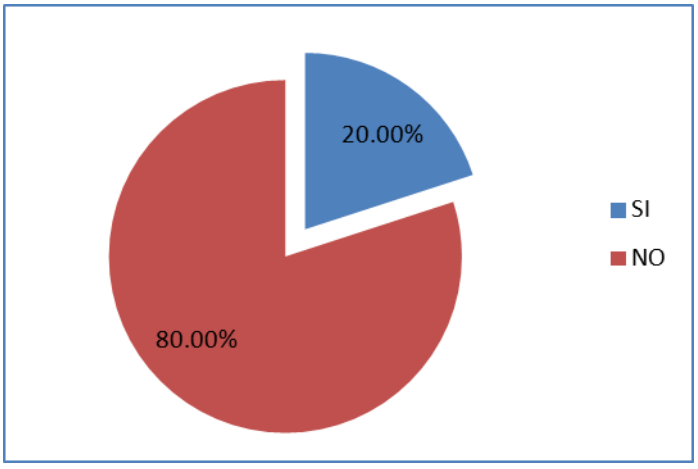
Análisis e Interpretación

En la novena pregunta que tiene que ver con Niveles de Acceso, se evidenció según el 80% de las respuestas que no se establecen grupos determinados de usuarios que tengan acceso a determinadas funciones en los servidores donde todos los usuarios tienen acceso a todos los recursos.

Pregunta N 10.

Tabla N. 10 POLITICAS DE ACCESO : ¿Existen políticas de grupo aplicables para el acceso a la información?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	8	53.33%	53.33%	53.33%
NO	7	46.67%	46.67%	100.00%
TOTAL	15	100.00%	100.00%	



Fuente: Encuestas Gráfico Nº 4.10

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decima pregunta que tiene que ver con Niveles de Acceso, igual que la anterior que el 80% de los usuarios tienen los mismos privilegios de acceso a los recursos de la información sin un control específico.

Pregunta N 11.

Tabla N. 11 REGISTRO DE TRANSACCIONES : ¿Existe un procedimiento de identificación y autenticación?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0%	0.00%	0.00%
NO	1	100.00%	100.00%	100.00%
TOTAL	1	100.00%	100.00%	

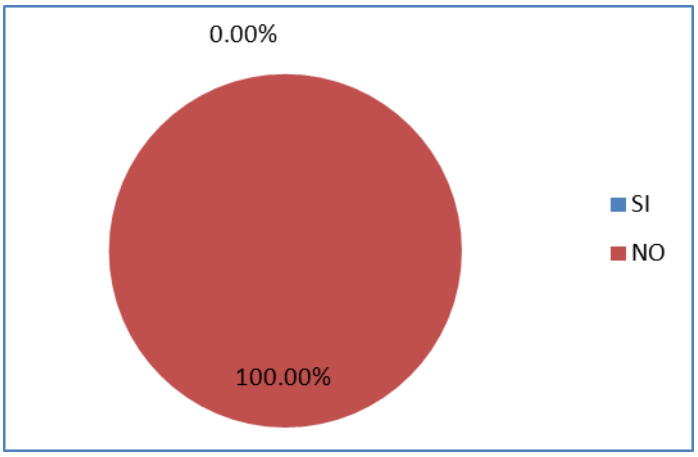


Gráfico Nº 4.11.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo primera pregunta que tiene que ver con Registro de Transacciones, el Jefe del Departamento de Sistemas identificó que no existe un procedimiento por escrito donde se determine la identificación y autentificación de los roles de un nuevo usuario.

Los nuevos registros de usuarios se los realiza pero no se los documenta.

Pregunta N 12

Tabla N. 12 REGISTRO DE TRANSACCIONES : ¿Las contraseñas se asignan de forma automática por el servidor?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	1	100.00%	100.00%	100.00%
TOTAL	1	100.00%	100.00%	

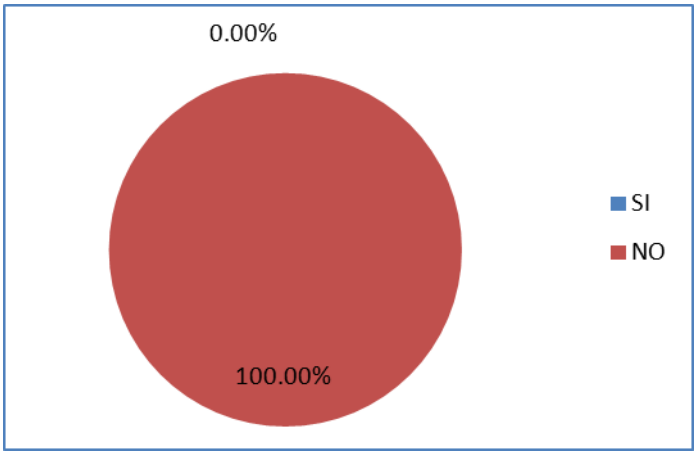


Gráfico Nº 4.12.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo segunda pregunta que tiene que ver con Registro de Transacciones, el Jefe del Departamento de Sistemas indicó que al crear un nuevo usuario se establece la contraseña que el mismo determine, nunca se establece una automáticamente por el servidor.

PREGUNTA N 13

Tabla N. 13 PUBLICACION : ¿Dispone de web site empresarial?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	3	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	3	100.00%	100.00%	

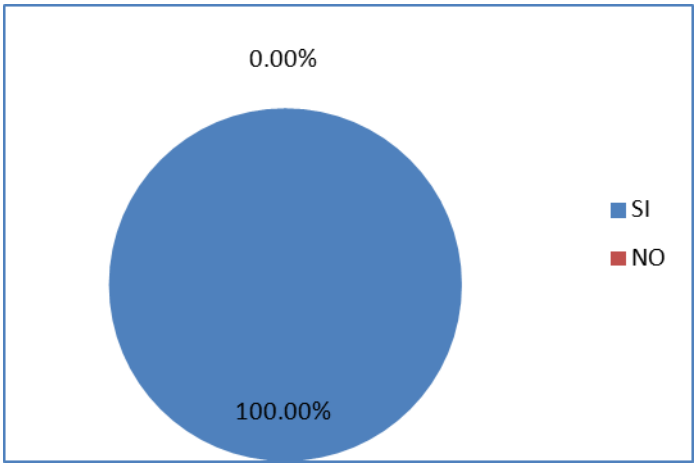


Gráfico Nº 4.13.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo tercera pregunta que tiene que ver con Publicación los usuarios entrevistados indicaron que la empresa posee un web site empresarial

PREGUNTA N 14

Tabla N. 14 SOFTWARE Y DATOS : ¿Existe un procedimiento de copia de seguridad del software y los datos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

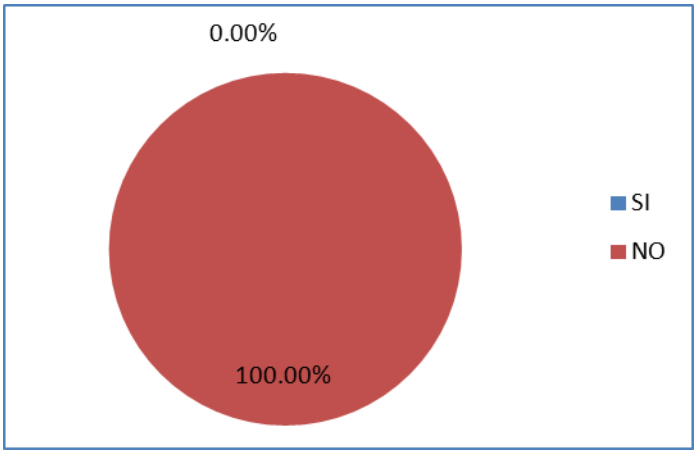


Gráfico Nº 4.14.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo cuarta pregunta que tiene que ver con Software y Datos, los usuarios entrevistados indicaron que la empresa cuenta con un procedimiento tanto de copia de seguridad de los datos del servidor central asi como de los archivos personales de cada estación de trabajo.

PREGUNTA N 15.

Tabla N. 15 SOFTWARE Y DATOS :¿Se almacena alguna copia del software y datos fuera de los locales de la empresa?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

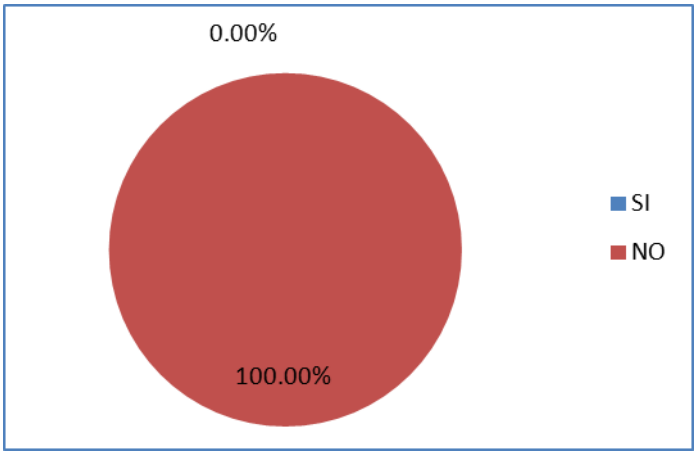


Gráfico Nº 4.15.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo quinta pregunta que tiene que ver con Software y Datos, los usuarios entrevistados indicaron que la empresa no cuenta con una unidad de respaldo fuera de la empresa.

PREGUNTA N. 16

Tabla N. 16 SOFTWARE Y DATOS : ¿Los respaldos de la información se lo realiza en discos duros externos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

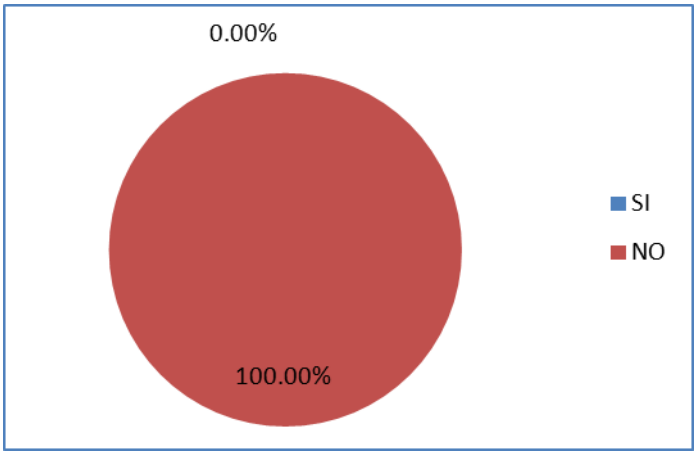


Gráfico Nº 4.16.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo sexta pregunta que tiene que ver con Software y Datos, los usuarios entrevistados indicaron que los respaldos no se sacan en discos duros extrenos sino en un DATA STORGE conectado en red.

PREGUNTA N. 17

Tabla N. 17 SOFTWARE Y DATOS : ¿Existe implementado un servidor espejo como backup?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

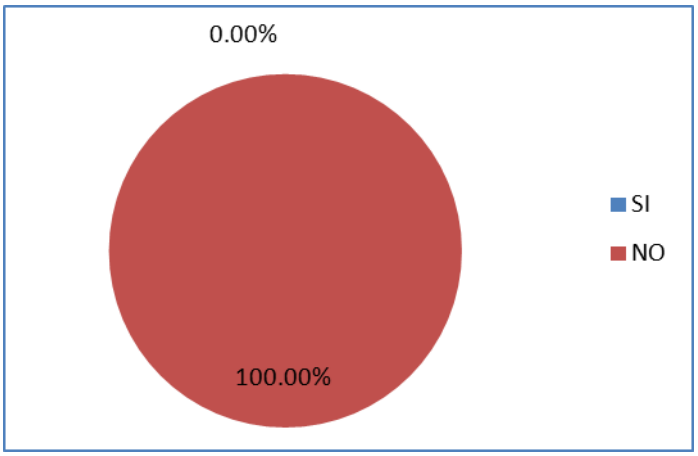


Gráfico Nº 4.17.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo Séptima pregunta que tiene que ver con Software y Datos, los usuarios entrevistados indicaron que todos los servidores que adquiere la empresa tienen implementada el principio de los discos espejo.

PREGUNTA N. 18

Tabla N. 18 SOFTWARE Y DATOS : ¿El servidor cuenta con discos espejo para la redundancia de la información?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

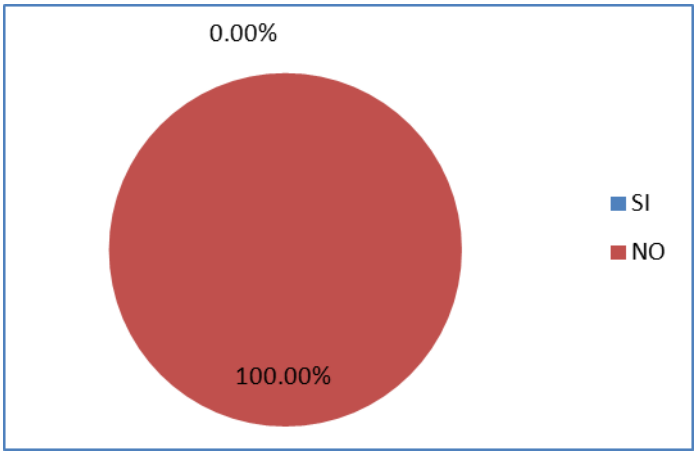


Gráfico Nº 4.18.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo octava pregunta que tiene que ver con Software y Datos, los usuarios entrevistados indicaron como en la pregunta anterior, que el servidor si cuenta con la tecnología del disco espejo, puesto que todos los equipos que se adquieren se lo hace con la tecnología espejo.

PREGUNTA N. 19

Tabla N. 19 NIVELES DE ACCESO : ¿Existen controles de acceso a los usuarios?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	6	40.00%	40.00%	40.00%
NO	9	60.00%	60.00%	100.00%
TOTAL	15	100.00%	100.00%	

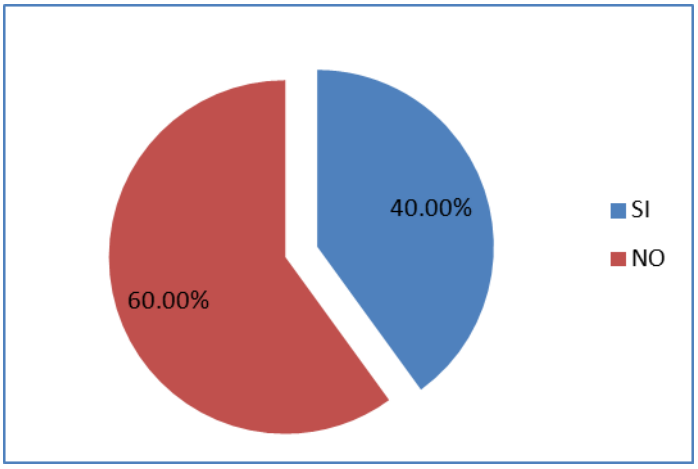


Gráfico Nº 4.19.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la decimo novena pregunta que tiene que ver con Control de acceso, el 60% de los usuarios indica que no se tiene ningún control de acceso a los recursos de la red, mientras que el 40% indica que si se realiza un control sobre los recursos de hardware y software de la empresa.

PREGUNTA N. 20

Tabla N. 20 ROLES DE USUARIO : ¿Al crear un nuevo usuario se le asignan roles?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	2	13.33%	13.33%	13.33%
NO	13	86.67%	86.67%	100.00%
TOTAL	15	100.00%	100.00%	

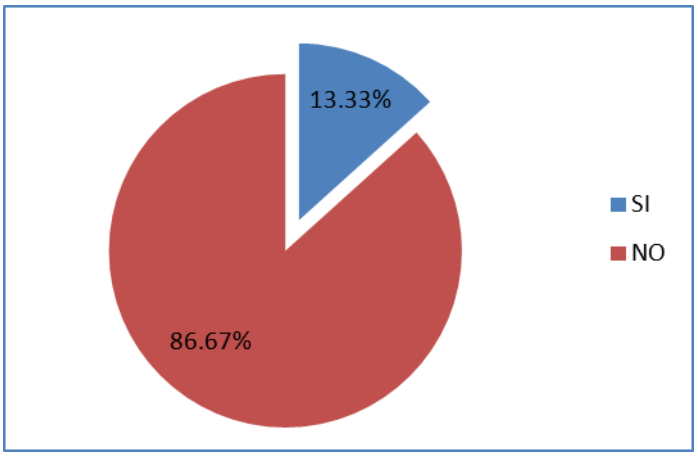


Gráfico Nº 4.20.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima pregunta que tiene que ver con Control de acceso, el 86.67% de los usuarios indica que se le asignan roles, ellos identifican esto porque pueden acceder a impresora, unidades de disco, unidades de red, que otros usuarios no pueden, el 13.33% representa a los usuarios administradores de la empresa que tienen un privilegio total de acceso a los recursos.

PREGUNTA N. 21

Tabla N. 21 ROLES DE USUARIO : ¿Cuándo un usuario nuevo es creado tiene acceso a todos los recursos del servidor?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	12	80.00%	80.00%	80.00%
NO	3	20.00%	20.00%	100.00%
TOTAL	15	100.00%	100.00%	

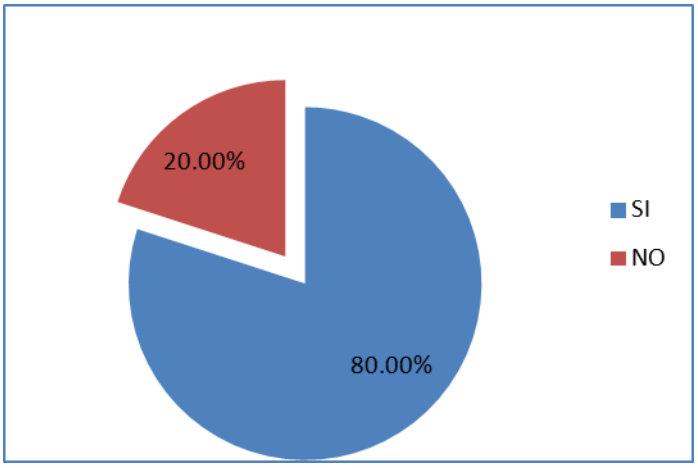


Gráfico Nº 4.21.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima primera pregunta que tiene que ver con Roles de Usuario, el 80% que si puede acceder a los recursos del servidor, es decir al sistema informático, bases de datos, etc, mientras que el 20% tiene acceso limitado a estos servicios.

PREGUNTA N.22

Tabla N. 22 REGISTRO DE TRANSACCIONES : ¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos ?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	1	100.00%	100.00%	100.00%
TOTAL	1	100.00%	100.00%	

Gráfico Nº 4.22.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima segunda pregunta que tiene que ver con Registro de Transacciones, el Jefe del Departamento de Sistema indica que no sabe como revisar el archivo log de transacciones del servidor.

PREGUNTA N. 23

Tabla N. 23 PUBLICACION : ¿Se realiza el mantenimiento por personal de la propia empresa?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	15	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	15	100.00%	100.00%	

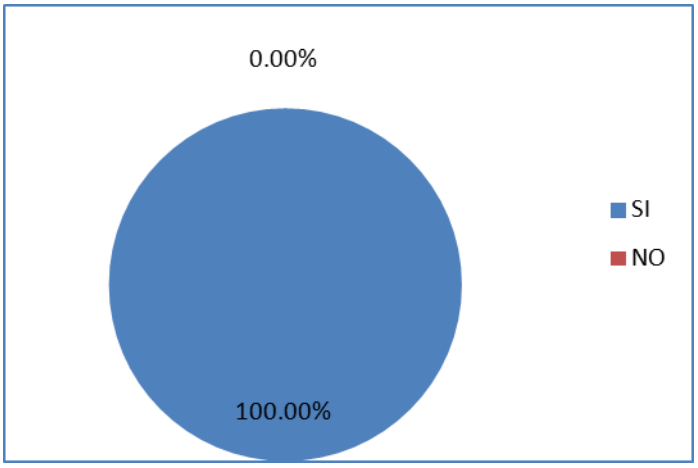


Gráfico Nº 4.23.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima tercera pregunta que tiene que ver con Publicación, el 100% de los encuestados indican que el mantenimiento de los servidores es realizados por personal de la misma empresa

PREGUNTA N. 24

Tabla N. 24 PUBLICACION : ¿Está alojado en la red empresarial el servidor web?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	15	100.00%	100.00%	100.00%
TOTAL	15	100.00%	100.00%	

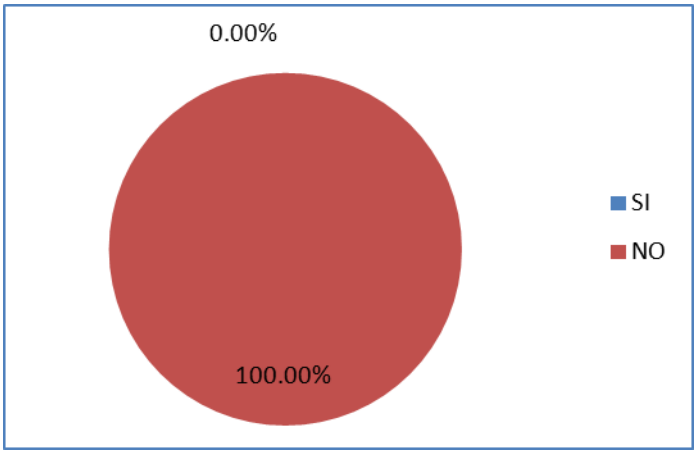


Gráfico Nº 4.24.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima cuarta pregunta que tiene que ver con Publicación, el 100% de los encuestados indican que el sitio web está alojado en un servidor externo.

PREGUNTA N. 25

Tabla N. 25 PUBLICACION : ¿Se ha contratado personal informático para que diseñe las aplicaciones?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	15	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	15	100.00%	100.00%	

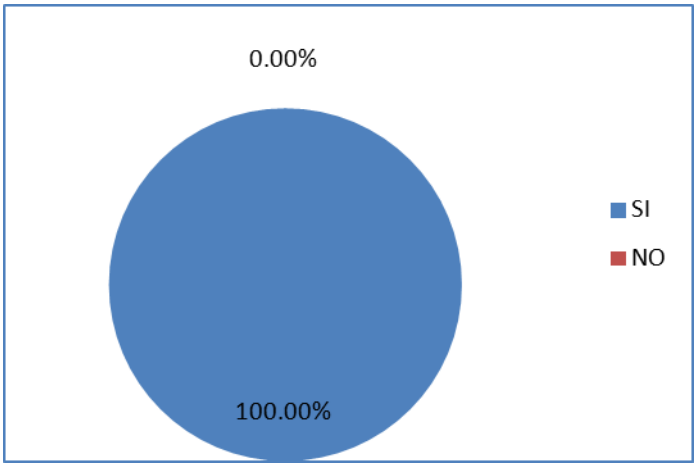


Gráfico Nº 4.25.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima quinta pregunta que tiene que ver con Publicación, el 100% de los encuestados testifican que las aplicaciones web y forms son desarrolladas por el personal del área informática de la empresa

PREGUNTA N. 26

Tabla N. 26 SEGURIDAD : ¿Se dispone de cortafuegos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	7	46.67%	46.67%	46.67%
NO	8	53.33%	53.33%	100.00%
TOTAL	15	100.00%	100.00%	

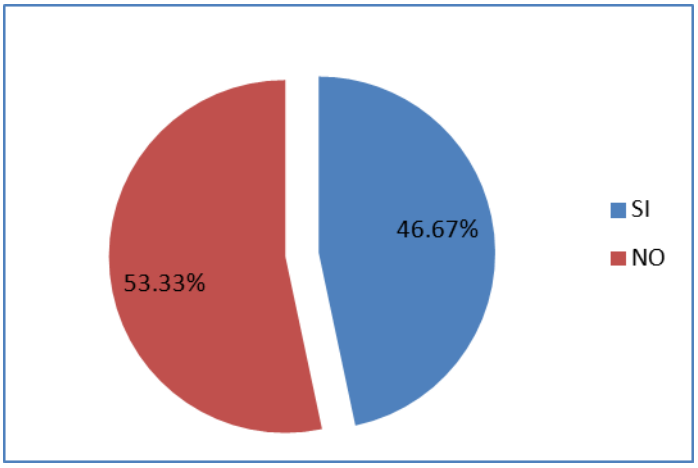


Gráfico Nº 4.26.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima sexta pregunta que tiene que ver con Seguridad, el 53.33% de los encuestados indican que no poseen un firewall activo o instalado en sus equipos, mientras que el 46.67% afirman que si, vale aclarar que el este porcentaje se encuentran los firewalls de los servidores, donde si se cuenta con este servicio.

PREGUNTA N. 27

Tabla N. 27 SEGURIDAD : ¿Dispone de herramientas que auditen intentos de accesos externos?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	0.00%
NO	1	100.00%	100.00%	100.00%
TOTAL	1	100.00%	100.00%	

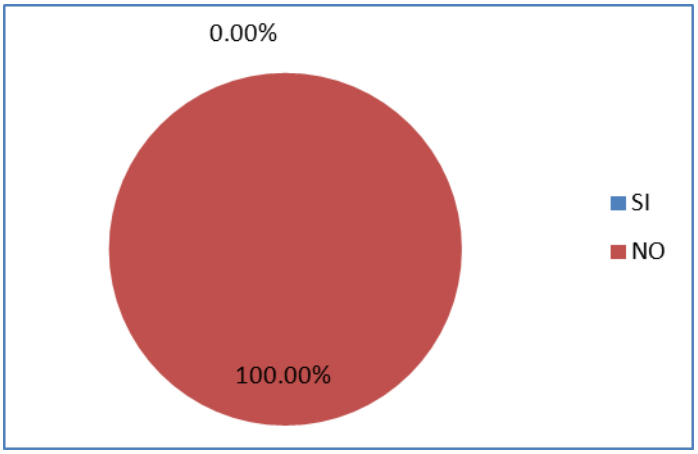


Gráfico Nº 4.27.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima séptima pregunta que tiene que ver con Seguridad, el Jefe del Departamento de Sistemas indica que no se cuentan con herramientas que auditen los intentos de acceso externos a la red empresarial.

PREGUNTA N. 28

Tabla N. 28 SEGURIDAD : ¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	9	60.00%	60.00%	60.00%
NO	6	40.00%	40.00%	100.00%
TOTAL	15	100.00%	100.00%	

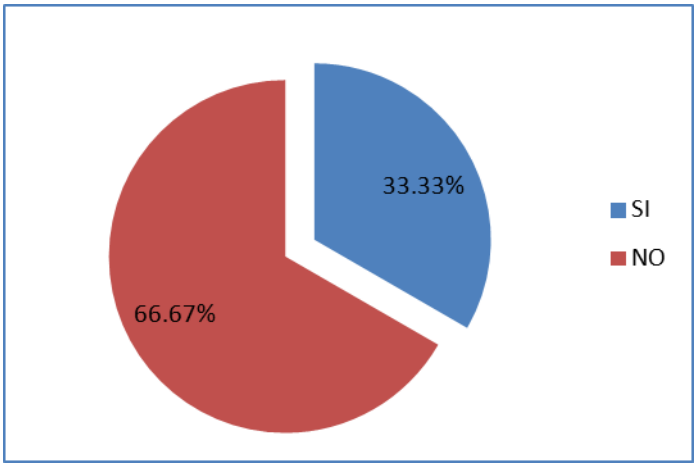


Gráfico Nº 4.28.

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésima octava pregunta que tiene que ver con Seguridad, el 66.67% de los encuestados indican que si se cuenta con estas herramientas, mientras que el 33.33% de los mismos indican que no.

PREGUNTA N. 29

NIVELES DE ACCESO : ¿Están los servidores protegidos en cuanto a inicios
Tabla N. 29. de sesión y acceso a través de la red?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	1	100.00%	100.00%	

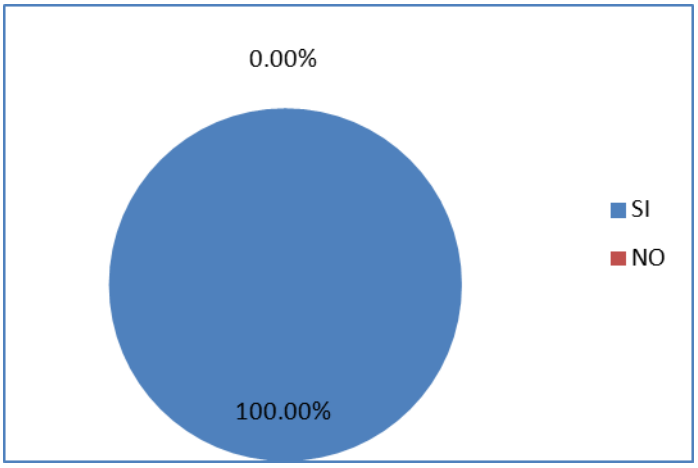


Gráfico Nº 4.29.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la vigésimo novena pregunta que tiene que ver con Niveles de acceso, el Jefe del Departamento de Sistemas indica que los servidores están protegidos con las respectivas contraseñas de seguridad de acceso ante cualquier elemento externo que pretenda acceder a los recursos de la misma.

PREGUNTA N. 30

Tabla N. 30 NIVELES DE ACCESO : ¿Cuenta Turbotech con niveles de acceso a los usuarios?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	100.00%	100.00%	100.00%
NO	0	0.00%	0.00%	100.00%
TOTAL	1	100.00%	100.00%	

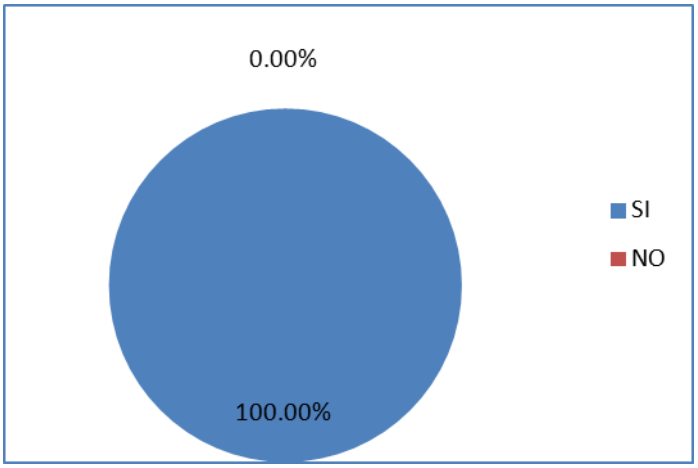


Gráfico Nº 4.30.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésima pregunta que tiene que ver con Niveles de acceso, el Jefe del Departamento de Sistemas indica que se especifican los niveles de acceso a los usuarios cuando se crea una nueva cuenta, de esta manera los recursos están protegidos ante cualquier ataque no deseado.

PREGUNTA N. 31

Tabla 31. PERMISOS : ¿El servidor otorga direcciones IP automática a los usuarios validados?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	0	0.00%	0.00%	00.00%
NO	1	100.00%	100.00%	100.00%
TOTAL	1	100.00%	100.00%	

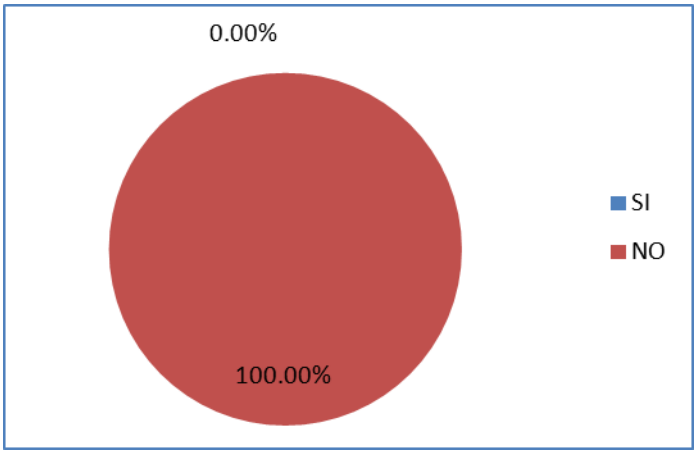


Gráfico Nº 4.31.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésima primera pregunta que tiene que ver con Permisos, el Jefe del Departamento de Sistemas indica que no se cuenta con un servidor DHPC que otorgue direcciones automática, indica que

PREGUNTA 32

Tabla N. 32 PERMISOS : ¿Conoce acerca de los niveles de acceso a los servidores web?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	6.67%	6.67%	6.67%
NO	14	93.33%	93.33%	100.00%
TOTAL	15	100.00%	100.00%	

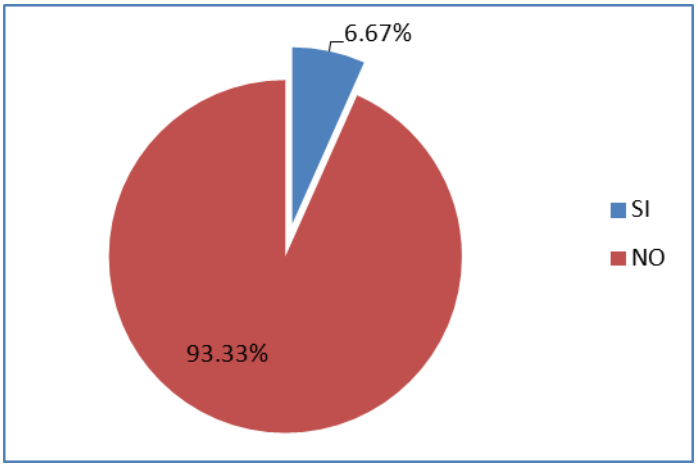


Gráfico Nº 4.32.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo segunda pregunta los usuarios no conocen acerca de las seguridades de los servidores web.

PREGUNTA 33.

Tabla N. 33 ATAQUES : ¿Tiene conocimiento del concepto de acceso a nivel del sistema?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	6.67%	6.67%	6.67%
NO	14	93.33%	93.33%	100.00%
TOTAL	15	100.00%	100.00%	

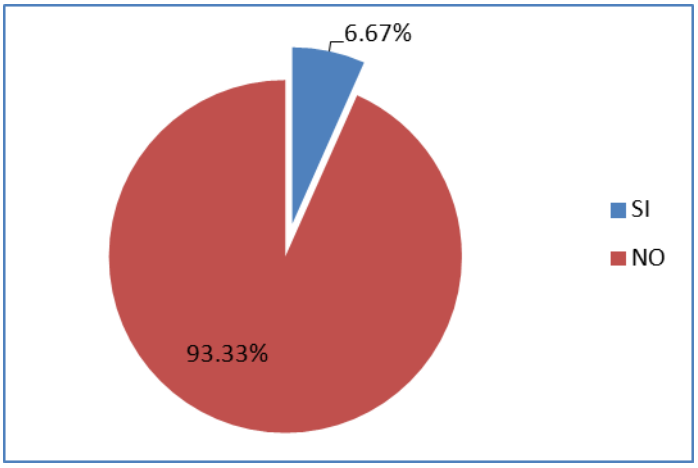


Gráfico Nº 4.33.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo tercera pregunta un 93.33% de usuarios no conocen acerca de los niveles de acceso al sistema, o bien tienen un concepto básico de este principio.

PREGUNTA 34.

Tabla N. 34 ATAQUES : ¿Tiene conocimiento del concepto de acceso a nivel de aplicación?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	6.67%	6.67%	6.67%
NO	14	93.33%	93.33%	100.00%
TOTAL	15	100.00%	100.00%	

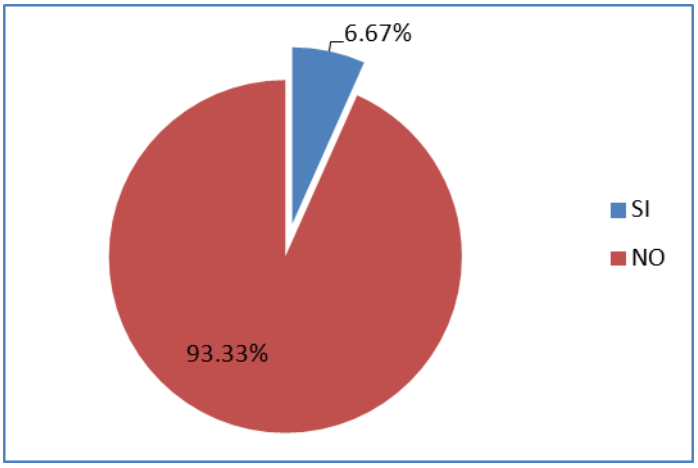


Gráfico Nº 4.35.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo cuarta pregunta un 93.33% de usuarios igual que en la anterior pregunta, conocen acerca de los niveles de acceso a las aplicaciones, o bien tienen un concepto básico de este tema.

PREGUNTA 35.

Tabla N. 35 ATAQUES : ¿Se asignan los permisos para el acceso a la aplicación web de la empresa?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	12	80.00%	80.00%	80.00%
NO	3	20.00%	20.00%	100.00%
TOTAL	15	100.00%	100.00%	

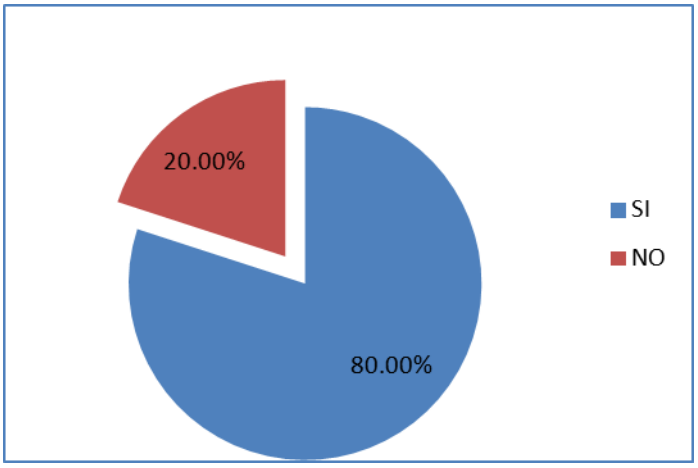


Gráfico Nº 4.35.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo cuarta pregunta un 93.33% de usuarios igual que en la anterior pregunta, conocen acerca de los niveles de acceso a las aplicaciones, o bien tienen un concepto básico de este tema.

PREGUNTA 36.

Tabla N. 36 ATAQUES : ¿Conoce acerca de los ataques a nivel de Internet?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	5	33.33%	33.33%	33.33%
NO	10	66.67%	66.67%	100.00%
TOTAL	15	100.00%	100.00%	

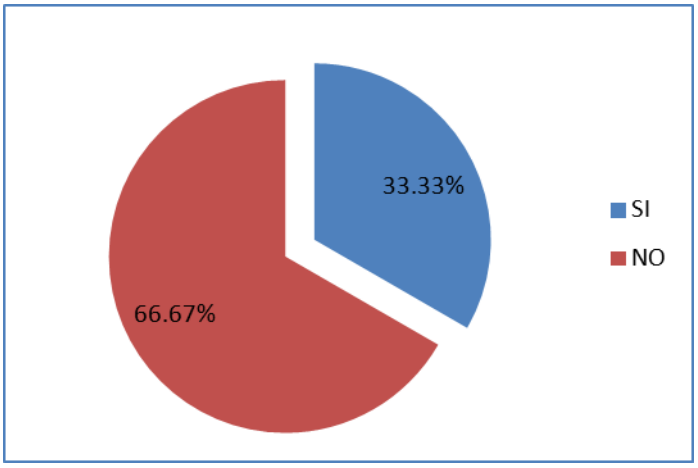


Gráfico Nº 4.36.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo sexta pregunta un 66.67% de usuarios tiene un conocimiento bastante aceptable del concepto de ataques de internet

PREGUNTA 37.

Tabla N. 37 ATAQUES : ¿Sabe lo que es un hacker?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	4	26.67%	26.67%	26.67%
NO	11	73.33%	73.33%	100.00%
TOTAL	15	100.00%	100.00%	

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo séptima pregunta un 73.33% de encuestados sabe lo que es un hacker.

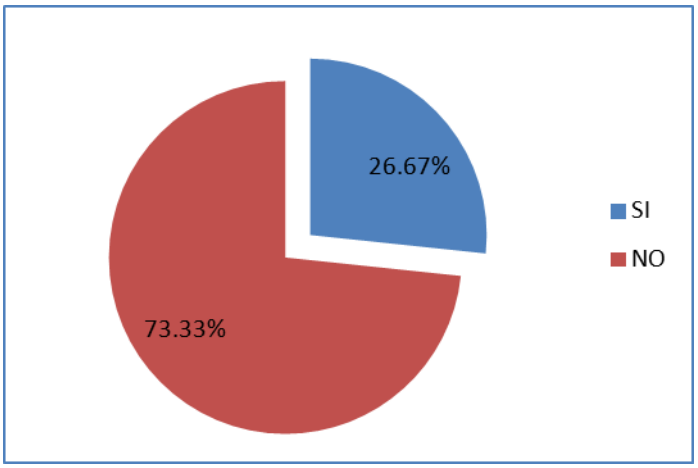


Gráfico Nº 4.37.

PREGUNTA 38.

Tabla N. 38 ATAQUES : ¿Conoce lo que es pishing?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	2	13.33%	13.33%	13.33%
NO	13	86.67%	86.67%	100.00%
TOTAL	15	100.00%	100.00%	

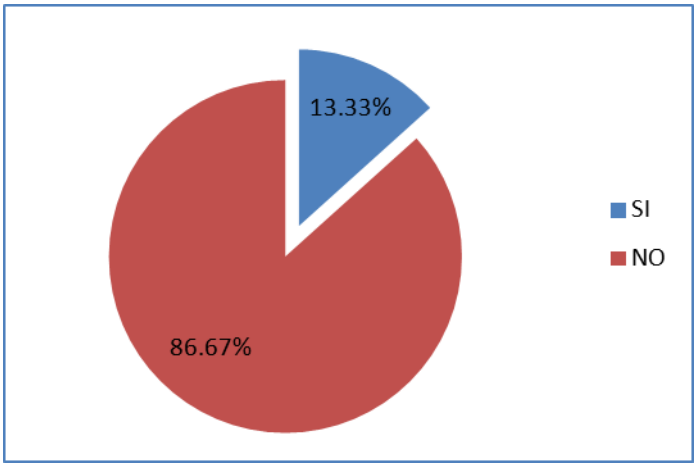


Gráfico Nº 4.38.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo octava pregunta un 87% de encuestados tiene conocimiento de lo que es pishing, esto se debe a que todos los usuarios recibieron una capacitación por parte de la entidad bancaria que administra las cuentas de los empleados, y en ella se dio un capítulo de seguridades en el manejo de las cuentas bancarias privadas, haciendo énfasis en el pishing.

PREGUNTA 39

Tabla N. 39 ATAQUES : ¿Existen un plan de contingencia ante un ataque externo?

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
SI	1	6.67%	6.67%	6.67%
NO	14	93.33%	93.33%	100.00%
TOTAL	15	100.00%	100.00%	

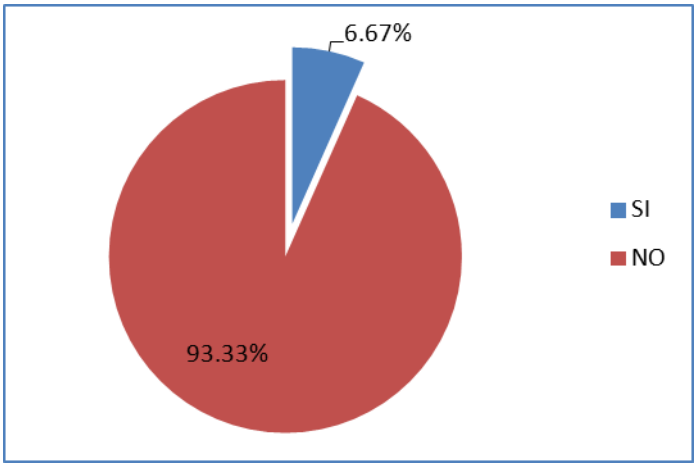


Gráfico Nº 4.39.

Fuente: Encuestas

Elaborado por: José Fabián Enríquez Miranda

Análisis e Interpretación

En la trigésimo novena pregunta un 93% de encuestados conoce que el Departamento de Sistemas ha preparado un plan de contingencia ante ataques externos.

VERIFICACIÓN DE HIPÓTESIS

Formulación de la hipótesis

H_0= Hipótesis nula

H_1 = Hipótesis alterna

H_0= La aplicación de políticas de seguridad informática **NO** minimizaran la vulnerabilidad de los entornos web en la empresa Turbotech

H_1 = La aplicación de políticas de seguridad informática **SI** minimizaran la vulnerabilidad de los entornos web en la empresa Turbotech

Definición del nivel de significación

El nivel de significación escogido para la investigación es del 5%.

Elección de la prueba estadística

Para la verificación de la hipótesis se escogió la prueba Ji Cuadrada, cuya fórmula es la siguiente:

$$\mathbf{X^2} = \frac{\Sigma\ (fo - fe)^2}{fe}$$

Simbología

Fo = Frecuencia observada

Fe = Frecuencia esperada

Para realizar la matriz de tabulación cruzada se toma en cuenta 2 preguntas del cuestionario como se muestra a continuación:

Pregunta Nº 10

¿Existen políticas de grupo aplicables para el acceso a la información?

2 NO
1 SI

Pregunta Nº 28

¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?

2 NO
1 SI

Zona de aceptación o rechazo

Grados de libertad

(gl) = (F-1) (C-1)

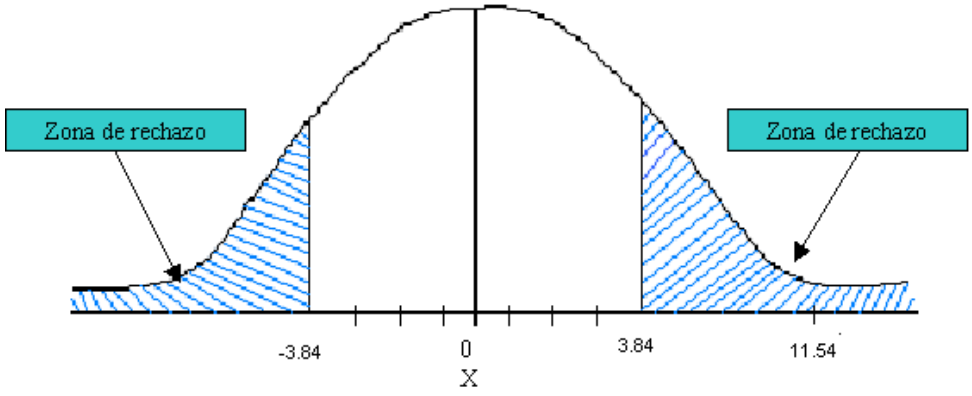
(gl) = (2-1) (2-1)

(gl) = (1) (1)

(gl) = 1

Nivel de significación = 5%

El valor tabulado de x^2 con 1 grado de libertad y un nivel de significación de 0.05 es de 3.84.



Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda

VALORES	ALTERNATIVAS		
ALTERNATIVAS	SI	NO	TOTAL
Políticas de Grupo Aplicables	8	7	15
Sistemas Operativos que impiden acceso	9	6	15
TOTAL	17	13	

Tabla 4.1.Valor Tabulado Ji Cuadrado

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda.

$$fe = \frac{(Total\ o\ marginal\ de\ renglon)(total\ o\ marginal\ de\ columna)}{N}$$

FRECUENCIA ESPERADA	ALTERNATIVAS	
ALTERNATIVAS	SI	NO
Políticas de Grupo Aplicables	8,5	6,5
Sistemas Operativos que impiden acceso	8,5	6,5

Tabla 4.2.Frecuencia Esperada

Fuente: Encuesta

Elaborado por: José Fabián Enríquez Miranda..

Una vez obtenidas las frecuencias esperadas, se aplica la siguiente fórmula:

Cálculo matemático

$$X^2 = \sum \frac{(O-E)^2}{E}$$

	O	E	O-E	$(O-E)^2$	$(O-E)^2/E$
Politicas de Seguridad / SI	3,00	8,50	-5,50	30,25	3,56
Politicas de Seguridad / NO	12,00	6,50	5,50	30,25	4,65
Politicas de Seguridad / SI	5,00	8,50	-3,50	12,25	1,44
Politicas de Seguridad / NO	10,00	6,50	3,50	12,25	1,88
				X^2	**11,54**

Tabla 4.3.Cáculo Matemático

Fuente: Encuesta

Elaborado por: José Fabían Enríquez Miranda.

Decisión

El valor de $X^2_t = 3.84 < X^2_C = 11.54$

La aplicación de políticas de seguridad informática minimizará la vulnerabilidad de los entornos web en la empresa Turbotech.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se evidenció que la empresa Turbotech no cuenta con procedimientos de seguridades físicas del Área Administrativa
- Se comprobó que las instalaciones físicas de la empresa Turbotech no son adecuadas ni seguras para la protección del Servidor Web de la empresa
- Se evidenció que no existe ningún control de acceso a los servidores.
- Se concluyó que no se ha instalado ninguna herramienta informática para el control de acceso a usuarios desde internet.
- Se evidenció que Turbotech no conoce ni aplica los principios de la Norma ISO 27001 en la seguridad de su información.

Recomendaciones

- Determinar un procedimiento para establecer las seguridades físicas del Área Administrativa de Turbotech, haciendo énfasis en el área física del Servidor Web.
- Reestructurar físicamente las instalaciones del Área Administrativa de Turbotech en el área del Servidor Web para mantener la seguridad física del mismo.
- Determinar una política de control de acceso lógico al Servidor Web de Turbotech, a través de procedimientos para la creación de usuarios, roles y transacciones.
- Instalar y configurar las herramientas informáticas necesarias en el Servidor Web de Turbotech para control de accesos y control de ataques y vulnerabilidades al que el Servidor puede estar expuesto.

- Establecer los procedimientos de seguridad informática apegados a los principios de la Norma ISO 27001.

CAPITULO VI
PROPUESTA

DATOS INFORMATIVOS

Nombre de la Empresa:	Turbotech
Provincia:	Tungurahua
Cantón:	Ambato
Dirección:	Av, Los Pericos y Pasaje Los Mirlos
Teléfono:	032 853 904
Beneficiarios:	Accionistas del empresa.
Tiempo Estimado:	Durante 3 años

Equipo Técnico Responsable:

- ✓ Gerente General de la empresa Turbotech
- ✓ Presidente de la empresa Turbotech
- ✓ Accionistas de la empresa Turbotech

Tema

POLITICAS DE SEGURIDAD INFORMÁTICA PARA REDUCIR LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010

Antecedentes de la propuesta

El presente trabajo surge como una necesidad de la empresa Turbotech, de contar con políticas de seguridad que permitan tener a salvo el activo fundamental de la empresa : sus datos.

La Administración o Gestión basada en Web es la aplicación de la tecnología World Wide Web a redes, que pretende aprovechar la amplia difusión de los navegadores como interfaz de usuario universal, para utilizarlos como interfaz para las aplicaciones de gestión.

El principal beneficio de los mecanismos de Gestión basados en Web es que los desarrolladores de aplicaciones no tienen por qué conocer los detalles de los protocolos de gestión para manejar dispositivos remotos. Adicionalmente esto permite abstraer los diferentes protocolos y unificarlos con una única visión.

Este trabajo plantea establecer políticas de seguridad para evitar que la gestión de los aplicativos web sea vulnerable a un ataque externo de un hacker, de esta manera los datos y aplicativos de la empresa Turbotech se verán seguros, y el acceso de los usuarios será validado a través del servidor de una forma confiable y eficiente.

Justificación

Asegurar los datos involucra algo más que conectarse en un firewall con una interface competente. Lo que se necesita es un plan comprensivo de defensa. Y se necesita comunicar este plan en una manera que pueda ser significativo para la gerencia y usuarios finales.

Esto requiere educación y capacitación, conjuntamente con la explicación, claramente detallada, de las consecuencias de las violaciones. La política puede incluir instalar un firewall, pero no necesariamente se debe diseñar su política de seguridad alrededor de las limitaciones del firewall.

Elaborar la política de seguridad no es una tarea innecesaria. Ello no solamente requiere que el personal técnico comprenda todas las vulnerabilidades que están involucradas, también requiere que ellos se comuniquen efectivamente con la gerencia.

La gerencia debe decidir finalmente cuánto de riesgo debe ser tomado con el activo de la empresa, y cuánto se debería gastar en ambos, en dólares e inconvenientes, a fin de minimizar los riesgos.

Es responsabilidad del personal técnico asegurar que la gerencia comprenda las implicaciones de añadir acceso a la red y a las aplicaciones sobre la red, de tal manera que la gerencia tenga la suficiente información para la toma de decisiones.

Si la política de seguridad no viene desde el inicio, será difícil imponer incluso medidas de seguridad mínimas. Es mejor trabajar con estos temas antes de tiempo y poner la política por escrito.

El desarrollo de una política de seguridad sobre entornos web, comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo, implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos, y el desarrollo de una política de uso. Debe crearse un procedimiento de auditoria que revise el uso de la red y sobre todo de los servidores web de forma periódica.

Objetivos

General

Plantear la definición de un procedimiento de políticas de seguridad informática para los entornos web de la empresa Tubotech.

Específicos

- Construir un procedimiento de políticas de seguridad informática para los entornos Web de la empresa Tubotech.
- Sugerir la reestructura física del Área de Servidores de la empresa Turbotech.
- Determinar las respectivas políticas de acceso Lógico para el control del servidor Web de Turbotech.

- Evaluar constantemente el procedimiento para realizar las mejoras respectivas conforme se requieran.

Análisis de Factibilidad.

Política Sociocultural.

La sociedad demanda que las empresas, mantengan la información confidencial resguardada, debido a que los clientes que realizan compras de algún determinado producto, bien o servicio, desean mantener su información personal y de las transacciones que realizan en completo resguardo.

La proliferación de los delitos informáticos a hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.
Pero lo importante es que un procedimiento de políticas implementadas para mantener la seguridad de los datos críticos de la empresa, crearán un nivel de confianza en los usuarios de los sistemas web de Turbotech, entonces el uso de estos servicios se incrementa y permite que los datos de consulta y transacciones estén disponibles en la web con todo nivel de seguridad.

Tecnológica.

La empresa Turbotech está implementando proyectos de mejora continua al Departamento de Sistemas, dotándole de equipos tecnológicos que ayuden a un mejor desempeño en las diferentes funciones que se realizan.

Al contar esta empresa privada con equipos de última tecnología para el cumplimiento de las funciones, se pueden implementar proyectos de una manera eficiente y en el menor tiempo, para el crecimiento tecnológico de esta institución.

Las lista de equipos que la empresa actualmente posee es la siguiente:

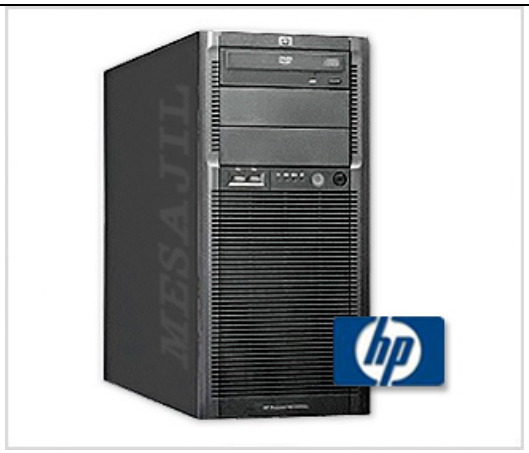
EQUIPO	FOTOGRAFIA	CARACTERÍSTICAS
Servidor HP Proliant ML150 Series (Web Server)		-Procesador Intel Xeon Quad Core E5504 de 2GHz -Soporta hasta dos procesadores -Dos GB (1 X 2GB) de memoria DDR3 PC3-10600 -Controlador Smart Array P410 (RAID 0, 1, 0+1) -Lector de DVD de media altura -NIC Gigabit Ethernet HP NC107i -Factor de forma: tower 5U
Servidor HP Proliant ML110 Series (Proxy Server)		Intel® Xeon® E5500 series processors up to 2.53 GHz (5.86 GT/s QPI) DDR3 memory architecture Integrated Lights Out remote management HP SIM support PCI-Express Gen 2 TPM 1.2 module sup

Tabla 6.1. Equipos Informáticos de Turbotech

Organizacional

Turbotech está debidamente organizada en diferentes departamentos, al contar con una Política Institucional, además de estar regida por las leyes tributarias y de la Superintendencia de Compañías de la República, se puede establecer que está debidamente organizada en función de un desempeño óptimo.

A continuación se presenta el organigrama estructural de la empresa:

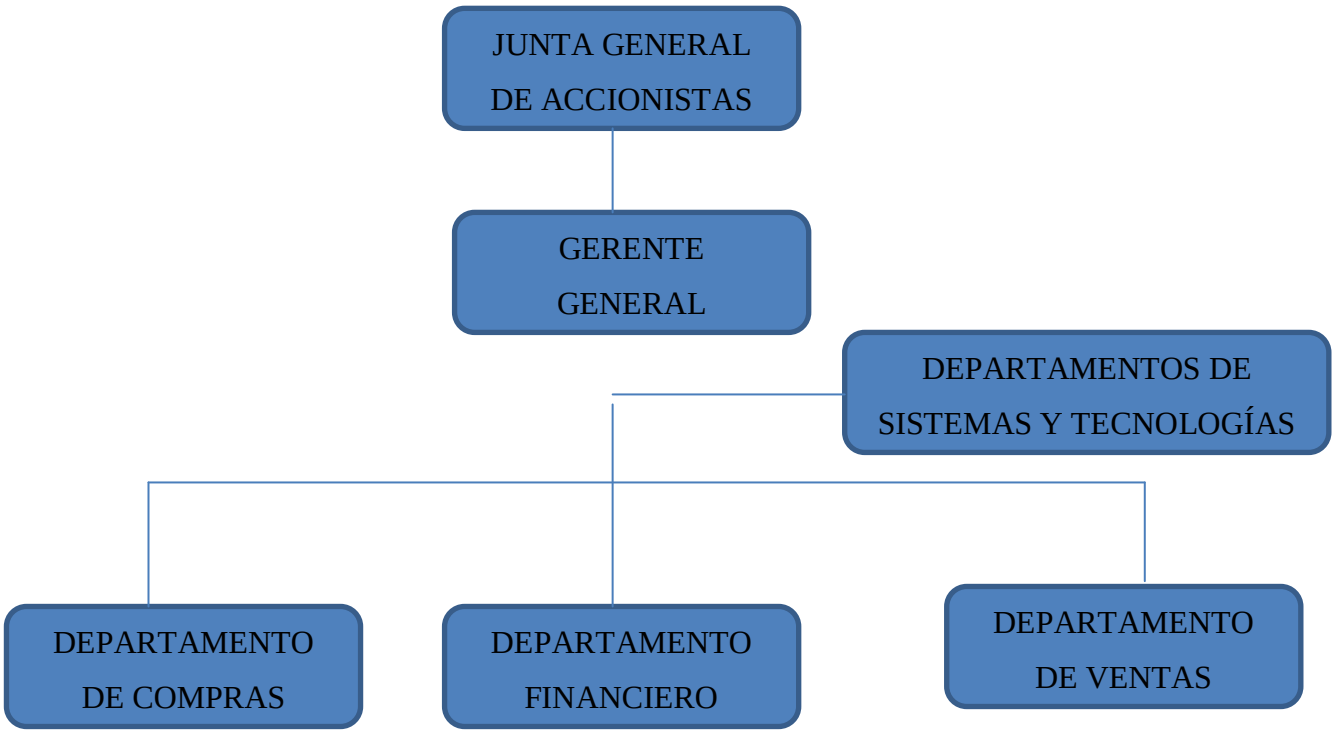


Grafico 6.1. Organigrama Estructural

Equidad de Género

Esta propuesta está dirigida a hombres y mujeres que se determinen en el manejo del área informática y que están en igualdad de condiciones legales, intelectuales y que serán los beneficiarios directos en la construcción del manual de procedimiento de las Políticas de Seguridad Informática para entornos Web.

Ambiental

Esta propuesta al ser de carácter tecnológico repercute directamente en un ambiente positivo de trabajo, tomando en cuenta que al ser los altos directivos y empleados los beneficiarios, se va a mejorar las seguridades de la entidad y por lo tanto la confianza en el trabajo.

Económica Financiera

La empresa Turbotech cuenta con un presupuesto para cada uno de los proyectos que emprende, el Departamento Informático, tiene asignado un presupuesto para proyectos de desarrollo encaminados a mejorar el servicio tecnológico al personal administrativo. Este financiamiento consta en el Presupuesto Anual de la empresa.

Legal

Turbotech al estar legalmente constituida por un Directorio de Accionistas, avalados por las leyes de la Superintendencia de Compañías, y al contar con una auditoria externa, posee un control legal donde rigen las leyes tributarias, de compañías, de seguridad social, etc que controlan la seriedad de esta entidad y por lo tanto de los Departamentos que la componen, estando dentro de este selecto grupo el Área Informática y sus proyectos establecidos.

Fundamentación Científico-Técnica

Metodología

En este trabajo se empleó una modalidad de investigación orientada tanto al aspecto cuantitativo como al cualitativo, por cuanto se asume una realidad estable. Esto

permitirá establecer políticas de seguridad adaptadas a los requerimientos de la sociedad actual.

El diseño del esquema de políticas de seguridad debe constar en todo plan estratégico y como tal la empresa Turbotech, tiene su Plan Estratégico.

Identificación de la vulnerabilidad	Actividad Correctiva
Vulnerabilidad Física de las oficinas de Sistemas	Propuesta de esquema de seguridad Física de las oficinas
Identificación de Sistemas de Control de Incendio en la empresa	Propuesta de esquema de implementación de un sistema anti-incendios del área administrativa
Identificación de la vulnerabilidad lógica de los sistemas operativos servidor.	Propuesta de esquema de seguridad Lógica de los Sistemas Operativos.
Identificación de Posibles ataques a la seguridad de Datos y Aplicativos	Implementación de herramientas de seguridad de software.

Tabla 6.2. Planificación Estratégica

MODELO OPERATIVO

Diagnóstico de la situación anterior de Turbotech

Antigua Área Física del Departamento Administrativo de la Empresa

Turbotech al ser una empresa pionera en la importación de Turbocargadores al mercado ecuatoriano, se ha expandido de una forma exponencial en los últimos cinco años, poniendo a sus directivos en una carrera tecnológica y física de crecimiento acelerado en sus instalaciones; donde el espacio de trabajo es uno de los principales

problemas de la organización y por ende, la ubicación de la empresa hace emergente la necesidad de dotar ante todo de seguridades que permitan salvaguardar no solo los activos informáticos de la empresa, sino la integridad de toda la infraestructura administrativa.

La ubicación de Turbotech en Ambato es la calle Los Pericos y Pasaje Los Mirlos Sector Oriente de la ciudad, el área física de la empresa en la ciudad es la siguiente:

6.2. Toma Satelital de las Instalaciones de Turbotech(cortesía Google Maps)

En este sitio podemos ver que el techado de las instalaciones muestra cierta inseguridad sobre todo en el área administrativa donde se ubicaba el servidor web.

El servidor web se encontraba en un área del edificio demasiado vulnerable del ataque físico de cualquier persona, además de encontrarse en un área de mucho tránsito de usuarios que pasaban a realizar sus reclamos o compras en el taller de servicio.

Este plano muestra con mayor detalle la situación de la empresa:

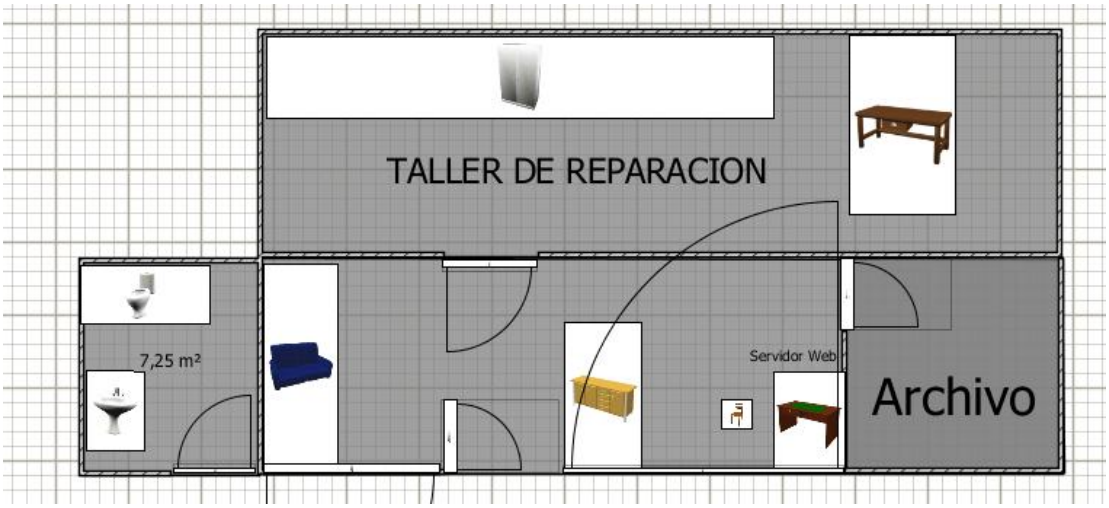


Gráfico 6.3. Plano del Área administrativa de Turbotech

Donde podemos determinar que el sitio físico del servidor Web no es el más adecuado.

Una vista de como lucían las oficinas en una planimetría de tres dimensiones es la siguiente:

Gráfico 6.4. Plano 3d de las antiguas instalaciones de Turbotech

Problemática de la Seguridad Lógica de Turbotech

La empresa presentó un gravísimo problema de falta de seguridad lógica en la validación de usuarios en el servidor web como en el servidor de datos.
No se tenía una política clara de creación de accesos a los servidores principales de la empresa, ya que la carga del sistema operativo siempre estuvo relegada a una empresa de venta de computadores, quienes sin esquema de seguridad creaban los usuarios sin códigos de acceso, incluyendo la deficiencia de que los servidores contaban con Sistemas Operativos Windows XP Home Edition, que son vulnerables a cualquier ataque.

Por este análisis de la situación actual de Tubotech, se procedió a crear la siguiente Guía de Implementación de Políticas de Seguridad, que permitieron a Turbotech corregir sus graves deficiencias en el Área de Transferencia de Tecnologías.

GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

Presentación

Durante los últimos años los servidores web se han convertido en una excelente fuente de diversión para piratas: cualquier empresa que se precie, desde las más pequeñas a las grandes multinacionales, tiene una página web en las que al menos trata de vender su imagen corporativa. Si hace unos años un pirata que quisiera atacar a una empresa se las tenía que ingeniar para obtener primero información de la misma y después buscar errores de configuración más o menos comunes de sus sistemas, hoy en día le basta con teclear el nombre de su objetivo en un navegador y añadir la extensión “.com” detrás del mismo para contactar con al menos una de sus máquinas: su servidor web.

Las políticas de seguridad informática para entonos web de la empresa Turbotech, buscan de una manera adecuada, proteger los recursos más valiosos de esta entidad que son los datos informáticos, que constituyen los activos mas preciados de esta y de cualquier empresa.

Puesto que en la empresa está tomando su accionar en el campo informático las transacciones on line van a ser la primordial fuente de comunicación y de comercio.

Considerando además que los principales directivos como son el Gerente y Presidente de Turbotech, realizan viajes al exterior para concretar los negocios de la empresa, y requieren conectarse a los servicios web de la empresa, por lo tanto la importancia de establecer seguridades en los datos de Turbotech son la principal idea del establecimientos de estas políticas.

Este conjunto de políticas informáticas presentadas en el siguiente manual indican los pasos a seguir para que el personal del área informática de la empresa tenga un lineamiento establecido de lo que deben hacer para implementarlas y mantenerlas.

DISEÑO DEL ESQUEMA DE SEGURIDAD

DISEÑO DE LA SEGURIDAD FÍSICA

Para realizar el diseño de seguridad tanto Física como Lógica y para el manual de políticas y procedimientos se siguieron los lineamientos de la norma ISO 27001.
Los objetivos de la seguridad física:
Proteger los activos de la empresa Turbotech, de los riesgos de desastres naturales y/o actos accidentales o mal intencionados.
Minimizar la pérdida de información y garantizar la recuperación de la misma.

Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

Área Seguras

Objetivo Principal: Proteger físicamente contra el acceso no autorizado o daño a la información de los sistemas web de Turbotech especialmente donde se procesan datos sensibles.

Perímetro Físico

El área de los servidores debe ser cerrada desde el piso real hasta el techo real contando con una ventilación adecuada y sus respectivas instalaciones eléctricas, donde el acceso solo será para las personas autorizadas tales como administradores de las aplicaciones, bases de datos y red

El departamento de Sistemas junto con el departamento Administrativo deberá crear normas a seguir para acceder y modificar al hardware. Cada empleado será responsable de sus computadores personales y no se permitirá que personas no autorizadas a los sistemas de información tengan acceso a los computadores sin autorización.

Controles de acceso físico

Toda persona externa que ingrese a la empresa por motivos específicos y/o autorizados deberá registrar su información en un documento: nombre, hora de ingreso, departamento al que se dirige

La información sensible como: respaldos de datos y códigos fuentes de los sistemas de información desarrollados en Turbotech será almacenada en un lugar de condiciones ambientales adecuadas, lejos de canalizaciones de agua y energía, se utilizara una caja fuerte y su acceso solo será permitido por las personas autorizadas en este caso al departamento de sistemas y al Gerente de la empresa.

Protección de oficinas

Se debe instalar un sistema de detección de intrusos en todas las puertas y ventanas accesibles y que será activado después de cerrar los departamentos. Las áreas donde se procesan datos el departamento de Sistemas, no deben ser accesibles al público todo el tiempo.

El área donde se almacena la información sensible, deberá estar ubicado en un lugar que no este expuesto al acceso público. El departamento de Sistemas debe tener un sistema de detección de incendios mediante el esquema de CO2 (véase Anexo 3)

SEGURIDAD DE LOS SERVIDORES

Objetivo Principal: Proteger físicamente a los, Servidores tanto web como aplicativos y Servidor Proxy, para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Empresa

Ubicación y protección de los Servidores

En el departamento de sistemas los servidores deberán ser ubicados en lugares que no afecten al mismo, por ejemplo no cerca de ventanas donde puedan ser afectados por la lluvia, polvo o por robo.

Turbotech pondrá políticas sobre comer, beber o fumar cerca de las instalaciones de los Servidores especialmente en el área de procesamiento de información.

Se deberá realizar por los menos dos veces al año un monitoreo de las condiciones ambientales en el área de servidores especialmente en el de procesamiento de datos para prevenir cualquier problema en los servidores.

Suministros de Energía

El área de los servidores debe contar con un UPS para asegurar el trabajo continuo hasta que el generador de energía sea activado.

Seguridad del Cableado

El cableado de red debe estar protegido por conductos como canaletas y ubicados en lugares que no obstruyan el paso a las personas para evitar daños al cable y que se vean interrumpidos los servicios de red.
Las instalaciones de cableado eléctrico deberá ser independiente del cableado de red para evitar interferencias.

Seguridad en Redes Inalámbricas

La información de configuración de los routers inalámbricos, debe ser almacenada en un formato que indique, El nombre asignado al router, la ubicación física en la empresa, la dirección IP asignada, nombre de Usuario y Contraseña, además la clave asignada será una palabra constituidas por letras, números y por lo menos un signo de puntuación.
Además estas claves no deben relacionarse con el Departamento donde está ubicado el router inalámbrico.

Mantenimiento de Servidores

El departamento de Sistemas, debe contar con un plan de mantenimiento preventivo de servidores que será calendarizado, para evitar que el trabajo se vea interrumpido por falla de algún hardware del Servidor y que exista pérdida de información.
El departamento de Sistemas, llevara una bitácora de daños mas frecuentes en los equipos para estar prevenidos de futuros problemas con los mismos.

El departamento de sistemas deberá contar con un sistema de backups distribuidos para asegurar la información sensitiva de los usuarios finales replicando los backups entre el servidor principal y un servidor backup es decir, replicar los datos del servidor principal de archivos a otro secundario y éste deberá contar con las seguridades respectivas para los servidores.

Baja o reutilización de Servidores

Si un servidor debe ser sustituido por otro se deberá formatear y configurar nuevamente para el nuevo usuario después de sacar los respaldos respectivos, con el fin de que no exista información del antiguo dueño.

ESQUEMA PLANIMÉTRICO DE LAS SEGURIDADES FÍSICAS IMPLEMENTADAS

El esquema de Seguridad Física de Turbotech en el área administrativa, se ha establecido de la siguiente manera:

Gráfico 6.5. Plano en 3D de la nueva distribución del Área administrativa de Turbotech

6.6. Plano del Área Administrativa de Turbotech.

Nótese que el área de Servidores de la empresa posee actualmente la seguridad de los parámetros descritos anteriormente.

DISEÑO DE SEGURIDAD LÓGICA

La Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.”

Consideremos que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso al o los servidores de la empresa Turbotech
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizado los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, y sobre los sistemas de aplicación

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no

autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

Para lo cual se ha determinado el siguiente procedimiento, a tomarse en cuenta para el control de acceso:

Identificación y Autentificación

La técnica que permitirá realizar la autenticación de la identidad del usuario, serán un nombre de Usuario y Contraseña, el nombre de usuarios será constituido por la primera letra del nombre en mayúsculas y a continuación el apellido en minúsculas.

El password del servidor estará constituido por letras, números y por lo menos un signo de puntuación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la empresa.

3. Se harán revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas se encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

4. Las revisiones se orientarán a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, se analizarán las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

5. Detección de actividades no autorizadas. Además se realizarán auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudarán a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

6. Para las consideraciones relacionadas con cambios en la asignación de funciones del empleado, en el caso de rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algún empleado, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

7. En el caso de despidos del personal de sistemas se presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la empresa, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Roles

El acceso a la información también se controlará a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, jefe departamental, usuario común, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Transacciones

También se implementa controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
Creación: permite al usuario crear nuevos archivos, registros o campos.
Búsqueda: permite listar los archivos de un directorio determinado.
Todas las anteriores.

Ubicación y Horario

El acceso a determinados recursos del sistema estará basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles

permitirán limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantendrá un control más restringido de los usuarios y zonas de ingreso.

Control de Acceso Interno

Listas de Control de Accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido.

Límites sobre la interface de Usuarios

Esto límites, generalmente, serán utilizados en conjunto con las listas de control de accesos y restringirán a los usuarios a funciones específicas. Básicamente serán de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre el aplicativo web de usuario.

Control de Acceso Externo

Firewalls o Puertas de Seguridad

Bloqueará o filtrar el acceso entre el servidor Web y el Servidor proxy, cumpliendo con la función de muro en primera instancia hacia la intranet.

Accesos de Personal contratado o Consultores

En el caso del personal que preste servicios temporarios en la empresa, se creará un perfil de acceso restringido como Usuarios Standart con limitación en el acceso a los servicios.

En el caso de requerir un acceso al sistema web de Turbotech, se creará en la base de datos un usuario con perfil de solo lectura para evitar modificaciones, de la información.

Administración de Personal y Usuarios

Niveles de Seguridad de Usuarios

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.
Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

Nivel D.

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS–DOS y System 7.0 de Macintosh.

Nivel C1: Protección Discrecional

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "super usuario"; quien tiene gran responsabilidad en la seguridad del 2 Orange Book. Department Of Defense. Library N° S225, 711. EEUU. 1985. http://www.doe.gov
mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

Nivel C2: Nivel de Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la

capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Nivel B1: Seguridad Etiquetada

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

Nivel B2: Seguridad Estructurada

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

Nivel B3: Dominios de Seguridad

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido
Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Nivel A: Protección Verificada

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

AUDITORIA Y CUANTIFICACIÓN DE LAS VULNERABILIDADES WEB

HERRAMIENTA ACUNETIX WEB VULNERABILITY SCANNER

Esta aplicación identifica primeramente los servidores web y, a continuación, rastrea todo el sitio para recopilar información acerca de los archivos.

Acunetix Web Vulnerability Scanner primero identifica los servidores web de un particular IP o intervalo. Después de eso, rastrea todo el sitio, reúne información sobre cada archivo que encuentra y muestra la estructura de todo el sitio Web. Después de esta etapa de descubrimiento, realiza una auditoría automática para los problemas de seguridad comunes. Acunetix Web Vulnerability Scanner es un software que detecta automáticamente la inserción de archivos.

El Port Scanner y las alertas de red nos permiten realizar un análisis de puerto contra el servidor web donde se ejecuta el sitio Web escaneado. Cuando se encuentran puertos abiertos, Acunetix WVS llevará a cabo complejas comprobaciones de seguridad a nivel de red contra el servicio de red que se ejecuta en ese puerto, como pruebas de recursión a las DNS abiertas, pruebas a servidores proxy mal

configurados, a las cadenas de comunidad SNMP débiles y muchos otros controles de seguridad a nivel de red.

Inyección SQL es uno de los muchos mecanismos de ataque de web utilizados por los piratas informáticos para robar datos de organizaciones. Quizá es una de las técnicas de ataque de aplicaciones más comunes usadas hoy en día. Es el tipo de ataque que aprovecha una codificación incorrecta de las aplicaciones web y permiten al pirata informático inyectar comandos SQL en un formulario de inicio de sesión para que puedan acceder a los datos de tu base de datos.

En esencia, inyección SQL surge porque los campos disponibles para los datos proporcionados por el usuario permiten instrucciones SQL para pasar y consultar la base de datos directamente.

Las aplicaciones web permiten a los visitantes del sitio Web legítimo presentar y recuperar datos desde una base de datos por Internet usando su navegador preferido. Las bases de datos son fundamentales para los sitios Web modernos – almacenan datos necesarios para que los sitios Web ofrezcan un contenido específico a los visitantes y procesa información a los clientes, proveedores, empleados y un host para las partes interesadas. Las credenciales de usuario, financieras y la información de pago, las estadísticas de la compañía, todas pueden residir dentro de una base de datos y ser accesada por los usuarios legítimos a través de aplicaciones web estándar y personalizados. Las aplicaciones Web y las bases de datos permiten ejecutar regularmente tu negocio.

Inyección SQL es la técnica de pirateo que intenta pasar comandos SQL (instrucciones) a través de una aplicación web para la ejecución de la base de datos por back-end. Si no se limpian correctamente, las aplicaciones web pueden provocar ataques de inyección SQL que permiten a los piratas informáticos ver la información de la base de datos o incluso erradicarla.

Características tales como páginas de inicio de sesión, soportes y formularios de solicitud de los productos, formas de comentarios, las páginas de búsqueda, compras de carros y la entrega general de contenido dinámico, forma moderna de sitios Web proporcionarán a las empresas los medios necesarios para comunicarse con los clientes y los posibles clientes. Estas características del sitio Web son ejemplos de aplicaciones web que pueden ser comprados diseñados para estas aplicaciones o desarrollados como programas a medida.

Estas características del sitio Web son todas susceptibles a los ataques de inyección SQL que surgen debido a que los campos disponibles para los datos proporcionados por el usuario permiten pasar directamente instrucciones SQL y consultar la base de datos.

La tecnología de AcuSensor de Acunetix es una nueva tecnología de seguridad que nos permite identificar vulnerabilidades más que un escáner de aplicación Web tradicional, mientras que genera menos falsos positivos. Además indica exactamente donde está la vulnerabilidad del código. La mayor precisión se consigue mediante la combinación de la técnica del escaneo caja negra con una exploración del código dinámico mientras el código fuente está siendo ejecutado.

Las ventajas de utilizar la tecnología de AcuSensor de Acunetix:

Permite localizar y corregir la vulnerabilidad más rápido debido a la capacidad de proporcionar más información acerca de la vulnerabilidad, tales como número de línea del código fuente, seguimiento de las pilas, la consulta SQL afectada, etc.
·Significativamente se pueden reducir los falsos positivos al analizar un sitio Web porque podemos internamente comprender mejor el comportamiento de la aplicación web.

Puede alertar de problemas de configuración de aplicación web que podrían dar lugar a una aplicación vulnerable o exponer los detalles de la aplicación interna. Por ejemplo, si 'errores personalizados' están habilitados en. NET, esto podría exponer detalles sensibles de la aplicación a un usuario malintencionado.
Detecta muchas más vulnerabilidades de inyección SQL. Anteriormente sólo podría encontrar vulnerabilidades de inyección de SQL si se informaba de errores de la base de datos o a través de otras técnicas comunes.

Capacidad para detectar las vulnerabilidades de inyección SQL en todas las instrucciones SQL, incluyendo en declaraciones SQL INSERT. Con un escáner de caja negra no pueden encontrarse dichas vulnerabilidades de inyecciones SQL.
Capacidad de saber acerca de todos los archivos presentes y accesibles a través del servidor web. Si un atacante obtiene el acceso al sitio Web y crea un archivo de puerta trasera en el directorio de la aplicación, el archivo será encontrado, se analizará cuando se utiliza la tecnología AcuSensor y se te avisará.

La tecnología AcuSensor es capaz de interceptar todas las entradas de una aplicación web y construye una lista completa de todas las posibles entradas en el sitio Web y las prueba.

No hay necesidad de escribir la dirección URL con sus reglas al análisis de las aplicaciones web que utilizan un motor de búsquedas URL amigables! Mediante la tecnología de AcuSensor el escaneador es capaz de volver a escribir direcciones URL SEO sobre la marcha.

Capacidad para probar las vulnerabilidades de creación y eliminación del archivo arbitrario. Por ejemplo, a través de una escritura vulnerable malintencionada el usuario puede crear un archivo en el directorio de la aplicación web y ejecutarlo para que tenga acceso privilegiado o para que elimine archivos importantes de la aplicación web.

Capacidad para probar las inyecciones del correo electrónico. Por ejemplo, un usuario malintencionado puede anexar información adicional tal como una lista o algunos destinatarios o información adicional al cuerpo del mensaje para enviarlo bajo un formulario web o a un gran número de destinatarios como spam de forma anónima.

Estas son algunas de las características clave de "Acunetix Web Vulnerability Scanner":

Acunetix Web Vulnerability Scanner detecta automáticamente las siguientes vulnerabilidades en las aplicaciones web:

Intersecciones de las encriptaciones de un sitio web.

Inyección SQL.

Inyección de CRLF.

Ejecución de códigos.

Directorio transversal.

Inserción de archivo.

Divulgación del código fuente de la secuencia de comandos.

Descubre archivos/directorios que pueden contener información confidencial.

Busca archivos comunes (como registros, trazas de aplicación, repositorios CVS web), copia de archivos o directorios.

Encuentra listados de directorios.

Descubre directorios con permisos débiles.

Descubre las tecnologías de los servidores web disponibles (por ejemplo, WebDAV, FrontPage, etc.).

Determina si hay métodos peligrosos HTTP habilitados en el servidor web (por ejemplo, PUT, TRACE, DELETE).

Inspecciona los banners de versión HTTP y busca productos vulnerables.

Prueba de la longitud de las contraseñas de las aplicaciones.

Ataques largos:

Con Acunetix Web Vulnerability Scanner, puedes construir las peticiones HTTP/HTTPS y analizar las respuestas del editor HTTP.

Espía de las conexiones:

Permitiéndote iniciar la sesión, interceptar y modificar todo el tráfico HTTP/HTTPS, Acunetix Web Vulnerability Scanner te ofrece una visión detallada de los datos que está enviando la aplicación web.

Longitud de la contraseña de prueba:

Para probar la fuerza de tus contraseñas, puedes realizar un ataque de diccionario sobre la HTTP básica, NTLM o autenticación basada en formularios.

Editor de la base de datos de las pruebas:

Acunetix Web Vulnerability Scanner incluye un editor de la base de datos de texto que te permite agregar ataques adicionales a la base de datos de prueba (sólo para versiones Enterprise y Asesor).

Es compatible con todas las tecnologías web importantes:

Utilizando CGI, PHP, ASP, ASP.NET todas pueden ser probadas para las vulnerabilidades.

Perfiles de exploración:

Acunetix Web Vulnerability Scanner te permite examinar rápidamente sitios con distintas opciones e identidades.

Informes:

Podremos guardar sesiones de análisis a las bases de datos MS SQL Server y Access y generar informes complejos sobre las anteriores sesiones de análisis usando información almacenada en la base de datos.

HERRAMIENTA WAPITI

Wapiti es un escáner de vulnerabilidades para aplicaciones web, licenciado bajo la GPL v2 , que busca fallos XSS, inyecciones SQL y XPath, inclusiones de archivos (local y remota), ejecución de comandos, inyecciones LDAP, inyecciones CRLF, para que pongamos a prueba la seguridad de nuestras aplicaciones web y podamos corregirlas.

El listado de vulnerabilidades detectadas es el siguiente:
Errores en el Manejo de Archivos (Inclusión remota o local usando include/require, fopen, readfile…)
Inyecciones en Bases de Datos (Soporta PHP/JSP/ASP e inyecciones SQL y XPath)
XSS (Cross Site Scripting)
Inyecciones LDAP
Ejecución de Comandos (eval(), system(), passtru()…)
Inyeccione CRLF (HTTP Response Splitting, session fixation…)

HERRAMIENTA SECURITY GUARDIAN

Una manera de buscar las vulnerabilidades a los que está expuesto un sitio web es a través del siguiente sitio:
http://www.security-guardian.com/
Una de las medidas para precautelar la seguridad de los entornos web, es la aplicación de la herramienta Security Guardian, que certificará nuestro sitio web como seguro, en base a los siguientes pasos:

1. Registro
2. Auditoría: Security Guardian verifica la identidad, datos de contacto, privacidad, protección de datos y la seguridad del Website.
3. Resultado Certificación: Si una empresa viene certificada por security Guardian, el sello de seguridad vendrá actualizado con la fecha de obtención de la certificación de seguridad y confianza para Websites.
4. Incremente las ventas online y la confianza aplicando el certificado de seguridad y confianza para Websites de Security Guardian.

Proceso de Security Guardian

Antes de realizar una auditoría de seguridad web y de vulnerabilidad informática, todo el mundo dice que su sitio Web es seguro, pero nadie lo sabe. **Security Guardian** proporciona a las empresas una forma fácil de asegurar su portal y notificarlo a sus clientes.
Después de contratar el servicio de **Security Guardian**, se efectúa un proceso de verificación con el fin de comprobar la información de su empresa. Vamos a verificar la dirección de su empresa, número de identificación fiscal, privacidad y protección de datos, número de teléfono de asistencia técnica y dirección de correo electrónico, los números de teléfono de su oficina principal, de atención al cliente y del gerente que represente su empresa (esta información se mantendrá en privado).

Este proceso de verificación asegurará que su empresa esté claramente identificada y que usted es quien dice ser para proporcionar a sus clientes o visitantes la garantía que el portal Web es lícito, identificado y autenticado.
Se dará acceso inmediato a la consola de administración e instrucciones claras sobre la forma de aplicar la certificación de seguridad para entornos Web de **Security Guardian** en su página.
El nombre de dominio de su sitio o dirección IP será necesario para comenzar a realizar las pruebas de intrusiones. Se analiza automáticamente el domino o servicio Web a certificarse con periodicidad diaria, semanal o mensual (dependiendo de la versión contratada). Tan pronto como se haya completado el escaneo de vulnerabilidad, usted será capaz de examinar los informes y ver si hay problemas que debe resolver.

Escáner de vulnerabilidades

El escáner de **Security Guardian** es un programa diseñado para buscar y detectar puntos débiles que afecten el portal auditado, consultándose una base de datos de vulnerabilidades conocidas con más de 30000 vulnerabilidades.
En el caso que no se detecte ninguna vulnerabilidad crítica, mostrará el sello de certificación de portal Web seguro (indicando la exploración efectuada, el logotipo de nuestra compañía y la fecha del escaneo) en su sitio.
El escaneo de vulnerabilidades de **Security Guardian**, ejecutará una amplia gama de pruebas para comprobar la seguridad de su Web como SQL Injection, Cross Site Scripting(XSS), HTTP Smuggling, HTTP splitting, Buffer Overflow, Format string, HTTP Methods, Server Side Including (SSI), CGIs, Trasversal Path, Directory Listing, etc. Todas estas pruebas son completamente transparentes para su sitio Web analizado y se le proporcionará un informe detallado con el tipo y el número de vulnerabilidades encontradas en su sitio Web.

Resultados de Escaneo de Vulnerabilidades

Security Guardian muestra los resultados del análisis en el área de administración. Allí es posible apreciar dos interfaces principales. La primera muestra el resultado de una exploración específica y de un dominio específico.

La segunda interfaz le permitirá seleccionar cualquiera de sus dominios que se está escaneando periódicamente y el grupo de las vulnerabilidades en función de su carácter crítico.

Éstas serán listadas y aparecerá un informe completo acerca de cualquiera de las vulnerabilidades detectadas.

Cada informe indicará, entre otras informaciones, el tipo de exploración solicitada, la respuesta recibida y una explicación acerca de la vulnerabilidad que se ha detectado, así como indicaciones de cómo resolver estas incidencias y su potencial impacto.

CASO PRÁCTICO

CONFIGURACIÓN DE SEGURIDAD EN LOS SERVIDORES

Elección del Sistema Operativo a Ejecutarse en los Servidores

Dentro de los estudios realizados en la empresa, luego de un análisis exhaustivo de los diversos sistemas operativos a instalarse en el servidor central y servidor proxy de Turbotech, se ha determinado, que el sistema operativo de estos equipos es Windows Server 2003, esta decisión, se tomó en cuenta por la factibilidad económica y la alta difusión de este sistema operativo en el mercado.

Se consideró dentro de las posibilidades también a Linux en su distribución Fedora, pero, se descartó esta posibilidad debido a que los profesionales que manejan este sistema operativo son escasos en el mercado y sobre todo el costo y la dificultad para la gerencia al conseguir un profesional que domine una distribución Linux es complicado, por lo tanto Windows es la mejor opción.

Instalación y configuración de Microsoft Windows Server 2003 en el Servidor Web

Podremos instalar Microsoft Windows 2003 Server (en adelante w2k3) de las siguientes formas:

• Manualmente, desde una unidad de CD-Rom o de Red compartida.

• Mediante un archivo de respuestas y la unidad de CD-Rom o de Red compartida.

• Utilizando Sysprep y algún programa de creación de imágenes, para crear una "imagen" de una instalación, que pueda implantarse mediante una unidad de CD-Rom o de Red compartida.

• Automatizada durante el inicio del sistema desde la Red con RIS (Remote Installation Services).

• Actualización del sistema operativo, mediante las características de instalación/mantenimiento de software con las directivas de grupo (Group Policy's Software Installation and Maintenance, Intellimirror) o con SMS (Microsoft Systems Management Server).

- Vamos a tener el equipo desconectado de internet.
- La partición será NTFS.
- La contraseña debe ser segura.
- Es interesante definir contraseña de acceso a la BIOS del equipo.

Política de contraseñas en el Servidor .

Se debe establecer la política de contraseñas para exigir contraseñas complejas, que contienen una combinación de letras mayúsculas y minúsculas, números y símbolos, y son típicamente un mínimo de seis caracteres o más para todas las cuentas, incluidas las cuentas administrativas, como el administrador local, de dominio administrador y administrador de la empresa.
De esta manera, cuando los usuarios requieran de un nuevo nombre de usuario y contraseña, la política de contraseñas determina si reúne los requisitos de complejidad establecidos.

Las contraseñas serán creadas por el Administrador de sistemas el cual registrará los nombres de usuario y contraseñas en base al siguiente formato:

Tipo de Usuario: Administrador____, Usuario Estandard____

Nombre de Usuario: _____

Contraseña : _____

Nombres:

_____

Apellidos:

_____

Departamento al que pertenece: _____

Correo electrónico:

_____

Fecha de Creación:_____

Autorizo al Administrador del área informática a utilizar los datos antes descritos, como fuentes de información en el caso de realizarse una auditoría informática.

_____

Firma

Administrador de Sistemas. Gerente General

Grafico 6.7. Formato de Creación de Usuarios

Implementación del Servidor Proxy

De manera similar al Servidor Web, el servidor Proxy correrá sobre una plataforma Windows Server 2003, donde se creará el siguiente nombre de Usuario y contraseña :

Nombre de Usuario : Administrator
Contraseña : %tbtech2010

En este sistema operativo se instalará el sofware SpoonProxy, como sistema de servidor proxy.

Características de Spoon Proxy

SpoonProxy es un completo servidor proxy que puede conectar varios ordenadores a Internet a la vez. Está especialmente diseñado para consumir pocos recursos y es fácil de configurar.

Este proxy soporta una amplia variedad de clientes que abarcan todas las funciones de Internet, entre ellos navegadores web, clientes de e-mail, mensajería instantánea, juegos en red y mucho más.

El programa incluye un asistente para configurar todos los servicios y permite establecer nombres de usuario y contraseñas para cada máquina conectada. Soporta UDP y SOCKS5.

El interfaz de SpoonProxy permite controlar las conexiones realizadas y el tráfico en bytes. Además se puede administrar remotamente, incluso desde un PC fuera de la red.

Instalación de Spoon Proxy

Realmente no hay ningún tipo de configuración necesarios para las operaciones básicas de proxy.. SpoonProxy se debe instalar en el servidor que tiene una conexión directa a Internet para que otros usuarios de la LAN puedan acceder a Internet a través del proxy. SpoonProxy funciona con cualquier tipo de conexión a Internet

Configuración del Servidor Web para el acceso al Servidor Proxy

Para el acceso al internet del Servidor Web vamos a seguir los siguientes pasos:
En el menú Herramientas, seleccione Opciones de Internet en la ficha Conexiones, que le llevará a la siguiente pantalla.

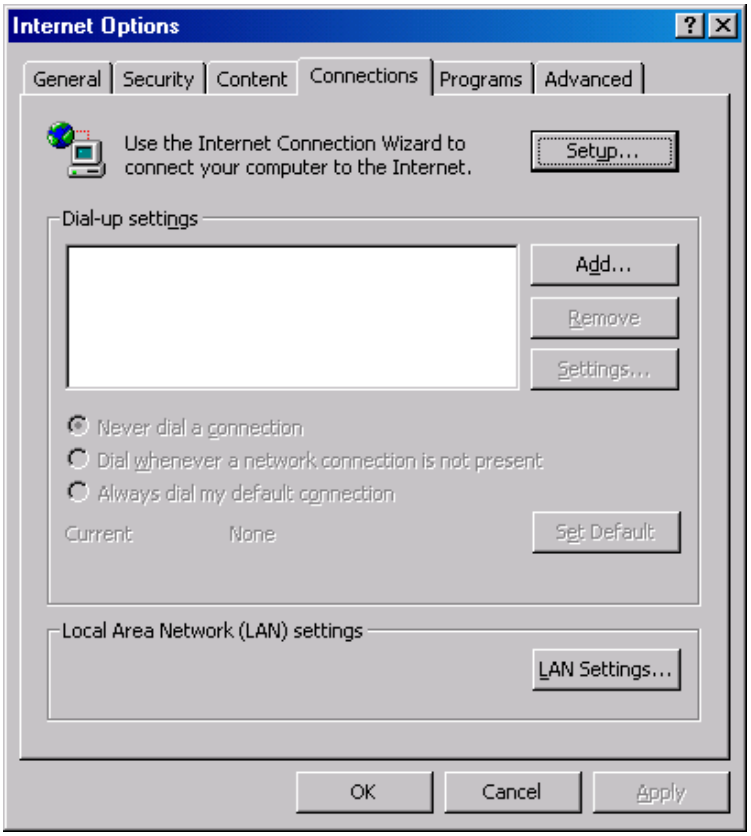


Grafico 6.8. Configuracion del Servidor Web para el acceso al Servidor Proxy

Haga clic en el botón Configuración de LAN, que le llevará a la siguiente pantalla.

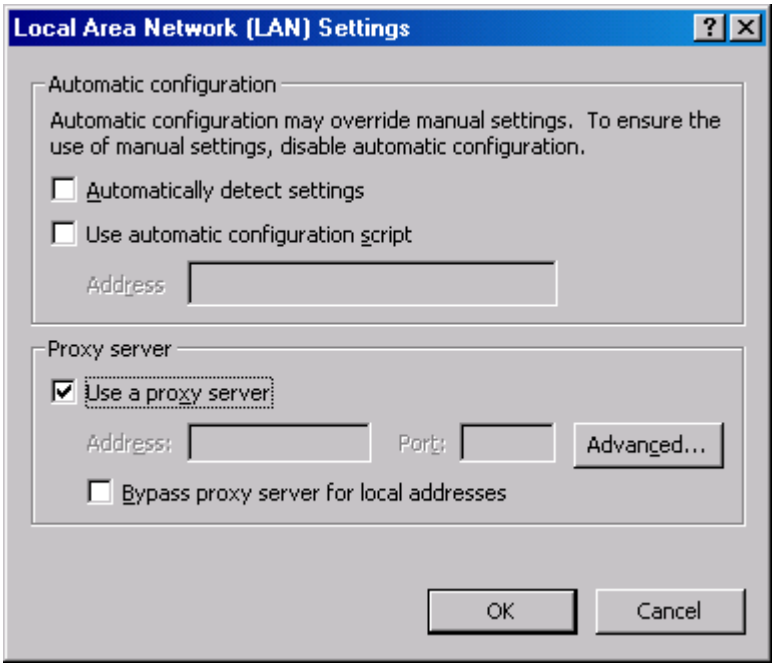


Grafico 6.9. Configuracion Proxy en el Navegador

Dar check en Uso de servidor proxy que a su vez le permitirá hacer clic en el botón Opciones avanzadas.

En el cuadro de diálogo avanzado verá la siguiente información de configuración de proxy. Rellene el puerto de direcciones de acuerdo con el siguiente ejemplo la sustitución de la dirección IP interna de la máquina está ejecutando SpoonProxy en la 192.168.0.1 si su dirección es diferente.

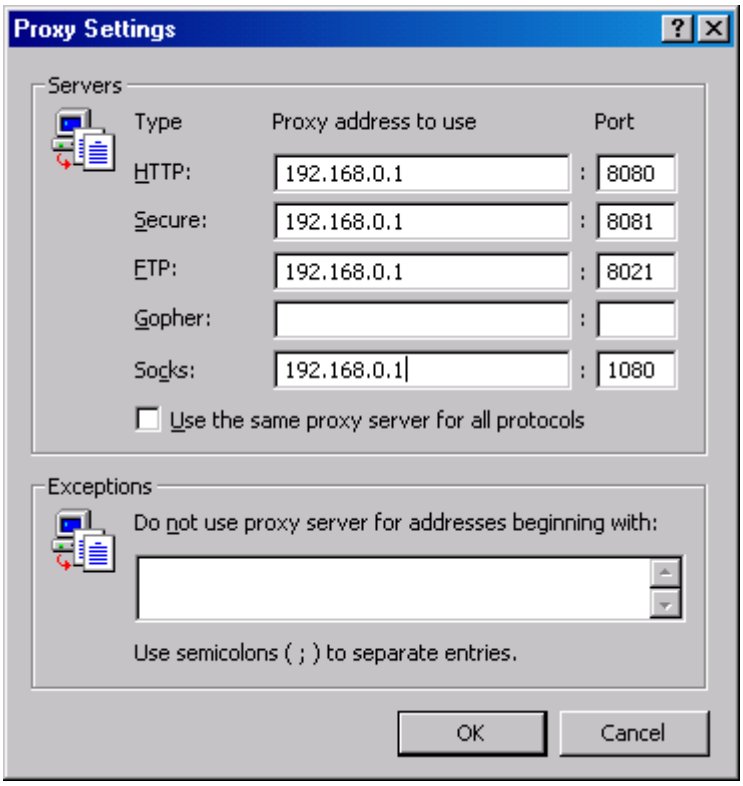


Grafico 6.10. Dirección Ip del Servidor Proxy

HERRAMIENTAS DE AUDITORIA Y CONTROL DE ACCESOS NO AUTORIZADOS AL SERVIDOR WEB DE TURBOTECH

Las siguientes son las herramientas aplicadas en el servidor proxy para evitar accesos no autorizados y mantener un registro de las IPS que están accediendo al servidor:

Super Winspy 3.5.

Esta herramienta permitirá determinar que direcciones URL están siendo invocadas por los usuarios de la red, de tal manera que se gestionarán los posibles ataques

externos que sean invocados por cookies y troyanos almacenados en cualquiera de las maquinas.

Una visión general de Super Winspy 3.5 es la siguiente:

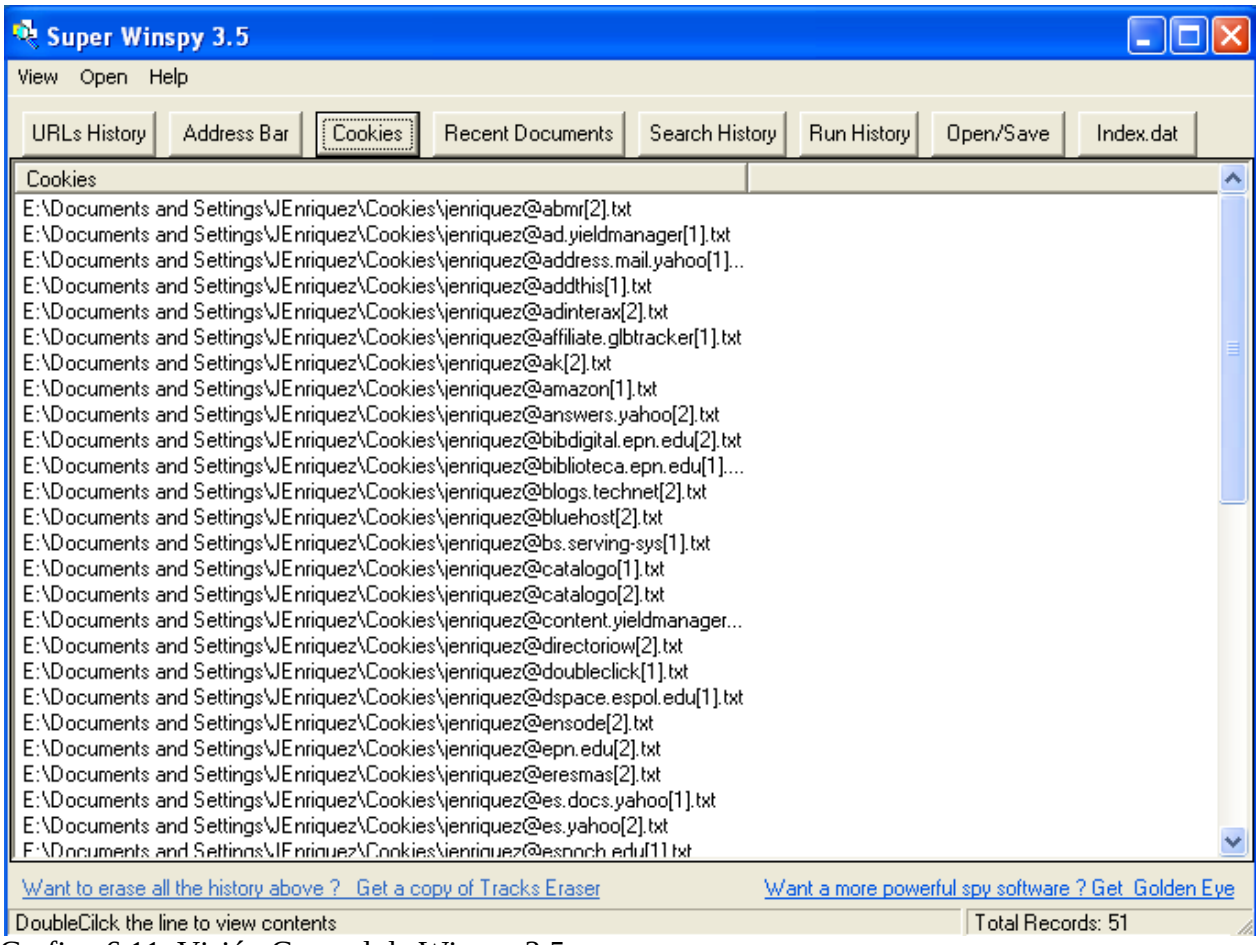


Grafico 6.11. Visión General de Winspy 3.5

Esta aplicación se instalará en el servidor proxy de la empresa.

Sistema de Detección de Intrusos.

Para el monitoreo de la red , se ha establecido la instalación en el servidor web de la empresa el software **LookaNet,** que permitirá escanear puertos, verificar la existencia de paquetes sniffer, monitoreo de paquetes y un sistema de monitoreo LAN.

La siguiente figura muestra el funcionamiento de la herramienta antes indicada.

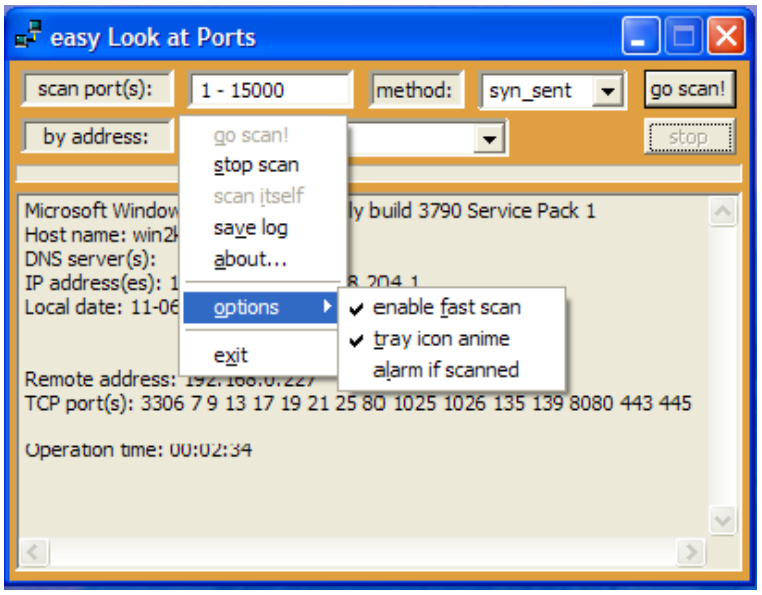


Gráfico 6.12. Visión General de LooksaNet

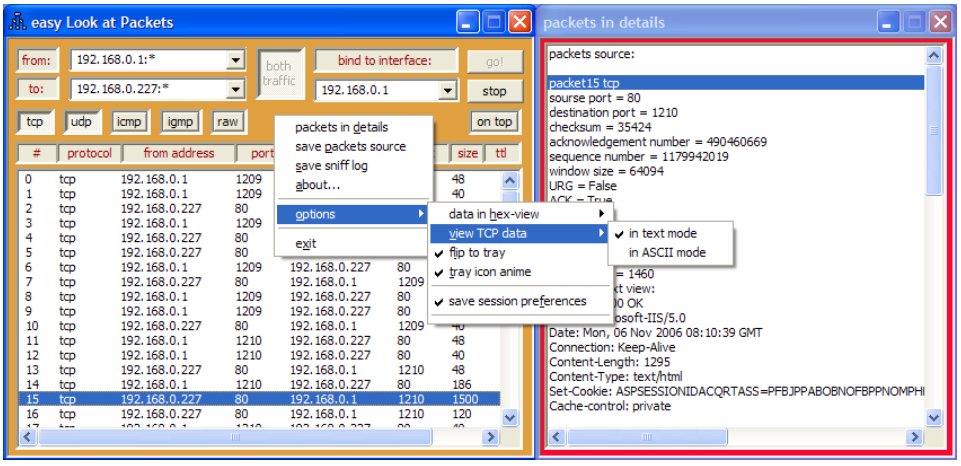


Gráfico 6.13. Reporte General de LooksaNet

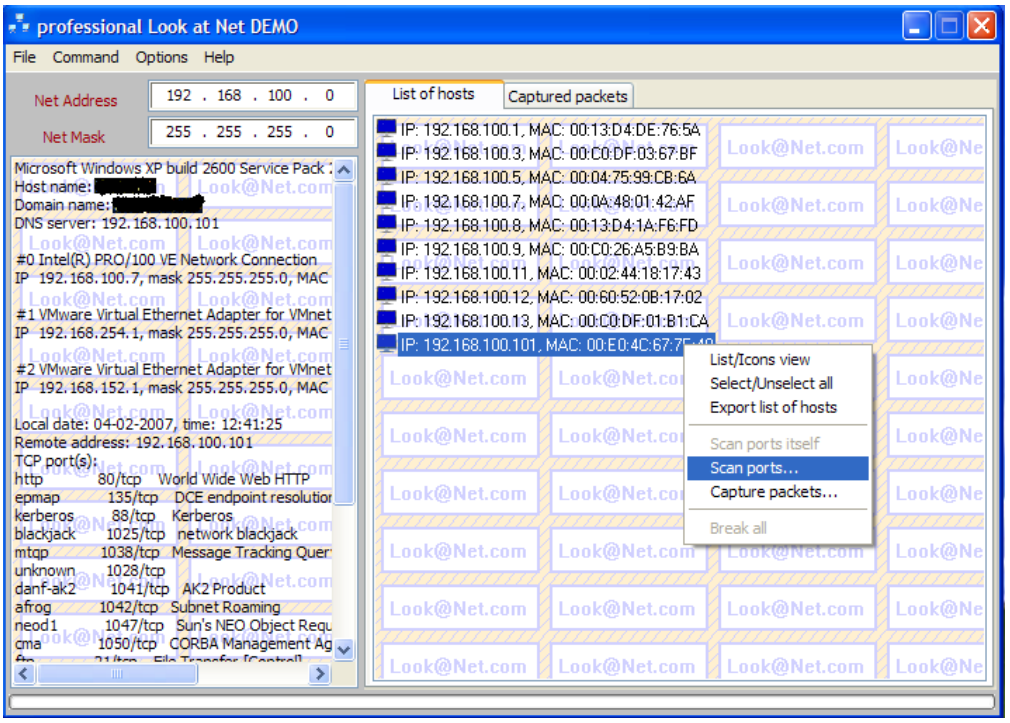


Gráfico 6.14. Ips conectadas en la Red del Web Server

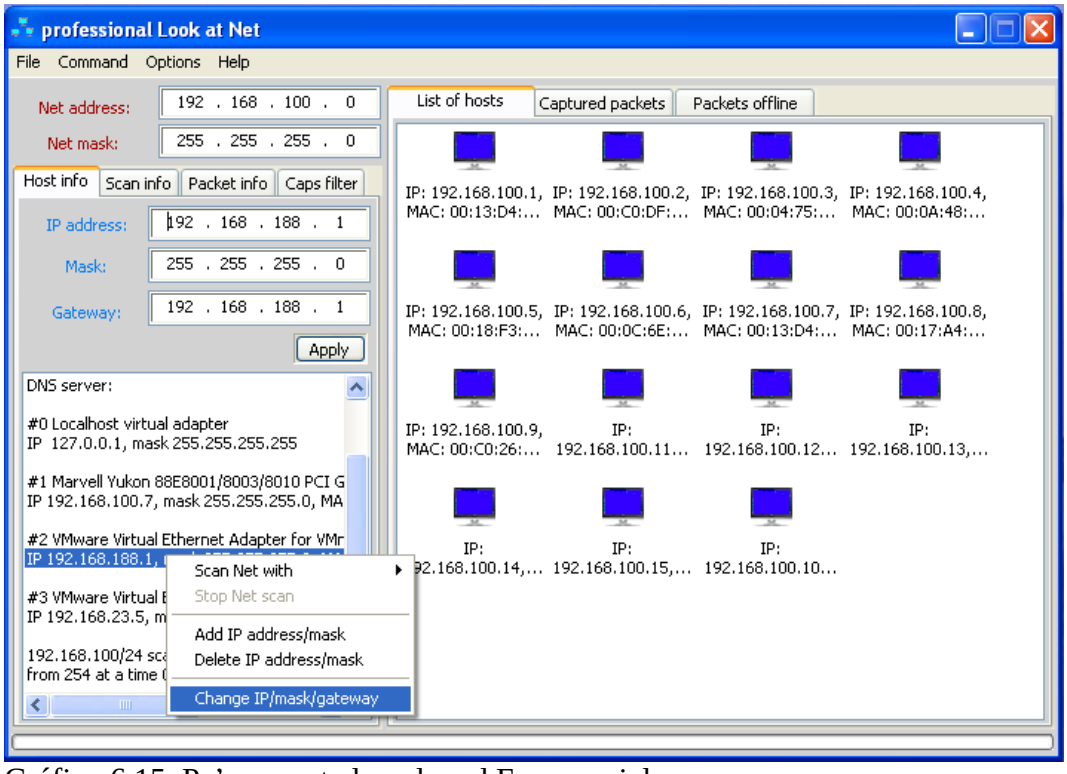


Gráfico 6.15. Pc's conectadas a la red Empresarial

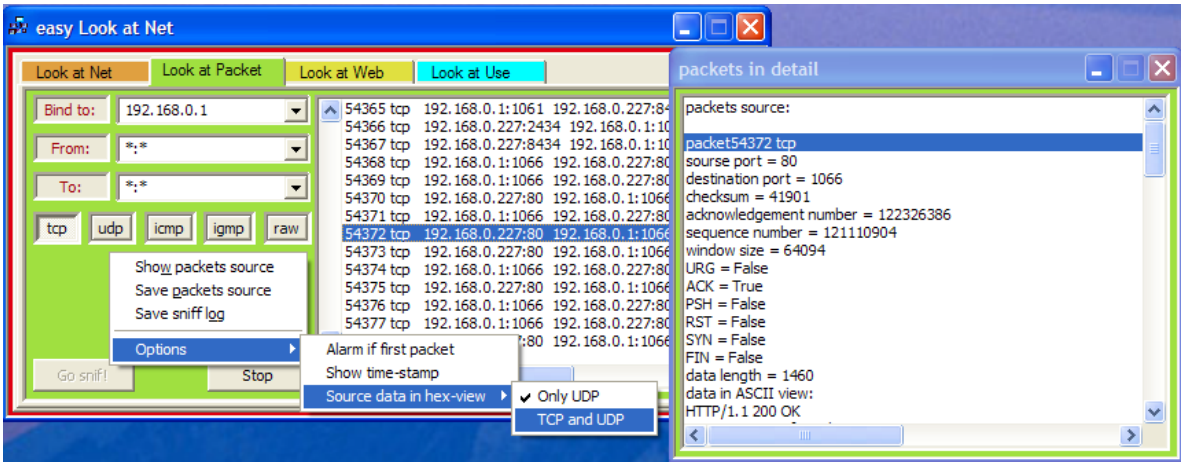


Gráfico 6.16. Escaneo de Puertos de Pc´s conectadas

Esta aplicación está instalada en el servidor web de la empresa, y le permitirá al administrador de sistemas detectar cualquier intruisión.

Politicas de acceso a sistemas Web Gerenciales

Para los aplicativos web Gerenciales y las aplicaciones Cliente servidor de consulta de datos del Gerente y Presidente de la empresa, se ha instalado una Red Privada Virtual, de esta manera la política de accesos a estos datos confidenciales como Balances, Indice de Ventas, Precios actuales e históricos de los turbos solo estarán disponibles para los principales directivos de la empresa.

Leaf Software

El aplicativo gestionador de la conexión VPN es Leaf software, el cual respetando los principios de software libre permite crear una red privada virtual que permitirá conectar al gerente y subgerente de la empresa con los datos críticos de la organización.

Se ha considerado a Leaf como gestionador de VPN puesto que es un software completamente libre, a diferencia de Hamachi que cuyo costo y versatilidad no se comparan con la herramienta escogida.

En Leaf software se ha creado una red virtual denominada Turbotech, a continuación se muestra la figura de Leaf Software:

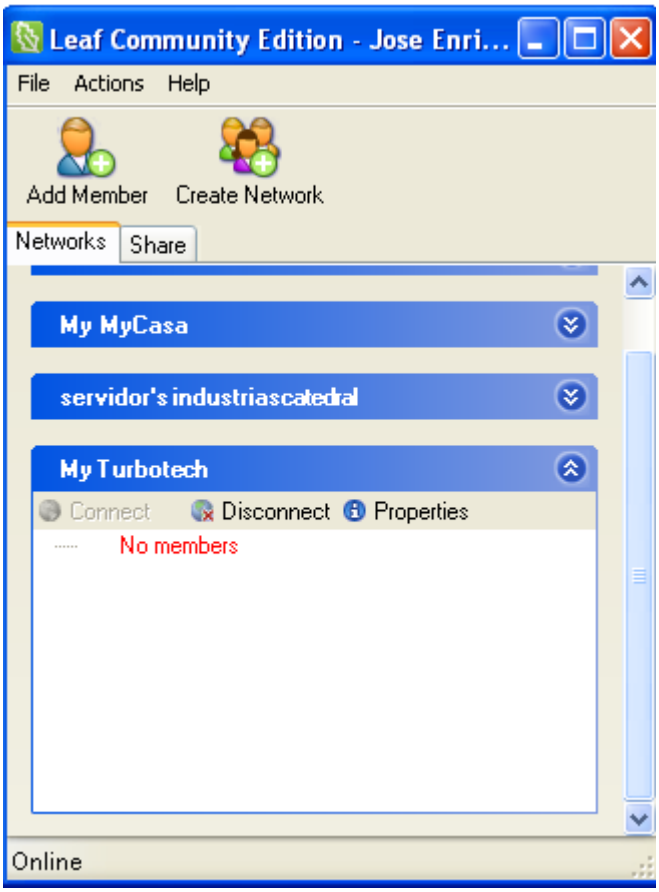


Gráfico 6.10**.** Configiración de la VPN

Leaf generará una Ip pública que servirá de conexión con el servidor principal a través del servicio de escritorio remoto.

Acceso a través del escritorio remoto.

Las cuentas generadas para el acceso a través del escritorio remoto al servidor web, serán:

Dmayorga	Cuenta de Gerente de Turbotech
Gmayorga	Cuenta de Presidente de Turbotech.

Estos usuarios tendrán privilegios de usuario administrador para realizar cualquier consulta, cambio o modificación de los datos del sistema informático.

Cada uno de ellos portará una laptop con conexión a internet, donde el software Leaf estará previamente instalado y configurado, formando parte de la red virtual establecida como My Turbotech.

La Ip pública del servidor web otorgada por Leaf Software será: 5.3.130.24, a través de ella se realizará la respectiva validación tanto en el escritorio remoto como al invocar los datos del servidor Web.

La imagen a continuación indica como los Sres. Gerente y subgerente se conectarán remotamente al servidor.

Una vez validados ingresarán al servidor web de la empresa y podrán entrar a este directamente para realizar las respectivas consultas, o podrán acceder a los aplicativos web a través del navegador de internet haciendo referencia a la dirección anteriormente especificada, así:

Gráfico 6.18. Conexión de Escritorio Remoto

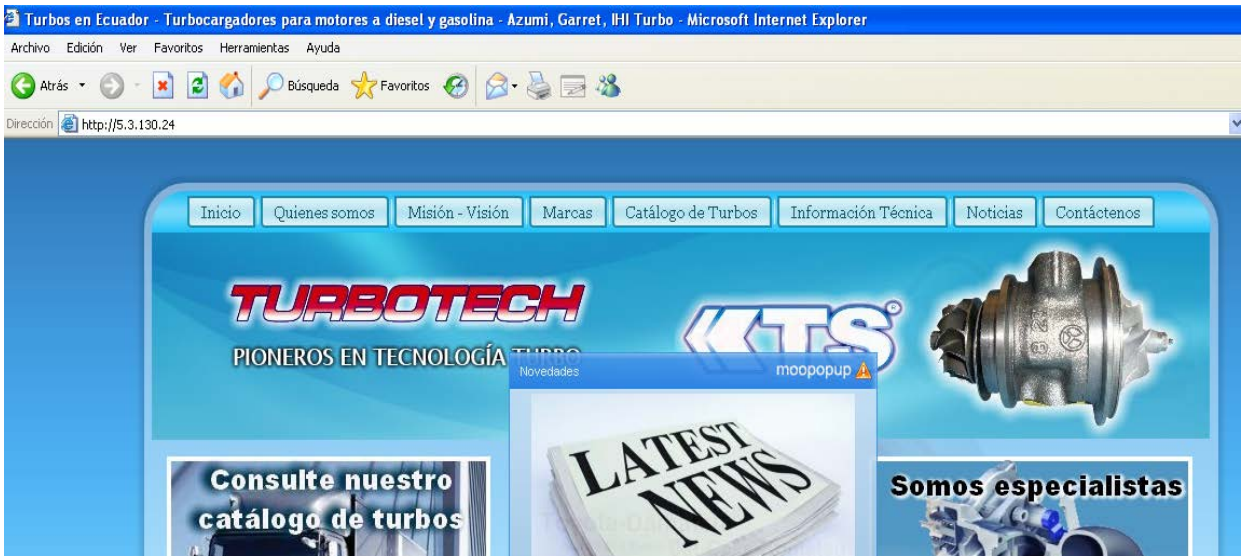


Gráfico 6.19. Entorno Web de Turbotech

Las imágenes anteriormente expuestas muestran la validación de los usuarios en el escritorio remoto provisto por la red VPN de la empresa Turbotech.

PLAN DE ACCIÓN

Actividad	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE
Identificación de los principales debilidades físicas del área de servidores								
Evaluación de debilidades de seguridad física								
Identificación del hardware de los servidores								
Identificación de los sistemas operativos servidores								
Desarrollo de políticas de seguridad física del área informática								
Desarrollo de políticas de seguridad física del área de sistemas en la empresa								
Evaluación de las debilidades a los que están espuestos los servidores								
Desarrollo de políticas de seguridad lógica en los servidores								
Evaluación de herramientas de conexión de internet working								
Selección de las herramientas de conexión de internet working								
Implementación de la tecnología de internet working								
Evaluación de herramientas de control de intrusos								
Selección de la herramienta de control de intrusos								
Elaboración del informe final								

Tabla 6.3. Plan de Acción

ADMINISTRACIÓN

Recursos que dispone la Empresa:

Talento Humano de la Empresa Turbotech

Personal Docente	Título	Cargo en la Empresa
Ing, Galo David Mayorga Poveda	Ing. Mecánico	Gerente General
Ing. Galo Fernando Mayorga Pazmiño	Ing. Mecánico	Presidente General
Ing. Ismael Sebastián Mayorga Poveda	Ing. En Economía	Jefe de Ventas
Ing. José Fabián Enriquez Miranda	Ing. En Sistemas	Auxiliar Contable y Responsable del Área Informática

Tabla 6.4.Talento Humano de Turbotech

RECURSOS MATERIALES

Recursos Tecnológicos

Tipos	Número disponible	Estado de conservación	Número necesario
Servidores	**2**	Excelente	2
Computadores	**10**	Excelente	4
Servicio de Internet en la empresa(Conexión Principal y Backup)	2	Excelente	2
Banda Ancha Movil	2	Excelente	2

Tabla 6.5. Recursis Tecnológicos

PREVISIÓN DE LA EVALUACIÓN

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Quiénes requieren políticas de seguridad informática para reducir la vulnerabilidad de los entornos web?	El área administrativa de la empresa Turbotech.
¿Por qué implementar políticas de seguridad?	Porque todo proyecto encaminado a un mejoramiento debe estar sujeto a un seguimiento valorativo que ayudará a las unidades organizativas de una empresa.
¿Para qué implementar políticas de seguridad informática?	Para reducir la vulnerabilidad de los entornos web de la empresa Turbotech.
¿Qué implementa políticas de seguridad informática?	Las diferentes herramientas y normas de calidad orientadas a la seguridad de la información.
¿Quién implementa políticas se seguridad informática?	El maestrante, como miembro activo del área administrativa de la empresa..
¿Cuándo implementar políticas de seguridad informática?	Inmediatamente luego de analizadas las diferentes herramientas.
¿Cómo implementar políticas de seguridad informática?	Con un miembro del área administrariva especialista en redes que analice las nuevas vulnerabilidades y aplique sobre estas normas y herramientas que eviten un robo de información
¿Con qué implementar políticas de seguridad informática?	Con los principos establecidos por la norma ISO 27000

Tabla 6.6. Previsión de la Evaluación

PRESUPUESTO DE LA PROPUESTA

El presupuesto para la implementación de las políticas de seguridad informática es la siguiente:

DESCRIPCION	VALOR
Adquisición del servidor proxy	2.100
Sistema anti-incendios para área de servidores	9.000
Capacitación al personal del área administrativa sobre seguridades en la información	1.000
TOTAL	11.100

Tabla 6.7. Presupuesto de la Propuesta

FINANCIAMIENTO

Los recursos serán asignados por la empresa Turbotech

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se determinó una guía con los procedimientos necesarios para establecer las políticas de seguridad para los entornos Web de la Empresa Turbotech.
- Se ha establecido un procedimiento de políticas de seguridad.
- Se ha capacitado y dialogado con los directivos de la empresa sobre la importancia de la seguridad informática.
- Se han estudiado varias herramientas de auditoria y control de vulnerabilidades.
- Se ha implementado la mejor herramienta de auditoria y control de vulnerabilidades de los entornos Web para la empresa Turbotech

Recomendaciones

- Se recomienda que el Departamento de Sistemas, designe a una persona responsable del mantenimiento de las políticas de seguridad, puesto que las empresas de hoy en día requieren que el Área Tecnológica de Sistemas controle ataques externos que provienen del Internet.
- Al establecer una herramienta de auditoria en la Empresa, se debe tomar en cuenta el software de código libre., puesto que las políticas informáticas del Ecuador tienden a utilizar programas sin costo y muy robustos.
- Los procedimientos estudiados e implementados de preferencia deben ser revisados en un período no mayor de tres años, con el fin de mantener reglas y herramientas actualizadas para la auditoria y control de las políticas se seguridad.

BIBLIOGRAFIA

AREAS FIGUEROA, Daniel Herramientas de Gestion Basada en Web, Universidad Nacional de la Plata, La Plata, 1999.

ArCERT, Manual de Seguridad en Redes
Secretaria de Tecnologías Informáticas de la Administración Pública Argentina, Buenos Aires, 2009.

AGUILERA DIAZ , Vicente Inseguridad de los sistemas de autenticación en aplicaciones Web, Barcelona, Marzo del 2010.

FUENTES DE INFORMACIÓN EN INTERNET

- http://books.google.com.ec/books?id=Mgvm3AYIT64C&pg=PA21&dq=politicas+de+seguridad+informatica&hl=es&ei=r_nyTIWBOsL-8AbH6qzeDA&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCkQ6AEwAA#v=onepage&q&f=false
- http://www.segu-info.com.ar/politicas/
- http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica
- http://es.wikipedia.org/wiki/Seguridad_informática
- http://es.debugmodeon.com/articulo/principales-vulnerabilidades-en-aplicaciones-web
- http://www.desarrolloweb.com/articulos/principales-vulnerabilidades-web.html
- http://vtroger.blogspot.com/2006/04/vulnerabilidades-de-pginas-web-y.html
- http://www.forosdelweb.com/f15/vulnerabilidad-web-750558/
- http://foro.portalhacker.net/index.php/topic,90398.0.html

- http://www.dragonjar.org/vulnerabilidades-web-que-permiten-acceder-al-sistema.xhtml
- http://www.informaticanova.com/seguridad-informatica/cursos-eventos-y-publicaciones/curos-presenciales-especializados-en-seguridad-web.html
- http://www.seguridadinformatica.es/profiles/blogs/1024177:BlogPost:461
- http://seguinfo.wordpress.com/category/vulnerabilidades/
- http://cursowebavanzado.uji.es/docs/seguridad_web.pdf
- http://translate.google.com/translate?hl=es&langpair=en%7Ces&u=http://www.acros.si/papers/session_fixation.pdf
- http://amap.cantabria.es/confluence/display/DOCS/Vulnerabilidades+mas+frecuentes
- http://www.dragonjar.org/moth-entorno-virtualizado-para-entrenamiento-en-seguridad-con-aplicaciones-web-vulnerables.xhtml
- http://nevada.ual.es:81/cursosverano/2010/index.php?option=com_content&view=article&id=62:seguridad-en-entornos-web-e-comercio-y-e-administracion&catid=36:vicar&Itemid=73
- http://elinternet.es/2010/09/primeros-ataques-en-el-internet-por-asp-net/
- http://www.israelviana.es/blog/Post/79/el-ataque-de-eu2010es-en-otra-web-de-la/
- http://vtroger.blogspot.com/2008/04/inseguridad-en-upnp.html
- http://www.morales-vazquez.com/fhack.html
- http://www.mcafee.com/us/local_content/white_papers/wp_webw_browsers_w_es.pdf
- http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SeguridadWin2000.PDF
- http://foro.bitsdelocos.es/hacking/ataques-a-ldap/
- http://bitsignals.com/
- http://www.gfihispana.com/mailsecurity/msecfeatures.htm
- http://www.siainternational.com/articles/10_S.htm
- http://www.qualys.com/docs/QG_WAS_DS_ES.pdf

- http://jaimeescobar.espacioblog.com/
- http://www.canaleficiencia.com/ciudades-azules/nature-news/vulnerables-a-los-ataques_1255_518_1973_0_1_in.html
- http://www.yaguarete-sec.com/the-news/49-amenazas.html
- http://www.pdfgeni.org/fd/vulnerabilidades--hacker-pdf.html
- http://www.forospyware.com/t214198.html
- http://blog.txipinet.com/2006/07/30/7-introduccion-a-la-seguridad-informatica/
- http://www.accesomedia.com/display_release.html?id=9736
- www.wapiti.com
- www.pi-soft.com
- www.leafnetworks.net

ANEXOS

ANEXO 1

ENCUESTA APLICADA AL DEPARTAMENTO ADMINISTRATIVO DE TURBOTECH

ENCUESTA APLICADA AL GERENTE, SUBGERENTE, JEFES DE AREA Y AUXILIARES DEPARTAMENTALES			
	PREGUNTAS	**SI**	**NO**
1	¿Existen filtros y estabilizadores en la red eléctrica de suministros de los equipos?		
2	¿Tienen instaladas fuentes de alimentación redundantes?		
3	¿Tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos?		
4	¿Los servidores cuentan con UPS's?		
5	¿Se realizan copias de los datos con periodicidad?		
6	¿El área de servidores está expuesta a usuarios no autorizados?		
7	¿Se crea un nuevo nombre de usuario y contraseña por cada empleado que ingrese a la empresa?		
8	¿Con qué periodicidad se realiza el cambio de contraseñas?		
9	¿Se establecen grupos de usuarios para el acceso a los recursos de los servidores?		
10	¿Existen políticas de grupo aplicables para el acceso a la información?		
11	¿Existe un procedimiento de identificación y autenticación?		
12	¿Las contraseñas se asignan de forma automática por el servidor?		
13	¿Dispone de web site empresarial?		
14	¿Existe un procedimiento de copia de seguridad del software y los datos?		
15	¿Se almacena alguna copia del software y datos fuera de los locales de la empresa?		
16	¿Los respaldos de la información se lo realiza en discos duros externos?		
17	¿Existe implementado un servidor espejo como backup?		
18	¿El servidor cuenta con discos espejo para la redundancia de la información?		
19	¿Existen controles de acceso a los usuarios?		
20	¿De qué depende la asignación de los roles de usuario al crear uno nuevo?		
21	¿Cuándo un usuario nuevo es creado tiene acceso a todos los recursos del servidor?		
22	¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos ?		
23	¿Se realiza el mantenimiento por personal de la propia empresa?		
24	¿Está alojado en la red empresarial el servidor web?		
25	¿Se ha contratado personal informático para que diseñe las aplicaciones?		
26	¿Se dispone de cortafuegos?		

27	¿Dispone de herramientas que auditen intentos de accesos externos?		
28	¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?		
	PREGUNTAS	**SI**	**NO**
29	¿Están los servidores protegidos en cuanto a inicios de sesión y acceso a través de la red?		
30	¿Cuenta Turbotech con niveles de acceso a los usuarios?		
31	¿El servidor otorga direcciones IP automática a los usuarios validados?		
32	¿Conoce acerca de los niveles de acceso a los servidores web?		
33	¿Tiene conocimiento del concepto de acceso a nivel del sistema?		
34	¿Tiene conocimiento del concepto de acceso a nivel de aplicación?		
35	¿Cómo se asignan los permisos para el acceso a la aplicación web de la empresa?		
36	¿Conoce acerca de los ataques a nivel de Internet?		
37	¿Sabe lo que es un hacker?		
38	¿Conoce lo que es pishing?		
39	¿Existen un plan de contingencia ante un ataque externo?		

ANEXO 2

RESULTADO DE LAS HERRAMIENTAS DE AUDITORIA DE LOS ENTORNOS WEB DE TURBOTECH

Dentro de las herramientas propuestas se ha considerado para la auditoria de los entornos web

Herramienta Acunetix Web Vulnerability Scanner

Resumen del Escaneo del Sitio Web de Turbotech

Threat Level

Acunetix Threat Level 0
No vulnerabilities have been discovered by the scanner.

Alerts Found

Total alerts found	**0**
High	0
Medium	0
Low	0
Informational	0

Target Information

Target	www.turbotech.com.ec
Server banner	Apache mod_fcgid/2.3.5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Operating system	Unknown
Web server	Apache
Technologies	PHP,FrontPage

Web Scan Progress

Start time	2/1/2011, 19:38:05
Finish time	
Scan time	5 minutes, 53 seconds
Scan iteration	1
Scanning mode	Heuristic
Scanning stage	Crawling

Current module	Crawler skip
Testing on	N/A
Current test(s)	N/A
Running tasks	N/A
Total number of requests	483
Average response time (ms)	2415,59

Port Scan Progress

	99%
Open ports	21/ftp, 53/domain, 80/http, 110/pop3, 143/imap, 443/https, 465/smtps, 993/imaps, 995/pop3s, 3306/mysql

Scripts Progress

	96%
Running scripts	

VENTANA DE ACTIVIDADES

enero 2 19:37.05, Parse Frame Config XML ...
enero 2 19:37.05, Acunetix Web Vulnerability Scanner, version 6.5, build 20100706
enero 2 19:37.20, Populate application menus ...
enero 2 19:37.21, Populate tools bar ...
enero 2 19:37.21, Populate tool explorer ...
enero 2 19:37.21, Load ServerInfo XML ...
enero 2 19:37.22, Load module "Version check" ...
enero 2 19:37.22, Load module "CGI Tester" ...
enero 2 19:37.23, Load module "Parameter manipulation" ...
enero 2 19:37.23, Load module "MultiRequest parameter manipulation" ...
enero 2 19:37.24, Load module "File checks" ...
enero 2 19:37.25, Load module "Directory checks" ...
enero 2 19:37.25, Load module "Web Applications" ...
enero 2 19:37.26, Load module "Text search" ...
enero 2 19:37.26, Load module "File Uploads" ...
enero 2 19:37.27, Load module "Authentication" ...
enero 2 19:37.27, Load module "GHDB - Google hacking database" ...
enero 2 19:37.27, Load module "Knowledge base" ...
enero 2 19:37.28, Load module "Web Services - Parameter manipulation" ...
enero 2 19:37.29, Load module "Web Services - Multirequest parameter manipulation" ...
enero 2 19:37.30, 14 modules loaded.
enero 2 19:37.44, Determining necessary updates ...
enero 2 19:38.05, Started scanning www.turbotech.com.ec ...
enero 2 19:38.05, Start URL : www.turbotech.com.ec
enero 2 19:38.05, Scanning Mode : Heuristic
enero 2 19:38.05, Server banner: Apache
enero 2 19:38.05, Starting port scanner (1278 ports)
enero 2 19:38.05, Crawling started, URL: http://www.turbotech.com.ec/
enero 2 19:38.07, Processing file /
enero 2 19:38.08, Processing file /modules/mod_moopopup/moopopup/moopopup03.css
enero 2 19:38.08, Processing file /templates/system/css/general.css
enero 2 19:38.08, Processing file /templates/system/css/system.css
enero 2 19:38.09, Processing file /rss
enero 2 19:38.09, Processing file /index.php (variation 1)
enero 2 19:38.09, Processing file /atom
enero 2 19:38.10, Processing file /index.php
enero 2 19:38.11, Processing file /informacion/mision-vision
enero 2 19:38.11, Processing file /informacion/productos

enero 2 19:38.11, Processing file /templates/turbotechazul/css/template.css
enero 2 19:38.12, Processing file /informacion/news
enero 2 19:38.13, Processing file /informacion/funcionamiento-diagnostico-y-mantenimieto-de-turbos
enero 2 19:38.14, Processing file /informacion/informacion
enero 2 19:38.14, Processing file /informacion/mapa
enero 2 19:38.14, Processing file /informacion/quienes-somos
enero 2 19:38.20, Processing file /volvo-scania
enero 2 19:38.20, Processing file /caterpillar-case-komatsu
enero 2 19:38.21, Processing file /cummins
enero 2 19:38.21, Processing file /hyundai-mitsubishi-kia
enero 2 19:38.22, Processing file /volskwagen
enero 2 19:38.22, Processing file /mack-detroit
enero 2 19:38.23, Processing file /mazda
enero 2 19:38.24, Processing file /media/system/js/caption.js
enero 2 19:38.24, Processing file /modules/mod_moopopup/moopopup/mooMessageBox.js
enero 2 19:38.25, Processing file /modules/mod_rokslideshow/tmpl/rokslideshow.js
enero 2 19:38.25, Processing file /mercedes-benz-man
enero 2 19:38.25, Processing file /templates/turbotechazul/script.js
enero 2 19:38.25, Processing file /modules
enero 2 19:38.26, Processing file /modules/mod_moopopup
enero 2 19:38.26, Processing file /modules/mod_moopopup/moopopup
enero 2 19:38.26, Processing file /templates
enero 2 19:38.26, Processing file /templates/system
enero 2 19:38.26, Processing file /templates/system/css
enero 2 19:38.27, Processing file /templates/turbotechazul/css
enero 2 19:38.27, Processing file /templates/turbotechazul
enero 2 19:38.28, Processing file /nissan
enero 2 19:38.29, Processing file /toyota-daihatsu
enero 2 19:38.30, Processing file /modules/mod_joomulus/swfobject.js
enero 2 19:38.30, Processing file /qmc-jac
enero 2 19:38.30, Processing file /media/system/js/mootools.js
enero 2 19:38.36, Open port 21 - ftp
enero 2 19:38.36, Processing file /images
enero 2 19:38.36, Processing file /images/stories
enero 2 19:38.36, Processing file /media
enero 2 19:38.36, Processing file /media/system
enero 2 19:38.37, Processing file /informacion
enero 2 19:38.38, Processing file /media/system/js
enero 2 19:38.38, Processing file /modules/mod_rokslideshow
enero 2 19:38.39, Open port 53 - domain
enero 2 19:38.39, Processing file /modules/mod_rokslideshow/tmpl
enero 2 19:38.39, Processing file /modules/mod_joomulus
enero 2 19:38.39, Processing file /cache
enero 2 19:38.39, Processing file /components
enero 2 19:38.39, Processing file /includes
enero 2 19:38.39, Processing file /language
enero 2 19:38.39, Processing file /libraries
enero 2 19:38.40, Processing file /plugins
enero 2 19:38.40, Processing file /installation
enero 2 19:38.40, Processing file /administrator
enero 2 19:38.48, Processing file /tmp
enero 2 19:38.48, Processing file /xmlrpc
enero 2 19:38.49, Processing file /modules/mod_moopopup/moopopup/images
enero 2 19:38.49, Processing file /templates/system/images
enero 2 19:38.50, Processing file /caterpillar-case-komatsu/turbo-cat-950b
enero 2 19:38.50, Processing file /caterpillar-case-komatsu/core-para-kodiak
enero 2 19:38.51, Processing file /caterpillar-case-komatsu/cummins-6ct-6cta-y-6ctaa-de-8-3l
enero 2 19:38.51, Processing file /caterpillar-case-komatsu/turbo-cat-320c
enero 2 19:38.51, Processing file /cummins/cummins-6ct-6cta-y-6ctaa-de-8-3l-sin-intercooler
enero 2 19:38.51, Processing file /turbos-para-autos-y-motores-a-diesel-reparacion-y-venta-de-turbocargadores-en-marcas-azumi-garret-ihi-turbo-master-power-y-kts
enero 2 19:38.52, Processing file /cummins/turbo-para-motores-cummins-6btaa-5-9l-e-isb-5-9l
enero 2 19:38.52, Processing file /cummins/turbo-para-motores-cummins-6ctaa-8-3l
enero 2 19:38.52, Processing file /caterpillar-case-komatsu/cummins-6bt-5-9l-y-6btaa-5-9lt
enero 2 19:38.52, Processing file /cummins/cummins-6bt-5-9l-y-6btaa-5-9l-130hp-y-160hp
enero 2 19:38.53, Processing file /caterpillar-case-komatsu/turbo-cat-s4kt

enero 2 19:38.53, Open port 80 - http
enero 2 19:38.55, Open port 110 - pop3
enero 2 19:38.56, Processing file /cummins/turbo-ford-cargo-815
enero 2 19:38.56, Processing file /caterpillar-case-komatsu/turbo-cat-320b
enero 2 19:38.57, Processing file /hino/turbo-hino-fd-ff-ho6ct-a-r-1-00
enero 2 19:38.58, Processing file /hino/turbo-hino-fd-ff-h06ct-a-r-0-84
enero 2 19:38.58, Processing file /hino/core-para-turbo-super-hino-vx53-motor-h07ct
enero 2 19:38.59, Processing file /hino/turbo-hino-gd-gh-ff-fg-j08ct
enero 2 19:38.59, Processing file /hino/core-para-turbo-hino-gd-gh-ff-fg-motor-j08-ct
enero 2 19:38.59, Processing file /hyundai-mitsubishi-kia/turbo-para-hyundai-hd72-hd78-y-mitsubishi-canter-moderno
enero 2 19:38.59, Processing file /hyundai-mitsubishi-kia/turbo-para-hyunday-h1-y-terracane
enero 2 19:38.59, Processing file /hyundai-mitsubishi-kia/core-tdo5h-para-turbo-de-hyundai-hd72-hd78-y-mitsubishi-canter-4d34
enero 2 19:39.00, Processing file /hyundai-mitsubishi-kia/core-tdo6-para-turbos-de-hyundai-y-mitsubishi-4-4-lt-en-marca-kts
enero 2 19:39.00, Processing file /hyundai-mitsubishi-kia/core-gt20-para-turbo-de-hyundai-hd65-y-hd72
enero 2 19:39.00, Processing file /hino/turbo-super-hino-vx53-h07ct
enero 2 19:39.01, Processing file /hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-4-5l-en-marca-kts-con-roseta-de-titanio
enero 2 19:39.01, Processing file /hino/turbo-hino-fd-h06ct-con-caracol-de-escape-original-y-valvula
enero 2 19:39.01, Processing file /hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-h100
enero 2 19:39.01, Processing file /hino/turbo-super-hino-h07ct-a-r-0-84
enero 2 19:39.01, Processing file /hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-h1-y-terracanece
enero 2 19:39.01, Processing file /hyundai-mitsubishi-kia/core-turbo-hyundai-tucson-kia-sportage
enero 2 19:39.02, Processing file /hyundai-mitsubishi-kia/core-kia-carens
enero 2 19:39.02, Processing file /hino/core-para-turbo-hino-fb-fc-motor-j05ct
enero 2 19:39.04, Open port 143 - imap
enero 2 19:39.10, Processing file /isuzu/turbo-isuzu-nhr-nkr
enero 2 19:39.11, Processing file /isuzu/turbo-isuzu-npr-sin-valvula
enero 2 19:39.12, Processing file /isuzu/turbo-isuzu-npr-antiguo-con-valvula
enero 2 19:39.12, Processing file /isuzu/turbo-isuzu-ftr
enero 2 19:39.12, Processing file /isuzu/turbo-isuzu-ftr-2000-2007
enero 2 19:39.12, Processing file /isuzu/turbo-chevrolet-dmax-3-0
enero 2 19:39.14, Processing file /isuzu/turbo-chevrolet-luv-y-luv-d-max
enero 2 19:39.15, Processing file /isuzu/core-para-el-isuzu-npr-con-valvula-modelo-1998-2000
enero 2 19:39.15, Processing file /isuzu/core-chevrolet-luv-motor-2-8l
enero 2 19:39.16, Processing file /isuzu/core-isuzu-nhr-nkr
enero 2 19:39.16, Processing file /isuzu/core-para-el-isuzu-npr-sin-valvula
enero 2 19:39.18, Processing file /mack-detroit/mack-e675-y-676
enero 2 19:39.18, Processing file /isuzu/core-para-el-isuzu-npr-con-valvula-y-multiple
enero 2 19:39.18, Processing file /mack-detroit/detroit-serie-60-con-valvula
enero 2 19:39.18, Processing file /mack-detroit/detroit-serie-60-sin-valvula
enero 2 19:39.19, Processing file /mack-detroit/detroit-serie-60-sin-valvula-11-1-lt
enero 2 19:39.20, Processing file /mazda/turbo-mazda-bt-50
enero 2 19:39.20, Processing file /isuzu/core-chevrolet-luv-y-luv-d-max-2-2l-y-2-5l
enero 2 19:39.20, Processing file /isuzu/core-isuzu-ftr
enero 2 19:39.21, Processing file /mazda/core-turbo-mazda-bt-50
enero 2 19:39.21, Processing file /mercedes-benz-man/cartridge-para-turbo-mercedes-om366
enero 2 19:39.21, Processing file /mercedes-benz-man/turbo-mercedes-motor-om366-intercooler-de-alto-rendimiento
enero 2 19:39.21, Processing file /mercedes-benz-man/turbo-ta31
enero 2 19:39.22, Processing file /isuzu/core-isuzu-ftr-2000-2007
enero 2 19:39.22, Processing file /isuzu/core-chevrolet-luv-d-max-3-0l
enero 2 19:39.22, Processing file /mercedes-benz-man/turbo-para-mercedes-1728
enero 2 19:39.23, Processing file /mercedes-benz-man/turbo-para-mercedes-benz-om422la-om442la-y-402la
enero 2 19:39.23, Processing file /mercedes-benz-man/turbo-para-mercedes-benz-actros-3348-y-3353
enero 2 19:39.23, Processing file /mercedes-benz-man/mercedes-benz-oh1636
enero 2 19:39.24, Processing file /mercedes-benz-man/mercedes-1722
enero 2 19:39.24, Processing file /mercedes-benz-man/mercedes-914-y-915
enero 2 19:39.25, Processing file /nissan/turbo-para-motores-nissan
enero 2 19:39.26, Processing file /mercedes-benz-man/man-280
enero 2 19:39.26, Processing file /nissan/core-nissan-frontier-3-0l
enero 2 19:39.26, Processing file /nissan/core-nissan-frontier-2-5l
enero 2 19:39.26, Processing file /qmc-jac/qmc-jac-motores-chinos-de-2-7l
enero 2 19:39.27, Processing file /qmc-jac/qmc-jac-motores-chinos-de-3-3l
enero 2 19:39.28, Processing file /volskwagen/turbo-volskwagen-17240-17260-con-valvula
enero 2 19:39.28, Processing file /volskwagen/turbo-volskwagen-9-150

enero 2 19:39.28, Processing file /volskwagen/turbo-motores-cummins-6ctaa-8-3l
enero 2 19:39.29, Processing file /volvo-scania/turbo-volvo-n12-nl12edc-f12-b12
enero 2 19:39.29, Processing file /volvo-scania/turbo-volvo-n10-nl280-b10m-b58
enero 2 19:39.29, Processing file /volvo-scania/turbo-scania-p94-r300-r320
enero 2 19:39.29, Processing file /nissan/core-turbo-nissan-pkc212
enero 2 19:39.29, Processing file /volvo-scania/turbo-scania-124-r400-r420
enero 2 19:39.30, Processing file /templates/turbotechazul/images
enero 2 19:39.30, Processing file /toyota-daihatsu/core-turbo-daihatsu-delta-toyota-15b
enero 2 19:39.30, Processing file /index.php (variation 3)
enero 2 19:39.30, Processing file /volskwagen/turbo-para-volkswagen-17210-mwm-6-10-tca
enero 2 19:39.30, Processing file /hino
enero 2 19:39.31, Processing file /index.php (variation 4)
enero 2 19:39.31, Processing file /isuzu
enero 2 19:39.31, Processing file /index.php (variation 5)
enero 2 19:39.32, Processing file /toyota-daihatsu/core-toyota-hilux-2-7-td
enero 2 19:39.32, Processing file /pdf
enero 2 19:39.33, Processing file /index.php (variation 2)
enero 2 19:39.33, Processing file /images/stories/marcas
enero 2 19:39.33, Processing file /index.php (variation 6)
enero 2 19:39.33, Processing file /index.php (variation 7)
enero 2 19:39.34, Processing file /index.php (variation 8)
enero 2 19:39.42, Processing file /plugins/content/plugin_jw_ts/tabs_slides.css
enero 2 19:39.42, Processing file /modules/mod_thumbsup/mod_thumbsup.css.php
enero 2 19:39.42, Processing file /index.php (variation 9)
enero 2 19:39.43, Processing file /plugins/content/plugin_jw_ts/tabs_slides_comp.js
enero 2 19:39.43, Processing file /index.php (variation 11)
enero 2 19:39.43, Processing file /plugins/content/plugin_jw_ts/tabs_slides_def_loader.js
enero 2 19:39.43, Processing file /modules/mod_thumbsup
enero 2 19:39.43, Processing file /plugins/content
enero 2 19:39.43, Processing file /component/jforms/submit/1.html
enero 2 19:39.44, Processing file /plugins/content/plugin_jw_ts
enero 2 19:39.44, Processing file /component/jforms/submit/1.html (variation 2)
enero 2 19:39.44, Processing file /component/jforms/submit/1.html (variation 4)
enero 2 19:39.44, Processing file /component/jforms/submit/1.html (variation 3)
enero 2 19:39.44, Processing file /component/jforms/submit/1.html (variation 5)
enero 2 19:39.44, Processing file /component/jforms/submit/1.html (variation 1)
enero 2 19:39.45, Processing file /index.php (variation 10)
enero 2 19:39.45, Processing file /component/jforms/submit/1.html (variation 6)
enero 2 19:39.45, Processing file /component/jforms/submit/1.html (variation 7)
enero 2 19:39.45, Processing file /component/jforms/submit/1.html (variation 8)
enero 2 19:39.48, Processing file /component/jforms/submit/1.html (variation 10)
enero 2 19:39.51, Open port 443 - https
enero 2 19:39.54, Processing file /component/jforms/submit/1.html (variation 9)
enero 2 19:39.54, Processing file /media/com_jforms/styles/themes/default.css
enero 2 19:39.54, Processing file /media/com_jforms/plugins/elements/securimage/securimage_show.php
enero 2 19:39.54, Processing file /media/com_jforms/plugins/elements/securimage/securimage_show.php (variation 1)
enero 2 19:39.54, Processing file /media/com_jforms
enero 2 19:39.54, Processing file /media/com_jforms/styles/themes
enero 2 19:39.55, Open port 465 - smtps
enero 2 19:39.55, Processing file /media/com_jforms/styles
enero 2 19:39.55, Processing file /component/jforms/submit
enero 2 19:39.55, Processing file /media/com_jforms/plugins
enero 2 19:39.55, Processing file /media/com_jforms/plugins/elements
enero 2 19:39.55, Processing file /media/com_jforms/plugins/elements/securimage
enero 2 19:39.55, Processing file /index.php (variation 12)
enero 2 19:39.55, Processing file /index.php (variation 13)
enero 2 19:39.56, Processing file /volvo-scania (variation 1)
enero 2 19:39.56, Processing file /volvo-scania (variation 2)
enero 2 19:39.56, Processing file /volvo-scania (variation 3)
enero 2 19:39.57, Processing file /volvo-scania (variation 4)
enero 2 19:40.05, Processing file /volvo-scania (variation 5)
enero 2 19:40.05, Processing file /volvo-scania (variation 6)
enero 2 19:40.05, Processing file /volvo-scania/rss
enero 2 19:40.06, Processing file /volvo-scania (variation 8)
enero 2 19:40.06, Processing file /volvo-scania (variation 7)
enero 2 19:40.06, Processing file /volvo-scania (variation 9)

enero 2 19:40.07, Processing file /volvo-scania/atom
enero 2 19:40.09, Processing file /caterpillar-case-komatsu (variation 1)
enero 2 19:40.10, Processing file /caterpillar-case-komatsu (variation 6)
enero 2 19:40.10, Processing file /caterpillar-case-komatsu/rss
enero 2 19:40.11, Processing file /caterpillar-case-komatsu/atom
enero 2 19:40.11, Processing file /caterpillar-case-komatsu (variation 7)
enero 2 19:40.11, Processing file /caterpillar-case-komatsu (variation 3)
enero 2 19:40.11, Processing file /cummins (variation 1)
enero 2 19:40.12, Processing file /caterpillar-case-komatsu (variation 2)
enero 2 19:40.12, Processing file /cummins (variation 2)
enero 2 19:40.13, Processing file /caterpillar-case-komatsu (variation 5)
enero 2 19:40.13, Processing file /caterpillar-case-komatsu (variation 4)
enero 2 19:40.13, Processing file /cummins (variation 3)
enero 2 19:40.13, Processing file /cummins (variation 4)
enero 2 19:40.13, Processing file /cummins (variation 5)
enero 2 19:40.14, Processing file /caterpillar-case-komatsu (variation 8)
enero 2 19:40.14, Processing file /cummins (variation 6)
enero 2 19:40.14, Processing file /cummins (variation 7)
enero 2 19:40.14, Processing file /caterpillar-case-komatsu (variation 9)
enero 2 19:40.14, Processing file /cummins (variation 8)
enero 2 19:40.15, Processing file /cummins/rss
enero 2 19:40.15, Processing file /cummins/atom
enero 2 19:40.16, Processing file /cummins (variation 9)
enero 2 19:40.16, Processing file /hyundai-mitsubishi-kia (variation 1)
enero 2 19:40.16, Processing file /hyundai-mitsubishi-kia (variation 2)
enero 2 19:40.16, Processing file /hyundai-mitsubishi-kia (variation 3)
enero 2 19:40.19, Processing file /hyundai-mitsubishi-kia (variation 6)
enero 2 19:40.21, Processing file /volskwagen (variation 3)
enero 2 19:40.21, Processing file /volskwagen (variation 1)
enero 2 19:40.21, Processing file /hyundai-mitsubishi-kia (variation 4)
enero 2 19:40.21, Processing file /volskwagen (variation 2)
enero 2 19:40.22, Processing file /hyundai-mitsubishi-kia (variation 5)
enero 2 19:40.22, Processing file /hyundai-mitsubishi-kia (variation 8)
enero 2 19:40.22, Processing file /hyundai-mitsubishi-kia/rss
enero 2 19:40.22, Processing file /hyundai-mitsubishi-kia (variation 7)
enero 2 19:40.23, Processing file /volskwagen/rss
enero 2 19:40.23, Processing file /volskwagen (variation 4)
enero 2 19:40.23, Processing file /volskwagen (variation 5)
enero 2 19:40.23, Processing file /hyundai-mitsubishi-kia/atom
enero 2 19:40.23, Processing file /hyundai-mitsubishi-kia (variation 9)
enero 2 19:40.24, Processing file /volskwagen/atom
enero 2 19:40.24, Processing file /volskwagen (variation 8)
enero 2 19:40.24, Processing file /volskwagen (variation 9)
enero 2 19:40.25, Processing file /mack-detroit (variation 1)
enero 2 19:40.25, Processing file /mack-detroit (variation 2)
enero 2 19:40.25, Processing file /mack-detroit (variation 3)
enero 2 19:40.25, Processing file /mack-detroit (variation 4)
enero 2 19:40.32, Processing file /volskwagen (variation 6)
enero 2 19:40.32, Processing file /volskwagen (variation 7)
enero 2 19:40.34, Processing file /mack-detroit (variation 5)
enero 2 19:40.34, Processing file /mack-detroit (variation 6)
enero 2 19:40.35, Open port 993 - imaps
enero 2 19:40.35, Processing file /mack-detroit/rss
enero 2 19:40.35, Open port 995 - pop3s
enero 2 19:40.36, Processing file /mack-detroit/atom
enero 2 19:40.36, Processing file /mack-detroit (variation 9)
enero 2 19:40.37, Processing file /mack-detroit (variation 7)
enero 2 19:40.37, Processing file /mazda (variation 1)
enero 2 19:40.37, Processing file /mazda (variation 3)
enero 2 19:40.38, Processing file /mazda (variation 6)
enero 2 19:40.38, Processing file /mazda/rss
enero 2 19:40.38, Processing file /mazda/atom
enero 2 19:40.39, Processing file /mazda (variation 7)
enero 2 19:40.39, Processing file /mazda (variation 9)
enero 2 19:40.39, Processing file /mack-detroit (variation 8)
enero 2 19:40.39, Processing file /mazda (variation 8)

enero 2 19:40.40, Processing file /mercedes-benz-man (variation 1)
enero 2 19:40.40, Processing file /mercedes-benz-man (variation 2)
enero 2 19:40.40, Processing file /mercedes-benz-man (variation 3)
enero 2 19:40.40, Processing file /mazda (variation 4)
enero 2 19:40.41, Processing file /mazda (variation 2)
enero 2 19:40.41, Processing file /mazda (variation 5)
enero 2 19:40.49, Processing file /mercedes-benz-man (variation 4)
enero 2 19:40.50, Processing file /mercedes-benz-man (variation 5)
enero 2 19:40.50, Processing file /mercedes-benz-man (variation 6)
enero 2 19:40.50, Processing file /mercedes-benz-man (variation 7)
enero 2 19:40.51, Processing file /mercedes-benz-man (variation 8)
enero 2 19:40.51, Processing file /mercedes-benz-man (variation 9)
enero 2 19:40.51, Processing file /modules/mod_moopopup/mod_moopopup.xml
enero 2 19:40.51, Processing file /modules/mod_moopopup/mod_moopopup.php
enero 2 19:40.52, Processing file /templates/turbotechazul/css/editor.css
enero 2 19:40.52, Processing file /templates/turbotechazul/css/template.ie7.css
enero 2 19:40.52, Processing file /templates/turbotechazul/css/template.ie6.css
enero 2 19:40.52, Processing file /mercedes-benz-man/rss
enero 2 19:40.53, Processing file /mercedes-benz-man/atom
enero 2 19:40.54, Processing file /nissan (variation 2)
enero 2 19:40.54, Processing file /nissan (variation 1)
enero 2 19:40.54, Processing file /nissan (variation 3)
enero 2 19:40.54, Processing file /nissan (variation 4)
enero 2 19:40.54, Processing file /nissan (variation 5)
enero 2 19:40.54, Processing file /nissan (variation 6)
enero 2 19:41.03, Processing file /nissan/rss
enero 2 19:41.04, Processing file /nissan/atom
enero 2 19:41.04, Processing file /toyota-daihatsu (variation 1)
enero 2 19:41.05, Processing file /toyota-daihatsu (variation 2)
enero 2 19:41.05, Processing file /toyota-daihatsu (variation 6)
enero 2 19:41.05, Processing file /toyota-daihatsu (variation 3)
enero 2 19:41.05, Processing file /toyota-daihatsu (variation 4)
enero 2 19:41.06, Processing file /toyota-daihatsu (variation 5)
enero 2 19:41.06, Processing file /toyota-daihatsu (variation 7)
enero 2 19:41.10, Processing file /toyota-daihatsu/rss
enero 2 19:41.10, Processing file /toyota-daihatsu/atom
enero 2 19:41.11, Processing file /toyota-daihatsu (variation 8)
enero 2 19:41.12, Processing file /qmc-jac (variation 1)
enero 2 19:41.12, Processing file /qmc-jac (variation 5)
enero 2 19:41.13, Processing file /qmc-jac (variation 7)
enero 2 19:41.13, Processing file /qmc-jac (variation 8)
enero 2 19:41.13, Processing file /qmc-jac/rss
enero 2 19:41.13, Processing file /qmc-jac/atom
enero 2 19:41.13, Processing file /toyota-daihatsu (variation 9)
enero 2 19:41.14, Processing file /qmc-jac (variation 9)
enero 2 19:41.14, Processing file /qmc-jac (variation 3)
enero 2 19:41.14, Processing file /informacion (variation 1)
enero 2 19:41.15, Processing file /informacion (variation 2)
enero 2 19:41.15, Processing file /qmc-jac (variation 2)
enero 2 19:41.15, Processing file /informacion (variation 3)
enero 2 19:41.15, Processing file /informacion (variation 4)
enero 2 19:41.15, Processing file /qmc-jac (variation 4)
enero 2 19:41.16, Processing file /qmc-jac (variation 6)
enero 2 19:41.16, Processing file /informacion (variation 8)
enero 2 19:41.26, Processing file /informacion (variation 5)
enero 2 19:41.26, Processing file /informacion (variation 9)
enero 2 19:41.26, Processing file /informacion (variation 7)
enero 2 19:41.26, Processing file /informacion (variation 6)
enero 2 19:41.29, Processing file /informacion/rss
enero 2 19:41.43, Open port 3306 - mysql
enero 2 19:41.44, Processing file /informacion/atom
enero 2 19:41.45, Processing file /images/stories/catalogo
enero 2 19:41.45, Processing file /index.php (variation 15)
enero 2 19:41.45, Processing file /index.php (variation 14)
enero 2 19:41.46, Processing file /index.php (variation 17)
enero 2 19:41.46, Processing file /index.php (variation 19)

enero 2 19:41.46, Processing file /index.php (variation 16)
enero 2 19:41.46, Processing file /index.php (variation 18)
enero 2 19:41.46, Processing file /index.php (variation 21)
enero 2 19:41.46, Processing file /index.php (variation 20)
enero 2 19:41.46, Processing file /index.php (variation 22)
enero 2 19:41.46, Processing file /index.php (variation 23)
enero 2 19:41.46, Processing file /index.php (variation 24)
enero 2 19:41.46, Processing file /index.php (variation 25)
enero 2 19:41.47, Processing file /index.php (variation 26)
enero 2 19:41.47, Processing file /images/stories/catalogo/Isuzu
enero 2 19:41.47, Processing file /index.php (variation 27)
enero 2 19:41.47, Processing file /index.php (variation 29)
enero 2 19:41.47, Processing file /index.php (variation 28)
enero 2 19:41.47, Processing file /index.php (variation 30)
enero 2 19:41.55, Processing file /images/stories/catalogo/Mazda
enero 2 19:41.56, Processing file /images/stories/catalogo/MercedesBenz-Man
enero 2 19:41.56, Processing file /images/stories/catalogo/Nissan
enero 2 19:41.56, Processing file /images/stories/catalogo/Volskwagen
enero 2 19:41.56, Processing file /images/stories/catalogo/Volvo-Scania
enero 2 19:41.56, Processing file /images/stories/catalogo/Toyota-Daihatsu
enero 2 19:41.57, Processing file /components/com_mailto/assets
enero 2 19:41.57, Processing file /components/com_mailto
enero 2 19:41.59, Processing file /hino (variation 4)
enero 2 19:42.01, Processing file /hino (variation 1)
enero 2 19:42.01, Processing file /hino (variation 2)
enero 2 19:42.01, Processing file /hino/atom
enero 2 19:42.02, Processing file /hino (variation 3)
enero 2 19:42.02, Processing file /hino (variation 6)
enero 2 19:42.03, Processing file /isuzu (variation 1)
enero 2 19:42.03, Processing file /isuzu (variation 2)
enero 2 19:42.03, Processing file /hino (variation 5)
enero 2 19:42.03, Processing file /hino (variation 8)
enero 2 19:42.03, Processing file /hino (variation 7)
enero 2 19:42.03, Processing file /isuzu (variation 3)
enero 2 19:42.04, Processing file /isuzu (variation 4)
enero 2 19:42.04, Processing file /hino/rss
enero 2 19:42.04, Processing file /isuzu (variation 5)
enero 2 19:42.04, Processing file /hino (variation 9)
enero 2 19:42.05, Processing file /isuzu (variation 6)
enero 2 19:42.06, Processing file /isuzu/rss
enero 2 19:42.06, Processing file /isuzu (variation 7)
enero 2 19:42.07, Processing file /isuzu (variation 9)
enero 2 19:42.07, Processing file /isuzu/atom
enero 2 19:42.07, Processing file /isuzu (variation 8)
enero 2 19:42.09, Processing file /plugins/content/plugin_jw_ts/tabs_slides.js
enero 2 19:42.09, Processing file /plugins/content/plugin_jw_ts/tabs_slides_opt_loader.js
enero 2 19:42.10, Processing file /hyundai-mitsubishi-kia/pagina-2
enero 2 19:42.10, Processing file /mercedes-benz-man/pagina-2
enero 2 19:42.10, Processing file /caterpillar-case-komatsu/pagina-2
enero 2 19:42.12, Processing file /hino/pagina-2
enero 2 19:42.12, Processing file /isuzu/pagina-2
enero 2 19:42.12, Processing file /isuzu/pagina-3
enero 2 19:42.13, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 1)
enero 2 19:42.13, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 2)
enero 2 19:42.13, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 3)
enero 2 19:42.14, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 6)
enero 2 19:42.15, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 8)
enero 2 19:42.15, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 7)
enero 2 19:42.15, Processing file /isuzu/pagina-4
enero 2 19:42.16, Processing file /mercedes-benz-man/pagina-2 (variation 2)
enero 2 19:42.16, Processing file /mercedes-benz-man/pagina-2 (variation 1)
enero 2 19:42.16, Processing file /mercedes-benz-man/pagina-2 (variation 4)
enero 2 19:42.18, Processing file /mercedes-benz-man/pagina-2 (variation 6)
enero 2 19:42.18, Processing file /mercedes-benz-man/pagina-2 (variation 7)
enero 2 19:42.18, Processing file /mercedes-benz-man/pagina-2 (variation 8)
enero 2 19:42.18, Processing file /mercedes-benz-man/pagina-2 (variation 9)

enero 2 19:42.18, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 4)
enero 2 19:42.18, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 9)
enero 2 19:42.19, Processing file /mercedes-benz-man/pagina-2 (variation 3)
enero 2 19:42.19, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 5)
enero 2 19:42.20, Processing file /mercedes-benz-man/pagina-2 (variation 5)
enero 2 19:42.20, Processing file /caterpillar-case-komatsu/pagina-2 (variation 2)
enero 2 19:42.20, Processing file /caterpillar-case-komatsu/pagina-2 (variation 3)
enero 2 19:42.20, Processing file /caterpillar-case-komatsu/pagina-2 (variation 1)
enero 2 19:42.22, Processing file /caterpillar-case-komatsu/pagina-2 (variation 4)
enero 2 19:42.23, Processing file /caterpillar-case-komatsu/pagina-2 (variation 6)
enero 2 19:42.23, Processing file /caterpillar-case-komatsu/pagina-2 (variation 5)
enero 2 19:42.23, Processing file /caterpillar-case-komatsu/pagina-2 (variation 8)
enero 2 19:42.23, Processing file /caterpillar-case-komatsu/pagina-2 (variation 7)
enero 2 19:42.26, Processing file /caterpillar-case-komatsu/pagina-2 (variation 9)
enero 2 19:42.29, Processing file /hino/pagina-2 (variation 6)
enero 2 19:42.29, Processing file /hino/pagina-2 (variation 5)
enero 2 19:42.30, Processing file /hino/pagina-2 (variation 1)
enero 2 19:42.31, Processing file /isuzu/pagina-2 (variation 2)
enero 2 19:42.31, Processing file /hino/pagina-2 (variation 2)
enero 2 19:42.31, Processing file /isuzu/pagina-2 (variation 3)
enero 2 19:42.31, Processing file /hino/pagina-2 (variation 4)
enero 2 19:42.31, Processing file /isuzu/pagina-2 (variation 4)
enero 2 19:42.32, Processing file /hino/pagina-2 (variation 8)
enero 2 19:42.33, Processing file /isuzu/pagina-2 (variation 5)
enero 2 19:42.33, Processing file /hino/pagina-2 (variation 3)
enero 2 19:42.33, Processing file /isuzu/pagina-2 (variation 6)
enero 2 19:42.34, Processing file /isuzu/pagina-2 (variation 7)
enero 2 19:42.34, Processing file /isuzu/pagina-2 (variation 1)
enero 2 19:42.34, Processing file /hino/pagina-2 (variation 9)
enero 2 19:42.34, Processing file /isuzu/pagina-2 (variation 8)
enero 2 19:42.34, Processing file /hino/pagina-2 (variation 7)
enero 2 19:42.34, Processing file /isuzu/pagina-2 (variation 9)
enero 2 19:42.34, Processing file /isuzu/pagina-3 (variation 1)
enero 2 19:42.36, Processing file /isuzu/pagina-3 (variation 2)
enero 2 19:42.36, Processing file /isuzu/pagina-3 (variation 3)
enero 2 19:42.37, Processing file /isuzu/pagina-3 (variation 4)
enero 2 19:42.37, Processing file /isuzu/pagina-3 (variation 5)
enero 2 19:42.37, Processing file /isuzu/pagina-3 (variation 6)
enero 2 19:42.37, Processing file /isuzu/pagina-3 (variation 7)
enero 2 19:42.40, Processing file /isuzu/pagina-4 (variation 1)
enero 2 19:42.41, Processing file /isuzu/pagina-4 (variation 3)
enero 2 19:42.41, Processing file /isuzu/pagina-4 (variation 7)
enero 2 19:42.42, Processing file /isuzu/pagina-4 (variation 9)
enero 2 19:42.43, Processing file /isuzu/pagina-4 (variation 8)
enero 2 19:42.44, Processing file /isuzu/pagina-3 (variation 8)
enero 2 19:42.44, Processing file /isuzu/pagina-3 (variation 9)
enero 2 19:42.44, Processing file /isuzu/pagina-4 (variation 2)
enero 2 19:42.44, Processing file /isuzu/pagina-4 (variation 6)
enero 2 19:42.44, Processing file /isuzu/pagina-4 (variation 5)
enero 2 19:42.44, Processing file /isuzu/pagina-4 (variation 4)
enero 2 19:42.44, Analyzing client side JavaScripts
enero 2 19:42.45, Analyzing file: http://www.turbotech.com.ec/
enero 2 19:42.45, Port scanning completed!
enero 2 19:42.45, Analyzing file: http://www.turbotech.com.ec/index.php
enero 2 19:42.46, Analyzing file: http://www.turbotech.com.ec/informacion/mision-vision
enero 2 19:42.46, Analyzing file: http://www.turbotech.com.ec/informacion/productos
enero 2 19:42.46, Analyzing file: http://www.turbotech.com.ec/informacion/news
enero 2 19:42.46, Analyzing file: http://www.turbotech.com.ec/informacion/funcionamiento-diagnostico-y-mantenimieto-de-turbos
enero 2 19:42.46, Analyzing file: http://www.turbotech.com.ec/informacion/informacion
enero 2 19:42.47, Analyzing file: http://www.turbotech.com.ec/informacion/mapa
enero 2 19:42.47, Analyzing file: http://www.turbotech.com.ec/informacion/quienes-somos
enero 2 19:42.47, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:42.47, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/

enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:42.48, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/turbo-cat-950b
enero 2 19:42.49, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/core-para-kodiak
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/cummins-6ct-6cta-y-6ctaa-de-8-3l
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/turbo-cat-320c
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/cummins/cummins-6ct-6cta-y-6ctaa-de-8-3l-sin-intercooler
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/turbos-para-autos-y-motores-a-diesel-reparacion-y-venta-de-turbocargadores-en-marcas-azumi-garret-ihi-turbo-master-power-y-kts
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/cummins/turbo-para-motores-cummins-6btaa-5-9l-e-isb-5-9l
enero 2 19:42.50, Analyzing file: http://www.turbotech.com.ec/cummins/turbo-para-motores-cummins-6ctaa-8-3l
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/cummins-6bt-5-9l-y-6btaa-5-9lt
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/cummins/cummins-6bt-5-9l-y-6btaa-5-9l-130hp-y-160hp
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/turbo-cat-s4kt
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/cummins/turbo-ford-cargo-815
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/turbo-cat-320b
enero 2 19:42.51, Analyzing file: http://www.turbotech.com.ec/hino/turbo-hino-fd-ff-ho6ct-a-r-1-00
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hino/turbo-hino-fd-ff-h06ct-a-r-0-84
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hino/core-para-turbo-super-hino-vx53-motor-h07ct
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hino/turbo-hino-gd-gh-ff-fg-j08ct
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hino/core-para-turbo-hino-gd-gh-ff-fg-motor-j08-ct
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/turbo-para-hyundai-hd72-hd78-y-mitsubishi-canter-moderno
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/turbo-para-hyunday-h1-y-terracane
enero 2 19:42.52, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-tdo5h-para-turbo-de-hyundai-hd72-hd78-y-mitsubishi-canter-4d34
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-tdo6-para-turbos-de-hyundai-y-mitsubishi-4-4-lt-en-marca-kts
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-gt20-para-turbo-de-hyundai-hd65-y-hd72
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hino/turbo-super-hino-vx53-h07ct
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-4-5l-en-marca-kts-con-roseta-de-titanio
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hino/turbo-hino-fd-h06ct-con-caracol-de-escape-original-y-valvula
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-h100
enero 2 19:42.53, Analyzing file: http://www.turbotech.com.ec/hino/turbo-super-hino-h07ct-a-r-0-84
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-para-turbo-de-hyundai-h1-y-terracanece
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-turbo-hyundai-tucson-kia-sportage
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/core-kia-carens
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/hino/core-para-turbo-hino-fb-fc-motor-j05ct
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-isuzu-nhr-nkr
enero 2 19:42.54, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-isuzu-npr-sin-valvula
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-isuzu-npr-antiguo-con-valvula
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-isuzu-ftr
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-isuzu-ftr-2000-2007
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-chevrolet-dmax-3-0
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/turbo-chevrolet-luv-y-luv-d-max
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/core-para-el-isuzu-npr-con-valvula-modelo-1998-2000
enero 2 19:42.55, Analyzing file: http://www.turbotech.com.ec/isuzu/core-chevrolet-luv-motor-2-8l
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/isuzu/core-isuzu-nhr-nkr
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/isuzu/core-para-el-isuzu-npr-sin-valvula
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/mack-detroit/mack-e675-y-676
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/isuzu/core-para-el-isuzu-npr-con-valvula-y-multiple
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/mack-detroit/detroit-serie-60-con-valvula
enero 2 19:42.56, Analyzing file: http://www.turbotech.com.ec/mack-detroit/detroit-serie-60-sin-valvula
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/mack-detroit/detroit-serie-60-sin-valvula-11-1-lt
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/mazda/turbo-mazda-bt-50

enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/isuzu/core-chevrolet-luv-y-luv-d-max-2-2l-y-2-5l
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/isuzu/core-isuzu-ftr
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/mazda/core-turbo-mazda-bt-50
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/cartridge-para-turbo-mercedes-om366
enero 2 19:42.57, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/turbo-mercedes-motor-om366-intercooler-de-alto-rendimiento
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/turbo-ta31
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/isuzu/core-isuzu-ftr-2000-2007
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/isuzu/core-chevrolet-luv-d-max-3-0l
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/turbo-para-mercedes-1728
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/turbo-para-mercedes-benz-om422la-om442la-y-402la
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/turbo-para-mercedes-benz-actros-3348-y-3353
enero 2 19:42.58, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/mercedes-benz-oh1636
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/mercedes-1722
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/mercedes-914-y-915
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/nissan/turbo-para-motores-nissan
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/man-280
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/nissan/core-nissan-frontier-3-0l
enero 2 19:42.59, Analyzing file: http://www.turbotech.com.ec/nissan/core-nissan-frontier-2-5l
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/qmc-jac/qmc-jac-motores-chinos-de-2-7l
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/qmc-jac/qmc-jac-motores-chinos-de-3-3l
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/volskwagen/turbo-volskwagen-17240-17260-con-valvula
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/volskwagen/turbo-volskwagen-9-150
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/volskwagen/turbo-motores-cummins-6ctaa-8-3l
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/volvo-scania/turbo-volvo-n12-nl12edc-f12-b12
enero 2 19:43.00, Analyzing file: http://www.turbotech.com.ec/volvo-scania/turbo-volvo-n10-nl280-b10m-b58
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/volvo-scania/turbo-scania-p94-r300-r320
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/nissan/core-turbo-nissan-pkc212
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/volvo-scania/turbo-scania-124-r400-r420
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/core-turbo-daihatsu-delta-toyota-15b
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2luZm9ybWFjaW9uL21pc2lvbi12aXNpb24=
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/volskwagen/turbo-para-volkswagen-17210-mwm-6-10-tca
enero 2 19:43.01, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=1:informacion&id=2:conozca-mas-de-nuestros-productos-y-servicios&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=2
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2luZm9ybWFjaW9uL3Byb2R1Y3Rvcw==
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/core-toyota-hilux-2-7-td
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=1:informacion&id=88:mision-vision&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=7
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=1:informacion&id=89:news&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=8
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2luZm9ybWFjaW9uL25ld3M=
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=16:informacion&id=92:funcionamiento-diagnostico-y-mantenimieto-de-turbos&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=11
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2luZm9ybWFjaW9uL2Z1bmNpb25hbWllbnRvLWRpYWdub3N0aWNvLXktbWFudGVuaW1pZXRvLWRlLXR1cmJvcw==
enero 2 19:43.02, Analyzing file: http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2luZm9ybWFjaW9uL2luZm9ybWFjaW9u
enero 2 19:43.03, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=16:informacion&id=84:catalogo&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.03, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=1:informacion&id=3:quienes-somos&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=3

enero 2 19:43.03, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29t
LmVjL2luZm9ybWFjaW9uL3F1aWVuZXMtc29tb3M=
enero 2 19:43.03, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.03, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.03, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.04, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:43.05, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.05, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.05, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.05, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.05, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.06, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.07, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.08, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.09, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.10, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.10, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.10, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.10, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.10, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.11, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.12, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.13, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/

enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.14, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.15, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.16, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.17, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.18, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.19, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.20, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.21, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29t
LmVjL2NhdGVycGlsbGFyLWNhc2Uta29tYXRzdS90dXJiby1jYXQtOTUwYg==
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=3:caterpillar-case-
komatsu&id=9:turbo-cat-950b&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.21, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29t
LmVjL2NhdGVycGlsbGFyLWNhc2Uta29tYXRzdS9jb3JlLXBhcmEta29kaWFr
enero 2 19:43.21, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29t
LmVjL2NhdGVycGlsbGFyLWNhc2Uta29tYXRzdS9jdW1taW5zLTZjdC02Y3RhLXktNmN0YWEtZGUtOC0zbA==
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=3:caterpillar-case-
komatsu&id=4:core-para-kodiak&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=3:caterpillar-case-
komatsu&id=6:cummins-6ct-6cta-y-6ctaa-de-
83l&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.21, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29t
LmVjL2NhdGVycGlsbGFyLWNhc2Uta29tYXRzdS90dXJiby1jYXQtMzIwYw==
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=3:caterpillar-case-
komatsu&id=7:turbo-cat-320c&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=4:cummins&id=11:cummins-
6ct-6cta-y-6ctaa-de-83l-sin-intercooler&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.21, Analyzing file:

http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2N1bW1pbnMvY3VtbWlucy02Y3QtNmN0YS15LTZjdGFhLWRlLTgtM2wtc2luLWludGVyY29vbGVy
enero 2 19:43.21, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=4:cummins&id=22:cummins-6btaa-59l-e-isb-59l&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.22, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2N1bW1pbnMvdHVyYm8tcGFyYS1tb3RvcmVzLWN1bW1pbnMtNmJ0YWEtNS05bC1lLWlzYi01LTls
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=4:cummins&id=33:cummins-6ctaa-83l&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.22, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2N1bW1pbnMvdHVyYm8tcGFyYS1tb3RvcmVzLWN1bW1pbnMtNmN0YWEtOC0zbA==
enero 2 19:43.22, Analyzing file:
http://www.turbotech.com.ec/index.php?option=com_mailto&tmpl=component&link=aHR0cDovL3d3dy50dXJib3RlY2guY29tLmVjL2NhdGVycGlsbGFyLWNhc2Uta29tYXRzdS9jdW1taW5zLTZidC01LTlsLXktNmJ0YWEtNS05bHQ=
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=3:caterpillar-case-komatsu&id=5:cummins-6bt-59l-y-6btaa-59lt&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/index.php?view=article&catid=4:cummins&id=34:cummins-6bt-59l-y-6btaa-59l-130hp-y-160hp&tmpl=component&print=1&layout=default&page=&option=com_content&Itemid=4
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.22, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.23, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.23, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.23, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.23, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.23, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.24, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.25, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.25, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.25, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.25, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.25, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.26, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.27, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.28, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.28, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.28, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.28, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.28, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.29, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2

enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.30, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.31, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.32, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.32, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.32, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.32, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.32, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.33, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.34, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.34, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.34, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.34, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.34, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.35, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.36, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.36, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.36, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.36, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.36, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.37, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.37, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.37, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.37, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.37, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.38, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.38, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.38, Script analysis done
enero 2 19:43.41, Processing file /volvo-scania (variation 10)
enero 2 19:43.41, Processing file /caterpillar-case-komatsu (variation 10)
enero 2 19:43.41, Processing file /cummins (variation 10)
enero 2 19:43.41, Processing file /hyundai-mitsubishi-kia (variation 10)
enero 2 19:43.41, Processing file /mazda (variation 10)
enero 2 19:43.41, Processing file /mack-detroit (variation 10)
enero 2 19:43.42, Processing file /nissan (variation 10)
enero 2 19:43.42, Processing file /mercedes-benz-man (variation 10)
enero 2 19:43.44, Processing file /informacion (variation 10)
enero 2 19:43.45, Processing file /hino (variation 10)
enero 2 19:43.45, Processing file /mercedes-benz-man/pagina-2 (variation 10)
enero 2 19:43.45, Processing file /volskwagen (variation 10)
enero 2 19:43.45, Processing file /toyota-daihatsu (variation 10)
enero 2 19:43.45, Processing file /hino/pagina-2 (variation 10)
enero 2 19:43.45, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 10)
enero 2 19:43.45, Processing file /isuzu (variation 10)
enero 2 19:43.45, Processing file /qmc-jac (variation 10)
enero 2 19:43.45, Processing file /caterpillar-case-komatsu/pagina-2 (variation 10)
enero 2 19:43.47, Processing file /isuzu/pagina-2 (variation 10)
enero 2 19:43.47, Processing file /isuzu/pagina-3 (variation 10)
enero 2 19:43.47, Processing file /isuzu/pagina-4 (variation 10)
enero 2 19:43.47, Analyzing client side JavaScripts
enero 2 19:43.47, Analyzing file: http://www.turbotech.com.ec/volvo-scania/

enero 2 19:43.47, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:43.47, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:43.48, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:43.48, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:43.48, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:43.48, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:43.48, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:43.49, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:43.50, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:43.51, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:43.51, Script analysis done
enero 2 19:43.54, Processing file /volvo-scania (variation 11)
enero 2 19:43.54, Processing file /hyundai-mitsubishi-kia (variation 11)
enero 2 19:43.54, Processing file /cummins (variation 11)
enero 2 19:43.54, Processing file /caterpillar-case-komatsu (variation 11)
enero 2 19:43.54, Processing file /mercedes-benz-man (variation 11)
enero 2 19:43.54, Processing file /mazda (variation 11)
enero 2 19:43.54, Processing file /nissan (variation 11)
enero 2 19:43.55, Processing file /mack-detroit (variation 11)
enero 2 19:43.55, Processing file /hino (variation 11)
enero 2 19:43.57, Processing file /mercedes-benz-man/pagina-2 (variation 11)
enero 2 19:43.57, Processing file /toyota-daihatsu (variation 11)
enero 2 19:43.58, Processing file /volskwagen (variation 11)
enero 2 19:43.58, Processing file /hyundai-mitsubishi-kia/pagina-2 (variation 11)
enero 2 19:43.58, Processing file /isuzu (variation 11)
enero 2 19:43.58, Processing file /qmc-jac (variation 11)
enero 2 19:43.58, Processing file /caterpillar-case-komatsu/pagina-2 (variation 11)
enero 2 19:43.58, Processing file /isuzu/pagina-2 (variation 11)
enero 2 19:43.59, Processing file /hino/pagina-2 (variation 11)
enero 2 19:43.59, Processing file /informacion (variation 11)
enero 2 19:43.59, Processing file /isuzu/pagina-4 (variation 11)
enero 2 19:43.59, Processing file /isuzu/pagina-3 (variation 11)
enero 2 19:43.59, Analyzing client side JavaScripts
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/volvo-scania/
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/cummins/
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/
enero 2 19:44.00, Analyzing file: http://www.turbotech.com.ec/mazda/
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/nissan/
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/mack-detroit/
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/hino/
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/mercedes-benz-man/pagina-2
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/toyota-daihatsu/
enero 2 19:44.01, Analyzing file: http://www.turbotech.com.ec/volskwagen/
enero 2 19:44.02, Analyzing file: http://www.turbotech.com.ec/hyundai-mitsubishi-kia/pagina-2
enero 2 19:44.02, Analyzing file: http://www.turbotech.com.ec/isuzu/
enero 2 19:44.02, Analyzing file: http://www.turbotech.com.ec/qmc-jac/
enero 2 19:44.02, Analyzing file: http://www.turbotech.com.ec/caterpillar-case-komatsu/pagina-2
enero 2 19:44.03, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-2
enero 2 19:44.03, Analyzing file: http://www.turbotech.com.ec/hino/pagina-2
enero 2 19:44.03, Analyzing file: http://www.turbotech.com.ec/informacion/
enero 2 19:44.03, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-4
enero 2 19:44.03, Analyzing file: http://www.turbotech.com.ec/isuzu/pagina-3
enero 2 19:44.03, Script analysis done
enero 2 19:44.03, Searching for possible site errors.

enero 2 19:44.03, Searching for aspect alerts.
enero 2 19:44.03, Crawling done.
enero 2 19:44.03, Executing test modules for www.turbotech.com.ec
enero 2 19:44.03, Test module: Parameter manipulation (3 of 12)
enero 2 19:44.03, Populate list of tests ...
enero 2 19:44.03, Populate test items ...
enero 2 19:44.03, Delay 0

enero 2 19:44.03, Parameter manipulation is executing on script "/index.php (1 of 24)" ...

CUANDO SE TRATA DE PROTEGER ACTIVOS DE IMPORTANCIA CRíTICA, NO HAY NADA COMO SAPPHIRE®

El uso de agua como agente de supresión de incendios en zonas en las que existen equipos electrónicos en funcionamiento o en las que se almacenan activos irremplazables de gran valor podría ser tan devastador como el propio incendio. Protéjalos con un sistema de agente limpio ANSUL® SAPPHIRE®, diseñado a medida para suprimir rápidamente incendios y proteger equipos sensibles sin causar daños a las personas o al medio ambiente.

LA DIFERENCIA SALTA A LA VISTA

El corazón del sistema es el revolucionario líquido de protección contra incendios 3M™ Novec™ 1230, un agente limpio transparente, incoloro e inoloro. Almacenado en recipientes en forma líquida, el agente Novec 1230 se evapora instantáneamente durante la descarga, inundando totalmente los espacios protegidos y absorbiendo el calor mejor que el agua. Conjuntamente con la sofisticada central ANSUL AUTOPULSE®, el sistema SAPPHIRE suprime un incendio antes de que empiece a propagarse, detectándolo a niveles invisibles. Una vez pasado el peligro, el agente Novec 1230 se evapora rápidamente sin dañar activos valiosos.

Los sistemas de supresión SAPPHIRE representan la protección contra incendios más eficaz existente hoy en día en el mercado. Estos sistemas son especialmente adecuados para la supresión de incendios en zonas en las que se requiere un medio no conductor de la electricidad, en las que no se puedan desconectar los sistemas electrónicos en caso de emergencia, en las que la limpieza de otros agentes supone un problema o en zonas normalmente ocupadas que precisen el uso de un agente no tóxico.

SUSTITUYE AL HALóN, HFC Y PFC n EFICAZ CONTRA FUEGOS DE CLASE A, B Y C

POTENCIAL NULO DE AGOTAMIENTO DE LA CAPA DE OZONO

REQUISITOS BAJOS DE CONCENTRACIóN DE DISEñO n LISTADO POR UL/ULC,

HOMOLOGADO POR FM Y OTRAS ORGANIZACIONES INTERNACIONALES

ANEXO 4.

NORMA ISO 27001

ESTÁNDAR INTERNACIONAL

ISO/IEC 27001

Primera Edicion
2005 - 10 - 15

Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

---

Tabla de Contenido

Prefacio

ISO (la Organización Internacional para la Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización universal. Los organismos nacionales miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de comités técnicos establecidos por la organización respectiva para lidiar con campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no-gubernamentales, junto con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido u comité técnico conjunto, ISO/IEC JTC 1.

Los Estándares Internacionales son desarrollados en concordancia con las reglas dadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico conjunto con enviados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

Se debe prestar atención a la posibilidad que algunos elementos de este documento estén sujetos a derechos de patente. ISO e IEC no deben ser responsables de la identificación de algún o todos los derechos de patentes.

ISO/IEC 27001 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

0 Introducción

0.1 General

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

0.2 Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información
b) implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) monitorear y revisar el desempeño y la efectividad del SGSI; y
d) mejoramiento continúo en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Figura 1 muestra cómo un SGSI

toma como Insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. La Figura 1 también muestra los vínculos en los procesos presentados en las Cláusulas 4, 5, 6, 7 y 8.

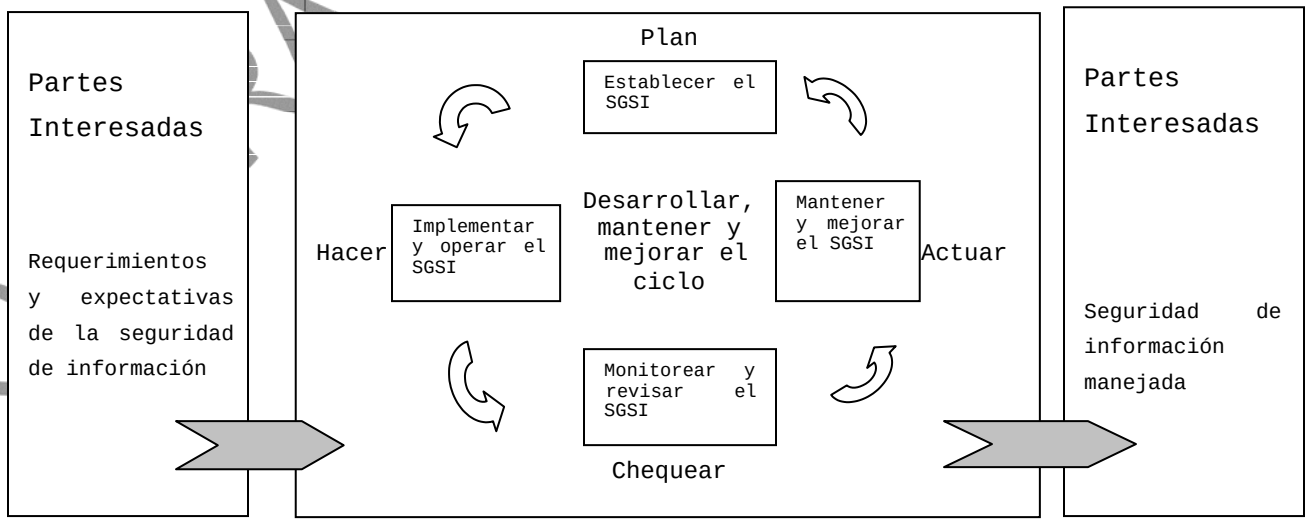
La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD (2002)[1] que gobiernan los sistemas y redes de seguridad de la información Este Estándar Internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

EJEMPLO 1

Un requerimiento podría ser que las violaciones de seguridad de la información no causen daño financiero a la organización y/o causen vergüenza a la organización.

EJEMPLO 2

Una expectativa podría ser que si ocurre un incidente serio –tal vez el pirateo del web site eBusiness de una organización- debería contarse con las personas con la capacitación suficiente en los procedimientos apropiados para minimizar el impacto.



[1] Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. París: OECD, Julio 2002. www.oecd.org.

	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
	Implementar y operar la política, controles, procesos y procedimientos SGSI.
	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Este Estándar Internacional se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares. La Tabla C.1 muestra la relación entre las cláusulas de este Estándar Internacional, ISO 9001:2000 e ISO 14001:2004.

Este Estándar Internacional está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado.

Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Importante – No es el propósito de esta publicación incluir todas las provisiones
necesarias de un contrato. Los usuarios son responsables de su correcta aplicación. El cumplimiento de un Estándar Internacional no quiere decir que

1 Alcance

1.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un contexto de los riesgos comerciales generales de la Especifica requerimientos para la implementación de controles de seguridad personalizados para las

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de
seguridad que protejan los activos de información y den confianza a las

NOTA 1: Las referencias a 'comerciales' en este Estándar Internacional se deben
implementar ampliamente para significar aquellas actividades que son básicas

NOTA 2: ISO/IEC 17799 proporciona un lineamiento de implementación que se puede

1.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

NOTA: Si una organización ya cuenta con un sistema de gestión de procesos comerciales operativos (por ejemplo, en relación con ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requerimientos de este Estándar Internacional dentro de este sistema de gestión existente.

2 Referencias normativas

Los siguientes documentos mencionados son indispensables para la aplicación de este documento. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento citado.

ISO/IEC 17799:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

3 Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

3.1
activo

cualquier cosa que tenga valor para la organización
(ISO/IEC 13335-1:2004)

3.2
disponibilidad

la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada
(ISO/IEC 13335-1:2004)

3.3

confidencialidad

la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

(ISO/IEC 13335-1:2004)

3.4

seguridad de información

preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad

(ISO/IEC 17799:2005)

3.5

evento de seguridad de la información

una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

(ISO/IEC TR 18044:2004)

3.6

incidente de seguridad de la información

un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

(ISO/IEC TR 18044:2004)

3.7

sistema de gestión de seguridad de la información SGSI

esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

NOTA: El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos

3.8

integridad

la propiedad de salvaguardar la exactitud e integridad de los activos.

(ISO/IEC 13335-1:2004)

3.9

riesgo residual

el riesgo remanente después del tratamiento del riesgo

(ISO/IEC Guía 73:2002)

3.10

aceptación de riesgo

decisión de aceptar el riesgo

(ISO/IEC Guía 73:2002)

3.11

análisis de riesgo

uso sistemático de la información para identificar fuentes y para estimar el riesgo

(ISO/IEC Guía 73:2002)

valuación del riesgo

proceso general de análisis del riesgo y evaluación del riesgo

(ISO/IEC Guía 73:2002)

3.13

evaluación del riesgo

proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo

(ISO/IEC Guía 73:2002)

3.14

gestión del riesgo

actividades coordinadas para dirigir y controlar una organización con relación al riesgo

(ISO/IEC Guía 73:2002)

3.15

tratamiento del riesgo

proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo

(ISO/IEC Guía 73:2002)

NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

3.16

enunciado de aplicabilidad

enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

NOTA: Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la organización para la seguridad de la información.

4 Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA que se muestra en la Figura 1.

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance (ver 1.2).

b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

   1) incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;

   2) tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;

   3) esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;

   4) establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);

   5) haya sido aprobada por la gerencia.

NOTA: Para propósitos de este Estándar Internacional, la política SGSI es considerada como un super-conjunto de la política de seguridad de la información. Estas políticas se pueden describir en un documento.

c) Definir el enfoque de valuación del riesgo de la organización

1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.

2) Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

NOTA: Existen diferentes metodologías para el cálculo del riesgo. Los ejemplos de las metodologías de cálculo del riesgo se discuten en ISO/IEC TR 13335-3, Tecnología de información – Lineamiento para la gestión de la Seguridad TI – Técnicas para la gestión de la Seguridad TI

d) Identificar los riesgos

1) Identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos.

2) Identificar las amenazas para aquellos activos.

3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.

4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analizar y evaluar el riesgo

1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.

3) Calcular los niveles de riesgo.

---

[2] El término ‘propietario’ identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término ‘propietario’ no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

4) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).

f) Identificar y evaluar las opciones para el tratamiento de los riesgos

Las acciones posibles incluyen:

1) aplicar los controles apropiados;

2) aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo (ver 4.2.1 c)2)) de la organización

3) evitar los riesgos; y

4) transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores.

g) Seleccionar objetivos de control y controles para el tratamiento de riesgos

Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento de riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver 4.2.1(c), así como los requerimientos legales, reguladores y contractuales.

Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.

NOTA: El Anexo A contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones. Se dirige a los usuarios de este Estándar Internacional como un punto de inicio para la selección de controles para asegurar que no se pase por alto ninguna opción de control importante.

h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

i) Obtener la autorización de la gerencia para implementar y operar el SGSI.

j) Preparar un Enunciado de Aplicabilidad

Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1 (g) y las razones para su selección

2) los objetivos de control y controles implementados actualmente (ver 4.2.1 (e) 2); y

3) la exclusión de cualquier objetivo de control y control en el Anexo A y la justificación para su exclusión.

NOTA: El Enunciado de Aplicabilidad proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo. El justificar las exclusiones proporciona un chequeo para asegurar que ningún control haya sido omitido inadvertidamente.

4.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información (ver 5).

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1(g) para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3 c)).

NOTA: La medición de la efectividad de los controles permite a los gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

e) Implementar los programas de capacitación y conocimiento (ver 5.2.2).

f) Manejar las operaciones del SGSI.

g) Manejar recursos para el SGSI (ver 5.2).

h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad.

4.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:

   1) detectar prontamente los errores en los resultados de procesamiento;

   2) identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos;

   3) permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;

   4) ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y

   5) determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorias de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:

   1) la organización;
   2) tecnología;
   3) objetivos y procesos comerciales;
   4) amenazas identificadas;
   5) efectividad de los controles implementados; y
   6) eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

e) Realizar auditorias SGSI internas a intervalos planeados (ver 6).

   NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI (ver 7.1).

g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI (ver 4.3.3).

4.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

b) Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

4.3 Requerimientos de documentación

4.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles.

Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI.

La documentación SGSI debe incluir lo siguiente:

a) enunciados documentados de la política SGSI (ver 4.2.1b)) y los objetivos;
b) el alcance del SGSI (ver 4.2.1a));
c) procedimientos y controles de soporte del SGSI;
d) una descripción de la metodología de evaluación del riesgo (ver 4.2.1c));
e) reporte de evaluación del riesgo (ver 4.2.1c) a 4.2.1g));
f) plan de tratamiento del riesgo (ver 4.2.2b));
g) Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c));
h) registros requeridos por este Estándar Internacional (ver 4.3.3); y
i) Enunciado de Aplicabilidad.

NOTA 1: Cuando aparece el término 'procedimiento documentado' dentro este Estándar Internacional, significa que el procedimiento se establece, documenta, implementa y mantiene.

NOTA 2: La extensión de la documentación SGSI puede diferir de una organización a otro debido a:

- el tamaño de la organización y el tipo de sus actividades; y
- el alcance y complejidad de los requerimientos de seguridad y el sistema que se está manejando.

NOTA 3: Los documentos y registros pueden estar en cualquier forma o medio.

4.3.2 Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones gerenciales necesarias para:

a) aprobar la idoneidad de los documentos antes de su emisión;
b) revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos;
c) asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos;

d) asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
e) asegurar que los documentos se mantengan legibles y fácilmente identificables;
f) asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;
g) asegurar que se identifiquen los documentos de origen externo;
h) asegurar que se controle la distribución de documentos;
i) evitar el uso indebido de documentos obsoletos; y
j) aplicarles una identificación adecuada si se van a retener por algún propósito.

4.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.

EJEMPLO
Son ejemplos de registros los libros de visitantes, los registros de auditoria y las solicitudes de autorización de acceso.

5 Responsabilidad de la gerencia

5.1 Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

a) establecer una política SGSI;
b) asegurar que se establezcan objetivos y planes SGSI;
c) establecer roles y responsabilidades para la seguridad de información;
d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;

e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1);
f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
g) asegurar que se realicen las auditorías internas SGSI (ver 6); y
h) realizar revisiones gerenciales del SGSI (ver 7).

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

a) establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;
b) asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
c) identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
d) mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
e) llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
f) donde se requiera, mejorar la efectividad del SGSI.

5.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para:

a) determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
b) proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el persona competente) para satisfacer estas necesidades;
c) evaluar la efectividad de las acciones tomadas;
d) mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (ver 4.3.3).

La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueder contribuir al logro de los objetivos SGSI.

6 Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

a) cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes;
b) cumplen con los requerimientos de seguridad de la información identificados;
c) se implementan y mantienen de manera efectiva; y
d) se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir e criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros (ver 4.3.3) se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación (ver 8).

NOTA: ISO 19011:2002, Lineamiento para auditar sistemas de gestión de calidad y/o ambiental, puede proporcionar un lineamiento útil para llevar a cabo auditorías internas.

7 Revisión Gerencial del SGSI

7.1 General

La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros (ver 4.3.3).

7.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

a) resultados de auditorias y revisiones del SGSI;
b) retroalimentación de las partes interesadas;
c) técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
d) status de acciones preventivas y correctivas;
e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
f) resultados de mediciones de efectividad;
g) acciones de seguimiento de las revisiones gerenciales previas;
h) cualquier cambio que pudiera afectar el SGSI; y
i) recomendaciones para el mejoramiento.

7.3 Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente:

a) mejoramiento de la efectividad del SGSI;
b) actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
c) modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    1) requerimientos comerciales;
    2) requerimientos de seguridad;
    3) procesos comerciales que afectan los requerimientos comerciales existentes;
    4) requerimientos reguladores o legales;
    5) obligaciones contractuales; y
    6) niveles de riesgo y/o criterio de aceptación del riesgo.
d) necesidades de recursos;
e) mejoramiento de cómo se mide la efectividad de los controles.

8 Mejoramiento del SGSI

8.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

a) identificar las no-conformidades;
b) determinar las causas de las no-conformidades;
c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
d) determinar e implementar la acción correctiva necesaria;
e) registrar los resultados de la acción tomada (ver 4.3.3); y
f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

a) identificar las no-conformidades potenciales y sus causas;
b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
c) determinar e implementar la acción preventiva necesaria;
d) registrar los resultados de la acción tomada (ver 4.3.3); y
e) revisar la acción preventiva tomada.

La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo.

NOTA La acción para evitar las no-conformidades con frecuencia es más una acción efectiva en costo que la acción correctiva.

Los objetivos de control y los controles enumerados en la Tabla A.1 se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en 4.2.1.

El BS ISO/IEC 17799:2005 Cláusulas del 5 al 15 proporciona consulta y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en A.5 al A.15.

Tabla A.1 – Objetivos de control y controles

Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad

de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
Objetivo	Manejar la seguridad de la información dentro de la organización.	
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
Objetivo Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad'[3] de una parte designada de a organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

[3] Explicación: El término 'propietario' identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

Objetivo Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las

[4] Explicación: Aquí la palabra 'empleo' se utiliza para abarcar todas las siguientes situaciones diferentes: empleo de personas (temporal o larga duración), asignación de roles laborales, cambios de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

		responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
Objetivo Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

27

A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1		Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información	Control

	disponible públicamente	Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1		Control Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2		Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		

A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de ‘routing’ de redes	Control Se deben implementar controles ‘routing’ para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la

		identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de

		procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
Objetivo Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la

		organización.
Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
Objetivo Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los

	continuidad comercial	requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
Objetivo Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1		Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2		Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoria de los sistema de información.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Los principios dados en los Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información [1] se aplican a toda las políticas y niveles operacionales que gobiernan la seguridad de los sistemas y redes de información. Este Estándar Británico proporciona un marco referencial del sistema de gestión de la seguridad de la información para implementar algunos de los principios OECD utilizando el modelo PDCA y los procesos descritos en las Cláusulas 4, 5, 6 y 8 como se indica en la Tabla B.1.

Tabla B.1 – Principios OECD y el modelo PDCA

	Esta actividad es parta de la fase

Los participantes deben estar al tanto de la necesidad de seguridad de los sistemas y redes de información y lo que pueden hacer para aumentar la seguridad	(ver 4.2.2 y 5.2.2)
Todos los participantes son responsables de la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase (ver 4.2.2 y 5.1)
Los participantes deben actuar de manera oportuna y cooperativa para evitar, detectar y responder a los incidentes de seguridad.	Esta es en parte una actividad de monitoreo de la fase (ver 4.2.3 y 6 al 7.3) y una actividad de respuesta de la fase (ver 4.2.4 y 8.1 al 8.3). Esto también puede ser abarcado por algunos aspectos de las fases y .
Los participantes deben realizar evaluaciones de riesgo.	Esta actividad es una parte de la fase (ver 4.2.1) y la evaluación del riesgo es parte de la fase (ver 4.2.3 y 6 al 7.3).
Los participantes deben incorporar la seguridad como un elementos esencial de los sistemas y redes de información.	Una vez que se ha completado la evaluación del riesgo, se seleccionan los controles para el tratamiento de riesgos como una parte de la fase (ver 4.2.1). La fase (ver 4.2.2 y 5.2) entonces abarca la implementación y uso operacional de estos controles.
Los participantes deben adoptar un enfoque integral para la gestión de la seguridad.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta a los incidentes, mantenimiento continuo, revisión y auditoria. Todos estos aspectos son parte de las fases
Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información, y realizar las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos.	La reevaluación de la seguridad de la información es una parte de la fase (ver 4.2.3 y 6 a 7.3) donde se deben realizar revisiones regulares para chequear la efectividad del sistema de gestión de seguridad de la información, y mejorar la seguridad es parte de la fase (ver 4.2.4 y 8.1 al 8.3).

7.1 General 7.2 Insumo de la revisión 7.3 Output de la revisión	5.6.1 General 5.6.2 Insumo de la revisión 5.6.3 Output de la revisión	
8.1 Mejoramiento continuo 8.2 Acción correctiva 8.3 Acción preventiva	8.5.2 Mejoramiento continuo 8.5.3 Acciones correctivas 8.5.3 Acciones preventivas	4.5.3 No-conformidad y acción correctiva y preventiva

Bibliografía

Publicación de estándares

(1) ISO 9001:2000, Sistemas de gestión de calidad - Requerimientos

(2) ISO/IEC 13335-1:204, Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones

(3) ISO/IEC TR 13335-3:1998,

(4) ISO/IEC 13335-4:2000,

(5) ISO 14001:2004, Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso

(6) ISO/IEC TR 18044:2004, Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información

(7) ISO/IEC 19011:2002, Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental

(8) ISO/IEC Guía 62:1996,

Otras publicaciones

(1) OECD,

. Paris: OECD, Julio 2002, www.oecd.org

(2) NIST SP 800-30, Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información

(3) Deming, W.E., Fuera de la Crisis, Cambridge, Mass:MIT, Centro de Estudios de Ingeniería Avanzada, 1986