REQUERIMIENTOS DE SEGURIDAD PARA IMPLEMENTAR SERVIDORES WEB PUBLICOS

MERLY ROCIO MANTILLA HERNANDEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS FISICO-MECANICAS
ESCUELA DE INGENIERIAS ELECTRICA, ELECTRONICA Y DE TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2006

REQUERIMIENTOS DE SEGURIDAD PARA IMPLEMENTAR SERVIDORES WEB PUBLICOS

MERLY ROCIO MANTILLA HERNANDEZ

Trabajo de grado para optar al título de Especialista en Telecomunicaciones

Orientador

SAMUEL GONZALO PINZON BARROS
Magíster en Ingeniería

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS FISICO-MECANICAS
ESCUELA DE INGENIERIAS ELECTRICA, ELECTRONICA Y DE TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2006

A
Dios por la sabiduría y la fortaleza que ha impreso en mi, a mi madre por toda su paciencia y por los grandes sacrificios que ha hecho por mi, a mi familia quien siempre me ha acompañado y apoyado en todos los proyectos que he emprendido, a Samuel quien desde siempre estuvo dispuesto a colaborarme y a orientarme lo mejor posible, a Juan por su paciencia y ayuda incondicional hasta último momento a pesar de todo y quien siempre creyó que este sueño podía ser realidad , a Oswaldo una persona maravillosa que Dios puso en mi camino y a todos mis amigos las personas más valiosas con las que siempre he podido contar.

Merly

AGRADECIMIENTOS

Expreso mis más sinceros agradecimientos a:

Mg. Samuel Gonzalo Pinzón Barros, director del presente trabajo y docente de la Universidad Industrial de Santander, por su apoyo, confianza, consejos y orientaciones.

Mg. Cesar Duarte, docente de la Universidad Industrial de Santander, por sus aportes y recomendaciones.

A mi familia, por su apoyo incondicional.

A todos mis amigos, en especial a Sylvana, a Diego, y a Gonzalo, quienes en los momentos difíciles supieron apoyarme y ayudarme.

TABLA DE CONTENIDO

TITULO: REQUERIMIENTOS DE SEGURIDAD PARA IMPLEMENTAR SERVIDORES WEB PUBLICOS

AUTOR: MANTILLA HERNANDEZ, Merly Rocío [**]

PALABRAS CLAVES:

Seguridad
Ataques
Autenticación
Fuerza bruta
Suplantación de contenido
Inyección de código SQL
Negación del Servicio
Internet

CONTENIDO:

Dadas las condiciones actuales de vulnerabilidad de los sistemas y de los constantes ataques que a diario sufren los servidores Web, los cuales ocasionan inconvenientes como, perdida de información, duplicación de la misma, modificación de contenidos de forma no autorizada, o no disponibilidad del servicio; surge la necesidad de estudiar las principales amenazas Web de manera que puedan plantearse algunas soluciones que eviten o mitiguen el impacto de las mismas.

Aprovechando la gran cantidad de información disponible y conociendo de la problemática actual en lo que respecta a las amenazas Web, se plantea el estudio de los diversos ataques y vulnerabilidades de un sitio, con el fin de definir los requerimientos para la implementación de un servidor seguro, generando ventajas a nivel de eficiencia y eficacia dentro del sitio y haciéndolo altamente competitivo a nivel tecnológico.

En este documento se presentan temas de interés, iniciando con el concepto de los principales tipos de ataques, las pautas de seguridad para servidores Web públicos, las recomendaciones del Instituto Nacional de Estándares y Tecnología sobre implementación de servidores Web seguros.

[**] Escuela de ingenierías eléctrica, electrónica y de telecomunicaciones
Especialización en telecomunicaciones
Director. Magíster Samuel Gonzalo Pinzón Barros

TITLE: SECURITY REQUIREMENTS TO IMPLEMENT PUBLIC WEB SERVERS

AUTHOR: MANTILLA HERNANDEZ, Merly Rocío [*]

KEYWORDS:

Security
Atacks
Autentication
Gross force
Content supplantation
SQL code injection
Deny of Service
Internet

CONTENTS:

The current conditions of vulnerability of the systems and of the constants attacks that the public Web servers suffer every day, which cause inconveniences as, lost of information, duplication of the same one, modification of contents in a not authorized way, or not availability of the service, are for those reason, that appear the necessity of studying the main Web attacks, so that I can think about some solutions that avoid or mitigate their impact.

Taking advantage of the great quantity of available information and knowing of the current problem in what concerns to the Web attacks, thinks about the study of the diverse attacks and vulnerabilities of a place, with the purpose of defining the requirements for the implementation of a secure server, generating advantages to level of efficiency and effectiveness inside the place and making it highly competitive at technological level.

This document presents several interesting topics, beginning with the concept of the main types of attacks, the security rules for public Web servers, the recommendations of the National Institute of Standard and Technology has more than enough implementation of Web servers insurance.

[*] Escuela de ingenierías eléctrica, electrónica y de telecomunicaciones
Especialización en telecomunicaciones
Director. Magister. Samuel Gonzalo Pinzón Barrios

INTRODUCCION

La extensión de las redes de ámbito mundial, que permite interconectar recursos informáticos de todo tipo, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas crezcan considerablemente y se diversifiquen, y que las medidas adoptadas internamente sean insuficientes.

En los últimos años todos los medios de comunicación han hecho alarde del futuro de las autopistas de la información, cuya semilla está representada por la red Internet. Debido al rápido crecimiento que éste ha tenido, ha permitido mayores formas de ataque a la seguridad de la información, incluyendo los virus, Caballos de Troya[1] y penetración de las redes internas.

A raíz de la interconexión del mundo empresarial a esta red, por ella viaja y se almacena gran información de todo tipo, que abarca desde noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren medidas de seguridad que garanticen la confidencialidad, la integridad y la disponibilidad de los datos. La transmisión electrónica, que permite la obtención y posible manipulación de información privada, y los sabotajes realizados tanto por atacantes externos como internos, están causando últimamente pérdida de grandes cantidades de dinero.

Los servidores Web están en capacidad de recibir solicitudes anónimas desde *clientes* auténticos y liberar solicitudes de información en una manera rápida y eficiente. De tal forma, ellos proveen un portal que puede ser utilizado por usuarios y atacantes igualmente. Por su naturaleza, son complicados programas que demandan un alto nivel de seguridad. El tipo de tecnología que mejor cumple con estas demandas se deduce a través de estudios que se realizan para la implementación de servidores Web seguros.

En la actualidad, la rápida evolución de los sistemas y la masificación de la información hacen que cada vez mas sitios sean vulnerables a ataques, ocasionado con ello múltiples disturbios a nivel de información, seguridad y costos. Es por ello que se busca tener una guía que permita analizar en detalle cada uno de los inconvenientes más destacados en lo que respecta a seguridad Web, así como el ejecutar las recomendaciones de los estudios de vulnerabilidad y las herramientas para configurar sitios seguros, logrando con esto tomar decisiones acertadas que minimicen los riesgos ante posibles ataques. Además, se toma como referencia a los diferentes entes que hoy día trabajan en la consolidación de

[1] Programas diseñados con el propósito de introducirse en un sistema de cómputo, infectar archivos y programas, para ejecutarse cada vez que se activa uno de estos y tienen como misión distribuir copias del mismo. Usualmente el daño se limita a borrar y alterar archivos. Los "Caballos de Troya", usualmente vienen ocultos dentro de un programa de manera oculta y se introducen al sistema.

servidores Web seguros, como es el caso de Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América (NIST) y el Web Application Security Consortium.[2]

En el presente libro se esbozarán los diferentes tipos de ataques a la seguridad Web, como tópico de gran importancia para los desarrolladores de aplicaciones, profesionales de la seguridad Web, entre otros. De igual forma, se presentaran los lineamientos y guías para el diseño, la implementación, y la operación de servidores Web públicos seguros.

[2] http://csrc.nist.gov/publications/nistpubs/index.html
http://www.webappsec.org/projects/threat/

OBJETIVOS

GENERAL:

Diseñar una guía de seguridad para la implementación de Servidores Web.

ESPECIFICOS:

- Estudiar y analizar los diferentes tipos de amenazas Web presentes actualmente, así como las vulnerabilidades que explotan.

- Realizar el análisis de los requerimientos para implementar un servidor Web seguro, evaluando y seleccionando un Sistema Operativo adecuado para la implementación de herramientas de seguridad informática en servidores de Web.

- Dar las recomendaciones más acertadas para mitigar la posibilidad de ataques exitosos.

- Establecer mecanismos y métodos eficaces con enfoque activo hacia la seguridad de la información para ser implementados al sistema.

1. ESTADO DEL ARTE

Teniendo en cuenta la globalización de la información que cada día hace, que ésta se valore y se aprecie más en cada una de las organizaciones, el desarrollo de estrategias de seguridad para minimizar los riesgos y debilitar las vulnerabilidades existentes no ha sido ajeno al desarrollo y avance de la misma información.

Hoy en día las empresas han tomado conciencia del valor de la información y es por ello que el desarrollo de políticas y estrategias de seguridad mantienen a las organizaciones actualizadas frente a estos temas. Es así como muchas de ellas invierten grandes sumas de dinero para garantizar la integridad, confidencialidad y disponibilidad de la información.

Según un estudio de la Universidad de Texas, sólo el 6% de las empresas que sufren un desastre informático sobreviven. El 94% restante tarde o temprano desaparece. Es por esto que Hitachi Data Systems asegura que el mercado de almacenamiento de datos crecerá alrededor de un 12% anual hasta 2008.

El desarrollo de nuevas tecnologías para el aseguramiento de la información, así como la implementación de estrategias de seguridad, permiten a los usuarios de los diferentes tipos de sistemas operativos tener una serie de herramientas para proteger sus activos. Existe un constante esfuerzo por entregar a los usuarios una experiencia de computación más segura y confiable, Se han realizado considerables progresos durante los últimos años en lo que respecta a la seguridad, con logros tales como una mayor conciencia por parte de los clientes sobre la existencia de correo electrónico no deseado, virus y otras amenazas de seguridad, así como la disponibilidad de protección más efectiva y potente contra ataques a software y agujeros de seguridad, ofreciendo mayor seguridad a los clientes

A pesar de que se han incrementado las medidas de seguridad, en esta misma medida continúan evolucionando las amenazas de seguridad, de igual forma, se siguen realizando importantes avances en el desarrollo de productos más seguros y en la entrega de guías y herramientas para ayudar a reforzar tecnologías de seguridad existentes.

En sus inicios los incidentes de seguridad informática se debían casi exclusivamente a errores de configuración por parte de administradores y usuarios. Las vulnerabilidades internas de los programas también causaban problemas, pero no con la frecuencia que se experimentan en la actualidad.

De modo que el panorama de Tecnologías en seguridad de la Información ha ido evolucionando hasta la situación actual, en que los errores en los programas son los responsables de la inmensa mayoría de los incidentes de seguridad informática.

Las causas de estos cambios son en su mayoría debidos a la mayor cantidad y calidad en la documentación que indica cómo instalar un programa; lo que reduce la presencia de sistemas mal instalados.

Sin embargo los programadores siguen cometiendo errores de seguridad en sus programas, debido a no necesariamente son expertos en seguridad. De igual forma no existe ninguna asignatura de "programación segura" en los currículos de universidades e institutos.

2. CLASIFICACIÓN DE AMENAZAS

En este capitulo el lector podrá situarse dentro del entorno tecnológico que envuelve cada una de las amenazas presentes hoy día en la gran mayoría de los sistemas informáticos. Se podrá conocer un poco más en detalle a cerca de la relación entre vulnerabilidades, las amenazas y el riesgo, así como en el impacto que producen. De igual forma se explicarán en detalle cada una de las formas de amenazas más aplicadas.

En el marco teórico muestran los conceptos básicos que hacen alusión al tema de esta monografía, **i**niciando los principales conceptos de las seguridad de la información, así como la clasificación de las principales amenazas Web, con el fin de desarrollar y promover una terminología estándar que ubique tanto, a desarrolladores de aplicaciones, como fabricantes de software y profesionales de seguridad en un marco cuyo lenguaje sea consistente, para estudiar las principales amenazas Web de manera que se puedan plantear algunas soluciones que mitiguen el impacto de dichos ataques.

2.1 MARCO TEORICO

Seguridad de la información:

Muchas organizaciones son amenazadas frecuentemente en sus activos, lo que representa miles o millones de dólares en pérdidas. Las vulnerabilidades en los sistemas de información pueden ocasionar problemas graves, por ello es muy importante comprender los conceptos necesarios para combatirlos y defenderse de posibles ataques a la información.

Desde tiempos atrás, el hombre ha buscado proteger la información importante y valiosa, para que ésta no sea utilizada de manera irregular. En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación, presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes.

La seguridad de la información es un asunto tan importante para todos, pues afecta directamente a los negocios de una empresa o de un individuo. La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de los computadores o incluso en la memoria de las personas que la conocen.

La seguridad de la información consiste en proteger los activos o elementos que forman parte de la comunicación. De esta forma, es necesario proteger, la información, los equipos que la soportan y las personas que la utilizan o usuarios.

Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor. Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

Los elementos que contienen información registrada, se pueden encontrar en medio electrónico o físico y algunos ejemplos de ella son:

- Documentos
- Informes
- Libros
- Manuales
- Correspondencias
- Patentes
- Información de mercado
- Código de programación
- Líneas de comando
- Reportes financieros
- Archivos de configuración
- Planillas de sueldos de empleados
- Plan de negocios de una empresa, etc.

Dentro de las más comunes vulnerabilidades para este tipo de activo se tiene, el robo de documentos, la pérdida de archivos de configuración, entre otros.

En cuanto a los equipos que soportan la información se debe analizar tanto el software, como el hardware.

El software contiene todos los programas de computador que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información, entre ellas están las aplicaciones comerciales, los programas institucionales, los sistemas operativos, entre otros.

Entre las mas posibles vulnerabilidades a las que pueden enfrentarse los equipos que contienen información se tienen, las fallas publicadas de los sistemas operativos y las aplicaciones no reparadas, las cuales pueden representar accesos indebidos a los equipos, usados por hackers y virus.

El hardware representa toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento. Se hablan entonces de servidores, computadores y cualquier otro medio de almacenamiento. Dentro de las principales vulnerabilidades a las que se pueden ver sometidos este tipo de activos se tienen, las fallas eléctricas que pueden ocasionar daño en equipos, inundaciones en centros de cómputo, robo de equipos portátiles.

Proteger los activos significa mantenerlos seguros contra amenazas que puedan afectar su funcionalidad, corrompiéndola, accediéndola indebidamente, o incluso eliminándola o hurtándola. Por tanto, la seguridad de la información tiene como objetivo proteger a estos activos, con base en la preservación de tres principios básicos: integridad, confidencialidad y disponibilidad de la información.

La integridad, nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra. Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada. Integridad es asegurarnos que sólo las personas autorizadas puedan hacer alteraciones en la forma y contenido de una información.

La confidencialidad de la información tiene como propósito asegurar que sólo la persona correcta acceda a la información que se quiere distribuir. Eso significa que los datos deben ser conocidos sólo por un grupo controlado de personas, definido por el responsable de la información. Tener confidencialidad en la comunicación, es la seguridad de que lo que se dijo a alguien o escribió en algún lugar será escuchado o leído sólo por quien tenga ese derecho. Pérdida de confidencialidad significa pérdida de secreto. Si una información es confidencial, es secreta, se deberá guardar con seguridad y no ser divulgada para personas no autorizadas.

Una vez se ha asegurado que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que se debe garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que una información se pueda utilizar, deberá estar disponible. La disponibilidad hace referencia a toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de dicha información. La disponibilidad de la información permite que se utilice cuando sea necesario, que esté al alcance de sus usuarios y destinatarios y que se pueda acceder en el momento en que necesita utilizar.

De igual forma es necesario conocer otros términos inherentes a la seguridad como lo son las amenazas, las vulnerabilidades, los riesgos, las probabilidades y su impacto.

Las amenazas son agentes capaces de explotar las fallas de seguridad que se denominan puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando sus negocios.
Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales se pueden deber a causas naturales o no naturales y causas internas o externas.

Por lo tanto, uno de los objetivos de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten alguno de los principios básicos de la seguridad de la información (integridad, disponibilidad, confidencialidad), causando daños al negocio de las empresas.
Las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia - tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil.

Las amenazas naturales se deben a condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos,

Las amenazas intencionales, son amenazas deliberadas, premeditadas y hacen parte de ellas los fraudes, el vandalismo, los sabotajes, el espionaje, las invasiones y los ataques, los robos y los hurtos de información, entre otras.

Las amenazas involuntarias, son amenazas resultantes de acciones inconscientes de los usuarios, debido a virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

Dentro de las principales amenazas a la información de la empresa se tienen los virus, la divulgación de contraseñas, los hackers, los accesos indebidos, la filtración de información, entre otros.

Los puntos débiles o vulnerabilidades son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información, para de esta manera dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección. La existencia de puntos débiles está relacionada con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se está utilizando. Otro objetivo de la seguridad de la información es la corrección de puntos débiles existentes en el ambiente en que se usa la información, con el objeto de reducir los riesgos a que está sometida, evitando así la concretización de una amenaza.

Entre los principales tipos de vulnerabilidades se tiene, las físicas, las naturales, de hardware, de software, de medios de almacenamiento, de comunicación y las vulnerabilidades del tipo humano.

El *World Wide Web* (WWW) es el principal sistema para intercambiar información en Internet. La Web se puede dividir en dos componentes principales: Los servidores *Web*, que se usan para garantizar la disponibilidad de la información en Internet (esencialmente publican la información) y los *Browsers* (clientes), que se utilizan para tener acceso y para visualizar la información almacenada en los servidores *Web*. Los servidores Web son los más comúnmente atacados en la red, en consecuencia, es esencial asegurar los servidores Web y la infraestructura tecnológica que los soporta.

Las amenazas específicas de seguridad para los servidores Web se pueden ubicar dentro de las siguientes categorías:

Hackers:

- Los atacantes pueden crear gusanos de software en el servidor Web, alterando el sistema operativo, o el contenido activo del servidor, para tener un acceso no autorizado a él. Algunos ejemplos de accesos no autorizados revelan intrusiones a carpetas o archivos que no pueden ni deben ser consultadas o manipuladas por el público, los cuales ejecutan ordenes privilegiadas y/o instalan software en el Servidor Web.

Ataques lógicos:

- El ataque de Negación del Servicio (DoS), se puede dirigir directamente sobre el Servidor Web, ocasionando que durante el ataque los usuarios válidos o clientes no puedan tener acceso a dicho Servidor.

- La información importante del Servidor Web, puede ser distribuida a individuos no autorizados.

- Información sensible no encriptada, puede ser interceptada cuando es transmitida entre el Servidor Web y el Browser.

- La información del Servidor Web puede ser cambiada para propósitos malévolos. La desconfiguración del sitio Web es un ejemplo comúnmente reportado por esta amenaza.

- Los atacantes pueden tener el acceso no autorizado a los recursos, en cualquier parte de la red de una organización por medio de un ataque efectivo contra el Servidor Web.

- Entidades malévolas pueden atacar organizaciones externas comprometiendo el Servidor Web y encubriendo sus identidades reales, y quizás haciendo que la organización atacada se vea obligada a responder por los daños.

- El servidor Web puede ser utilizado como punto de distribución de software, herramientas de ataque, o copias de pornografía ilegal, quizás haciendo que la organización esté obligada a responder por los daños.

2.2 TIPOS DE ATAQUES

Los principales tipos de ataques según su forma de interferir con la información se clasifican de la siguiente forma:

Autenticación	
1	**Fuerza Bruta** *Un ataque de fuerza bruta es un proceso automatizado de prueba y error utilizado para adivinar un nombre de usuario, contraseña, número de tarjeta de crédito o clave criptográfica.*
2	**Autenticación Insuficiente** *La autenticación insuficiente ocurre cuando un sitio web permite a un atacante acceder a contenido sensible o funcionalidades sin haberse autenticado correctamente.*
3	**Débil Validación en la Recuperación de Contraseñas** *La débil validación en la recuperación de contraseñas se produce cuando un sitio web permite a un atacante obtener, modificar o recuperar, de forma ilegal, la contraseña de otro usuario.*
Autorización	
4	**Predicción de Credenciales/Sesión** *La predicción de credenciales/sesión es un método de secuestro o suplantación de un usuario del sitio web.*
5	**Autorización Insuficiente** *La autorización insuficiente se produce cuando un sitio web permite acceso a contenido sensible o funcionalidades que deberían requerir un incremento de las restricciones en el control de acceso.*
6	**Expiración de Sesión Insuficiente** *La expiración de sesión insuficiente se produce cuando un sitio web permite a un atacante reutilizar credenciales de sesión o IDs de sesión antiguos para llevar a cabo la autorización.*

7	**Fijación de Sesión** *La fijación de sesión es una técnica de ataque que fuerza al ID de sesión de un usuario a adoptar un valor determinado.*
Ataques en la parte cliente	
8	**Suplantación de Contenido** *La suplantación de contenido es una técnica de ataque utilizada para engañar al usuario haciéndole creer que cierto contenido que aparece en un sitio web es legítimo, cuando en realidad no lo es.*
9	**Cross-site Scripting** *Cross-site Scripting (XSS) es una técnica de ataque que fuerza a un sitio web a repetir código ejecutable facilitado por el atacante, y que se cargará en el navegador del usuario.*
Ejecución de comandos	
10	**Desbordamiento de Buffer** *La explotación de un desbordamiento de buffer es un ataque que altera el flujo de una aplicación sobreescribiendo partes de la memoria.*
11	**Ataques de Formato de Cadena** *Los ataques de formato de cadena alteran el flujo de una aplicación utilizando las capacidades proporcionadas por las librerías de formato de cadenas para acceder a otro espacio de memoria.*
12	**Inyección LDAP** *La inyección LDAP es una técnica de ataque usada para explotar sitios web que construyen sentencias LDAP a partir de datos de entrada suministrados por el usuario.*
13	**Comandos de Sistema Operativo** *Los comandos de sistema operativo es una técnica de ataque utilizada para explotar sitios web mediante la ejecución de comandos de sistema operativo a través de la manipulación de las entradas a la aplicación.*
14	**Inyección de código SQL** *La inyección de código SQL es una técnica de ataque usada para explotar sitios web que construyen sentencias SQL a partir de entradas facilitadas por el usuario.*
15	**Inyección de código SSI** *La inyección de código SSI (Server-side Include) es una técnica de explotación en la parte servidora que permite a un atacante enviar código a una aplicación web, que posteriormente será ejecutado localmente por el servidor web.*
16	**Inyección XPath** *La inyección XPath es una técnica de ataque utilizada para explotar sitios web que construyen consultas Xpath con datos de entrada facilitados por el usuario.*
Revelación de información	

17	**Indexación de Directorio** *La indexación/listado automático de directorio es una función del servidor web que lista todos los ficheros del directorio solicitado si no se encuentra presente el fichero de inicio habitual.*
18	**Fuga de Información** *La fuga de información se produce cuando un sitio web revela información sensible, como comentarios de los desarrolladores o mensajes de error, que puede ayudar a un atacante para explotar el sistema.*
19	**Path Traversal** *La técnica de ataque Path Traversal fuerza el acceso a ficheros, directorios y comandos que potencialmente residen fuera del directorio "document root" del servidor web.*
20	**Localización de Recursos Predecibles** *La localización de recursos predecibles es una técnica de ataque usada para descubrir contenido y funcionalidades ocultas en el sitio web.*
Ataques lógicos	
21	**Abuso de Funcionalidad** *El abuso de funcionalidad es una técnica de ataque que usa las propias capacidades y funcionalidades de un sitio web para consumir, estafar o evadir mecanismos de control de acceso.*
22	**Denegación de Servicio** *La denegación de servicio (Denial of Service, DoS) es una técnica de ataque cuyo objetivo es evitar que un sitio web permita la actividad habitual de los usuarios.*
23	**Anti-automatización Insuficiente** *La anti-automatización insuficiente se produce cuando un sitio web permite a un atacante automatizar un proceso que sólo debe ser llevado a cabo manualmente.*
24	**Validación de Proceso Insuficiente** *La validación de proceso insuficiente se produce cuando un sitio web permite a un atacante evadir o engañar el flujo de control esperado por la aplicación.*

Tabla No. 1. Resumen de los principales tipos de ataques[3]

- **Autenticación**

  Contempla ataques cuyo objetivo es el método utilizado por un sitio Web para validar la identidad de un usuario, servicio o aplicación. La autenticación es realizada usando al menos uno de estos tres mecanismos:

[3] Tomado del documento *Clasificación de Amenazas:* Web Application Security Consortium: ww*w.webappsec.org*

"algo que se tiene ", "algo que se conoce" o “algo que se es ". Entre ellos podemos contemplar, los ataques por fuerza bruta, la autentificación insuficiente y la débil validación en la recuperación de contraseñas.

- **Autorización**

Cubre los ataques que tienen como objetivo un método de los sitios Web para determinar si un usuario, servicio o aplicación tiene los permisos necesarios para ejecutar una acción solicitada. Los privilegios a los que tienen acceso los usuarios deben ser restringidos, en aras de proteger la integridad de los servidores, en algunos casos, muchos sitios Web sólo permiten a ciertos usuarios acceder a contenidos o funcionalidades específicos, mientras que en otros casos, los accesos a ciertos recursos pueden estar restringidos. Usando varias técnicas, un atacante puede introducirse dentro de un sitio Web incrementando sus privilegios hacia áreas protegidas. Algunos métodos de los que se valen los atacantes son la predicción de contraseñas, la autorización insuficiente para ingresar a determinado sitio, la no expiración de una sesión y la fijación de una sesión, entre otras.

- **Ataques en la parte cliente**

Se centran en el abuso o aprovechamiento de los usuarios de los sitios Web. Cuando un usuario visita un sitio Web, se establece una relación de confianza entre las dos partes, tecnológica y psicológicamente. El usuario espera que el sitio Web que visita le entregue contenido válido. El usuario también espera que el sitio Web no le ataque durante su permanencia. Teniendo en cuenta estas esperanzas en la relación de confianza, un atacante puede emplear diversas técnicas para aprovecharse del usuario. Entre los métodos mas empleados podemos contar con la suplantación de contenido, que consiste en hacer creer al usuario que el contenido del sitio es legitimo y no proviene de ninguna fuente externa y el *Cross-site scripting,* el cual fuerza a un sitio Web a repetir el código ejecutable suministrado por un atacante, el cual se carga en el navegador del usuario.

- **Ejecución de comandos**

Abarca los ataques diseñados para ejecutar comandos remotos en el sitio web. Todos los sitios web utilizan datos suministrados por el usuario para satisfacer peticiones. A menudo los datos facilitados por el usuario son

usados para crear comandos de construcción resultando en contenido dinámico de una página web. Si este proceso es hecho de forma no segura, un atacante puede alterar la ejecucion de comandos. Entre los métodos mas empleados estan el desbordamiento del buffer, los ataques de formato de cadena, la ejecucion de ciertos comandos del sistema operativo para manipular las entradas a la aplicación y la inyeccion de codigo SQL la cual es usada para explotar sitios web que construyen sentencias SQL directamente a partir de datos facilitados por el usuario.

- **Revelación de información**

  Se centra en ataques diseñados para adquirir información específica del sistema sobre un sitio web. La información específica del sistema incluye la distribución de software, números de versión y niveles de parcheado. La información puede contener la ubicación de ficheros de backup y ficheros temporales. En muchos casos, no se requiere la divulgación de esta información para llevar a cabo las necesidades del usuario. Cuanta más información acerca del sitio web disponga el atacante, más fácil le resultará comprometer el sistema.

- **Ataques lógicos**

  Abarca el abuso o explotación del flujo lógico de una aplicación web. La lógica de la aplicación es el flujo de procedimientos esperados para realizar una cierta acción. Recuperación de contraseñas, puja en subastas, y compras en comercios electrónicos son, todos ellos, ejemplos de lógica de aplicación. Un sitio web puede requerir a un usuario un proceso específico de varios pasos para completar una acción particular. Un atacante puede ser capaz de burlar o abusar de esas características para dañar un sitio web y a sus usuarios.

3. RECOMENDACIONES DE SEGURIDAD

En este capítulo se muestran las diferentes estrategias para mantener servidores Web asegurados, incluyendo la plataforma tecnológica, la aplicación y sus usuarios. En primera instancia se detalla la importancia de un sistema de gestión de seguridad de la información dentro de la organización y posteriormente se especifican los controles de seguridad a implementar en una solución Web.

La seguridad en redes de telecomunicaciones está fundamentada en tres elementos:

La integridad. Hace referencia a que el contenido de la información no se altere al viajar por una red, no obstante el número y tipo de equipos que se encuentren involucrados; la infraestructura utilizada debe ser transparente para el usuario.

La disponibilidad. Implica que el servicio debe estar disponible en el momento que se requiera.

La confidencialidad. Es quizá la parte más estratégica, ya que contribuye a impedir que personas no autorizadas conozcan la información que se transmite.
Otras definiciones: [4]

> *(CONFIDENCIALIDAD) Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.*
>
> *(INTEGRIDAD) Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.*
>
> *(DISPONIBILIDAD) Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.*

La verdadera seguridad de un sistema va más allá de la instalación de la actualización más reciente, la configuración de un cierto archivo, o la cuidadosa administración del acceso de los usuarios a los recursos de sistema. Es una manera de ver las diferentes amenazas que acechan su sistema y lo que se está dispuesto a hacer para evitarlas.
Ningún sistema es totalmente seguro a menos que esté apagado (y aún así, es posible que se lo roben) Cada vez que el sistema esté encendido puede ser

[4] Definiciones tomadas del estándar ISO/IEC 17799:2000 Tecnología de la Información – Código de práctica para la gestión de seguridad de la información. Sección 2. Términos y definiciones, 2.1 Seguridad de la información, página 1.

atacado, desde una broma inocua hasta un virus capaz de destruir el hardware, y la posibilidad que los datos sean eliminados.[5]

Todo usuario de cualquier sistema operativo se enfrenta a un dilema en común al construir un paradigma de seguridad para su sistema. Por un lado, intenta evitar hacer el sistema tan seguro que nada en él funcione correctamente. Pero por otro lado, también trata de evitar dejar el sistema tan inseguro que cualquiera pueda hacerle lo que se le antoje, incluyendo el borrar trabajos de otros o cosas aún peores.

Si un sistema se encuentra en una red, ya sea en red de área local, ó en una red de área extendida o Internet, se debe ser consciente de que el sistema tendrá un nivel más alto de riesgo que si no estuviese conectado a una red.. Además de ataques brutales a los archivos de contraseñas y usuarios sin acceso apropiado, la presencia de un sistema, en una red más grande aumenta la oportunidad de que ocurra un problema de seguridad.

Muchas empresas reaccionan a las amenazas a la seguridad únicamente después de ocasionado el daño. Sin embargo, ésta no es una alternativa viable en el entorno actual, donde las llamadas “amenazas combinadas” están aumentando. Con los múltiples métodos automatizados de ataque, estas amenazas pueden propagarse a gran cantidad de Servidores (*hosts)*, causando daños extendidos rápidamente.

Una de las mejores formas para conocer las múltiples amenazas del ciberespacio, es realizar valoraciones periódicas de las vulnerabilidades, generalmente en asociación con un tercero. Una valoración de las vulnerabilidades evaluará los sistemas, al buscar las soluciones que faltan para los problemas conocidos, con el fin de ayudar a cerciorarse de que la protección del sitio Web esté activada y evitar un ataque potencialmente devastador. Además, una valoración puede evaluar los sistemas de información confidencial más importantes, como la información financiera y personal, los servidores de correo, etc.

Además de identificar vulnerabilidades explícitas de los sitios Web, la valoración también puede ayudar a resaltar las prácticas generales de seguridad de la empresa.

3.1 DESARROLLO DE POLÍTICAS DE SEGURIDAD

[5] Análisis de los requerimientos tecnológicos para la implementación de servidores web seguros (www.monografias.com)

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 organizaciones 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.

Todo sistema, desde una máquina usada sólo por una persona hasta un servidor en el ámbito empresarial utilizado por miles de usuarios, deberá tener políticas de seguridad.

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitivamente. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Las políticas de seguridad son un conjunto de pautas y directrices utilizadas por una organización para orientar a sus integrantes hacía el uso adecuado de sus destrezas tecnológicas y de esta forma obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

El término política de seguridad se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de `términos generales', aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica.

Para la elaboración de políticas de seguridad, el primer paso es hacer una relación de los aspectos sensibles dentro de la organización, tanto físicos (equipos, routers, servidores, etc.), como no físicos (aplicaciones, bases de datos, etc.). Una vez realizada esta lista de puntos sensibles a proteger, se pondera cada uno de ellos con un peso específico, y se calcula la posibilidad de que sea vulnerado, ya sea por ataques intencionados o por causas meramente accidentales.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que proteger

cada recurso. Las medidas diferirán notablemente en función de los usuarios de los que se pretenda proteger el recurso.

Las tres preguntas fundamentales que debe responder cualquier política de seguridad son:

- ¿Qué se quiere proteger?
- ¿Contra quién?
- ¿Cómo?

Cada organización es autónoma de definire cual respuesta a dar los tres interrogantes anteriores y esto es lo que se define como politica de seguridad, la cual debe estar perfectemnte documentada y difundida a toda la organización.

Tìpicamente se define que se deben proteger todos los elementos de la red interna, incluyendo hardware, software, datos, etc. de cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir. De igual forma se deben definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

La respuesta a la tercera pregunta es la más difícil de resolver y la que requiere unas soluciones más dinámicas y cambiantes en lo que se refiere a la vigencia de dicha política de seguridad.

Se pueden plantear distintas soluciones u opciones en varios aspectos :

- **Paradigmas de seguridad:**

  - **Permisivo:** Todo lo que no se prohibe expresamente está permitido
  - **Prohibitivo:** Todo lo que no se permite expresamente está prohibido

  Evidentemente la segunda aproximación es mucho mejor que la primera de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto - las no contempladas - serían consideradas ilegales.

- **Estrategias de seguridad:**

  - Paranoica: consiste en visitar diariamente sitios especializados que publican reportes de vulnerabilidades, para de esta forma estar simpre enterados. Requiere de gran dosis de disciplina y constancia.
  - Prudente: consiste en no ingresar a sitios de dudosa procedencia, donde se pueden albergar miles de medios de ataques.

- Permisiva
- Promiscua

- **Métodos de defensa:**

  - En profundidad
  - Perimetral: el acceso desde el exterior, está centralizado de manera efectiva en un único punto, en el que se concentran la gran mayoría de las medidas.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático:

- **Disponibilidad**

  Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

- **Utilidad**

  Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.

- **Integridad**

  La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

- **Autenticidad**

  El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- **Confidencialidad**

  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

- **Posesión**

  Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados normativas. El estándar ISO 17799[6] define las siguientes líneas de actuación:

- **Seguridad organizacional**

  Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, outsourcing, estructura del área de seguridad).

- **Clasificación y control de activos**

  Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

- **Seguridad del personal**

  Formación en materia de seguridad, clausulas de confidencialidad, reporte de incidentes, monitorización de personal.

- **Seguridad física y del entorno**

  Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos - incluyendo los humanos - de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

- **Gestión de comunicaciones y operaciones**

  Este es uno de los puntos más interesantes desde el punto de vista estrictamente técnico, ya que abarca aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la gestión de copias de seguridad o el intercambio de software dentro de la organización.

- **Controles de acceso**

6 ISO 17799 describe el análisis del Riesgo de la Seguridad y soluciones de la política de la seguridad. Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones

Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos.

- **Desarrollo y mantenimiento de sistemas**

  Seguridad en el desarrollo de las aplicaciones, cifrado de datos, control de software.

- **Gestión de continuidad de negocio**

  Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.

Otros aspectos muy importantes a incorporar en la política de seguridad son :

- Definir claramente el alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Sintetizar los objetivos de la política y elaborar una descripción clara de los elementos involucrados en su definición.
- Definir responsabilidades por cada uno de los servicios y recursos informáticos, aplicado a todos los niveles de la organización.
- Establecer los requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definir responsabilidades de los usuarios con respecto a la información a la que tienen acceso.
- Elaborar procedimientos para reconocer actividades no autorizadas.
- Definir acciones a tomar en caso de incidentes.
- Definir acciones a tomar cuando se sospeche de actividades no autorizadas y sanciones por no cumplir con las políticas. .
- Conseguir que la política sea refrendada por el estamento más alto posible dentro de la organización.
- Divulgar la política de forma eficiente entre los usuarios y administradores.
- Articular medidas de auditoría de nuestro propio sistema de seguridad.
- Establecer plazos de revisión de la política en función de resultados obtenidos.

Una vez se ha definido el modelo de seguridad a utilizar, es necesario definir las herramientas con las que se contará para su implementación práctica

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

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

También se debe identificar quién tiene la autoridad para tomar decisiones en la organización, pues es ella la interesada en salvaguardar sus activos críticos.

Se debe además monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente. De igual forma es necesario llevar a cabo auditorias periodicas a los mecanismos de seguridad implementados a fin de evaluar los resultados obtenidos y que mejoras sustanciales pueden llevarse a cabo.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

3.2 RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

A pesar de que un gran número de organizaciones centran sus esfuerzos en definir directrices de seguridad y concretarlas en documentos, muy pocas alcanzan el objetivo ya que la primera barrera a la que se enfrentan es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

Esta situación ha llevado a que muchas empresas con activos muy esenciales, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información importante y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que los altos directivos de la organización, quienes toman las desiciones, entienden la importancia de la seguridad, conocen los alcances y están de acuerdo con las politicas desarrolladas en relación con esos asuntos.
Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que

toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

3.3 CONTROLES DE SEGURIDAD

Ante la posibilidad de miles de ataques y conociendo cada una de las vulnerabilidades al interior de cada organización, los siguientes hitos se pueden enmarcar dentro de las principales recomendaciones de seguridad y así evitar que un servidor se convierta en el blanco de atacantes.

Un componente importante de la seguridad informática que se debe tener en cuenta para mantener un nivel aceptable de integridad, confidencialidad y disponibilidad, es la existencia de controles de seguridad para los sistemas que se desarollan o se emplean dentro de la organización.

El objetivo principal de estos requerimientos es que sean evaluados por las entidades a las que corresponda esta labor al interior de la organización, para que de esta forma se conviertan en verdaderos controles que prevengan pérdidas, modificaciones o mal uso de la información. Los costos de estos controles deben ser evaluados con respecto a la criticidad de la informacion que se está protegiendo a través de un análisis de riesgos con es fin de maximizar la relacion costo – beneficio.

Las principales recomendaciones para aplicaciones, donde se aseguran las mejores prácticas en cuanto a controles de seguridad, se enuncian a continuación:

- **Almacenamiento de datos:** existe una gran variedad de elementos a consisderar alrededor de una base de datos tales como:
  - Redundancia de datos
  - Consistencia en la información
  - Seguridad y controles de integridad

  Los sistemas de bases de datos alcanzan una gran variedad de tópicos de seguridad. La gran cantidad de información manejada por las bases de datos, incrementa el potencial de robo, así como la divulgación de información no autorizada. Es necesario que los sistemas de bases de datos puedan

automatizar y explotar sus cualidades para dar una mayor seguridad a la información que contienen.

Para tener un almacenamiento de datos eficiente y seguro, es necesario llevar a cabo un ejercicio de clasificación de información.

- **Control de acceso:** es la colección de mecanismos para limitar, controlar y monitorear los accesos de entidades (personas, procesos o dispositivos) a cierta información o los privilegios asociados a cierta entidad o pertenencia de ésta a un grupo predefinido. El control de acceso permite a los administradores y operadores de los sistemas, restringir el comportamiento, uso y contenido del sistema, con el fin de ser congruentes con los criterios de seguridad.

  El control de acceso responde a las siguientes preguntas: ¿Quién o qué debe accesar a los sistemas?, ¿Qué recursos del sistema pueden accesar? Y ¿Cómo deben utilizar dichos recursos?.

  Los métodos de control de acceso incluyen:

  - Identificación de usuarios
  - Contraseñas
  - Controles de login
  - Autorización de recursos
  - Auditorías

  Los controles de acceso lógicos examinan las decisiones que permiten a los usuarios acceder los recursos de los sistemas a través de una autorización que limita el tipo de acceso requerido. El propio sistema utiliza varios criterios para determinar la requisición para el acceso. Este criterio incluye:

  - Identidad (individual o por programa)
  - Rol (individual o grupal)
  - Localización (física o lógica)
  - Tiempo (horario del día, días de la semana)
  - Servicios aplicativos (basados en parámetros)
  - Modos de acceso comunes (lectura, escritura, ejecución, borrado, creación, búsqueda)

  Toda aplicación debe ser robusta y segura, lo cual equivale a la habilidad del sistema para proveer los niveles necesarios de integridad, confidencialidad y disponibilidad. Se requieren servicios de autenticación y autorización con el fin de prevenir accesos no autorizados. Se debe entonces:

- Restringir los accesos no autorizados al sistema a través de la interfase de operación y para las funciones a las cuales se tiene derecho.
- Poseer rastros y bitácoras de eventos para auditorías posteriores.
- Proveer los medios para autenticar la identidad de cualquier otro sistema que intente accesar la información de administración.
- Poseer las alarmas necesarias ante una violación.

❖ **Intercambio de informacion:** se debe garantizar un canal de comunicaicón seguro entre los clientes y los servidores con el objetivo de garantizar la confidencialidad e integridad de la información, cuando ésta sea transmitida.

Algunos puntos que deben cubrir estos protocolos de seguridad son:

- Autenticación del servidor
- Autenticación del cliente
- Integridad de la información
- Encripción de la información

❖ **Operación:** la seguridad no solo abarca lo referente a la infraestructura tecnológica con que cuenta una organización, si no que también está relacionada con ciertos procesos y la gente que los ejecuta. El área de operaciones debe tomar en cuenta ciertas recomendaciones que afectan de manera directa al ambiente de desarrollo y el funcionamiento global del negocio de la empresa. Estas recomendaciones están orientadas a ciertas tareas que dicha área debe efectuar continuamente con el fin de supervisar ciertos procesos de las demás áreas funcionales del negocio.

A continuación se muestran los controles recomendado que surgen de las mejores prácticas y que pueden o no establecerse dependiendo de la criticidad de la información que se quiere proteger.

Las categorías establecidas muestran varios niveles como son los siguientes:

- **Indispensable:** controles mínimos que deben existir en los desarrollos.
- **Necesarios**: controles para lograr una operación relativamente segura de las aplicaciones.
- **Deseable:** controles con los cuales se estaría operando con niveles de seguridad muy altos.

Almacenamiento de datos	
Indispensable	El almacenamiento de las contraseñas de los usuarios de las distintas aplicaciones debe ser ilegible para cualquier entidad.
	Se deben utilizar esquemas de cifrado de un solo sentido para contraseñas (one-way encription)
	Antes de registrar los datos en las bases de datos, las aplicaciones de validar y filtrar la información que proporcionan los usuarios conforme al tipo de datos que se solicita (caracteres numéricos, alfanuméricos o especiales), para evitar que los datos se corrompan.
	Se deben validar las entradas de datos: valores fuera de rango, caracteres inválidos, datos incompletos, número de datos excedido o por debajo del límite.
	La encripción de datos, verificación de precisión y completitud, deberán estar probadas y autorizadas por las reglas de negocio definidas por el usuario.
	Se deberán tener controles que aseguren que las rutinas están seguras contra técnicas salami (por ejemplo ir descontando centavos de las cifras y depositarlas en una cuenta que vaya acumulando estos centavos).
Necesario	La información generada por todas las aplicaciones debe almacenarse en bases de datos que se encuentran en el back-end de la infraestructura, preferentemente protegidas por un dispositivo de seguridad (Firewall, detectores de intrusos, etc.)
	Se encriptarán los datos sensibles dentro de las bases de datos por mecanismos propietarios.
	Se deberán implantar herramientas antivirus y herramientas contra software malicioso, caballos de Troya y puertas traseras.
Deseable	La información personal o privada de la gente que labora en la organización debe estar cifrada.
	Las bitácoras de transacciones deberán almacenarse de forma encriptada, ya sea en una base de datos o en archivos encriptados.
	La captura de datos críticos debe llevarse a cabo a través de un esquema de "doble captura", en donde la información es solicitada dos veces al usuario para evitar registrar información errónea.

Tabla No. 2 Controles para Almacenamiento de Datos

Control de acceso	
Indispensable	Cada usuario tendrá una cuenta única. Si varios operadores tienen la necesidad de compartir la misma cuenta, se deberá poner especial atención al control de acceso de estas cuentas.
	Las distintas interfases de usuario deberán mostrar o habilitar únicamente los menús y/o opciones que correspondan a los servicios con los que cuenta en usuario.
	Las sesiones que un usuario establezca con las distintas aplicaciones deben contar con un tiempo de expiración (time-out) después de no presentarse actividad por un tiempo determinado.

Las aplicaciones deben detectar y/o prohibir múltiples sesiones de una cuenta de usuario al mismo tiempo. Esto con la finalidad de identificar si la cuenta ha sido compartida.
Es necesario que las aplicaciones soporten las políticas de contraseñas que se implementarán con el fin de tener contraseñas robustas y difíciles de descifrar.
Todas las cuentas (administradores, operadores y usuarios) de las aplicaciones deben ser personales, intransferibles y no deben ser compartidas.
Las pantallas de captura de contraseñas no deben desplegarlo al momento de ser introducido por el usuario.
Realizar un cambio de contraseña, los usuarios deben proporcionar la contraseña anterior.
Ninguna contraseña debe almacenarse en el servidor que soporta la aplicación.
Todas las transacciones que efectúe un usuario o cualquier otra entidad autorizada deberán ser registradas en una bitácora (pistas de auditoria) con una etiqueta del usuario, fecha completa y la transacción realizada.
El diseño de las bases de datos debe restringir las vistas de datos que pueden tener distintos perfiles de usuarios con la finalidad de limitar sus acciones.
Debe existir una matriz de privilegios donde se encuentre la relación de permisos contra perfiles. A su vez, los privilegios deben estar estrictamente delimitados (lectura, escritura, lectura/escritura, crear, borrar, etc.)
Las reglas de negocio de las aplicaciones deben ejecutarse en los servidores aplicativos y no en los clientes.
No debe existir bajo ninguna circunstancia una conexión directa entre los usuarios y las bases de datos, estas deben darse siempre a través de las aplicaciones.
No debe existir bajo ninguna circunstancia contraseñas en blanco en cualquier tipo de aplicación...
Las contraseñas no deben vivir bajo ninguna circunstancia en el código (hardcode) de las aplicaciones.
Las funciones permitidas para cada usuario estarán determinadas por grupos de usuarios basados en perfiles. Ningún usuario podrá ver las opciones o funciones que no le corresponden. Por ejemplo: si la aplicación está orientada a menús, el usuario solamente podrá ver el menú correspondiente a su perfil. De la misma forma si la aplicación está orientada a la ejecución de comandos por medio de un intérprete de comandos, el usuario solo podrá ver y ejecutar los comandos correspondientes a su perfil.
Se deberán tomar en cuenta los criterios de seguridad que apliquen para servicios de directorio como el *Active Directy de W2k,* ya que este repositorio se convierte en crítico para la seguridad.
La autenticación de las entidades por las aplicaciones podrán ser: * Un factor. Username y password (algo que se) * Dos factores. Username, password y token o smart card (algo que se y algo que tengo) * Tres factores. Username, password y token o smart card y un control biométrico (algo que se, que tengo y que soy) Estos esquemas deberán estar en función de la clasificación de la aplicación.

Necesario	Las aplicaciones deben bloquear temporal o definitivamente una cuenta de usuario cuando se acumule un cierto número de intentos de *login* fallidos (por ejemplo 5 intentos)
	Una vez que la aplicación ha bloqueado una cuenta de usuario deberá enviar un mensaje de notificación a dicho usuario y al administrador de la aplicación.
	La política de contraseñas debe cumplir características de composición de caracteres (alfanuméricos y caracteres especiales), expiración (3 meses) y longitud (mínimo 8 caracteres)
	Las contraseñas iniciales deben expirar al momento en el que los usuarios entren a las aplicaciones o sistemas por primera vez, con la finalidad que las contraseñas sean conocidas únicamente por los usuarios.
	Con el fin de prevenir que las bitácoras de las transacciones sean modificadas, éstas deben ser firmadas digitalmente por medio de la aplicación que está generando dicha bitácora.
	La autenticación mediante múltiples factores (lo que un sujeto es, conoce y/o posee) mejora la confiabilidad de la autenticación de los sujetos o entidades.
	Se restringirá el acceso físico a los centros de procesamiento de datos.
	Las pistas de auditoría, el uso de esquemas de autentificación y bitacoreo, así como los mecanismos para la integridad y confidencialidad de las transacciones, deberán reforzar el principio de repudiación.
Deseable	Los terminales o estaciones de trabajo podrán ser también autenticadas.
	Las aplicaciones deben garantizar que las contraseñas no sean reutilizadas al menos 6 contraseñas anteriores.
	Si se realizó un cambio de contraseña de manera exitosa, las aplicaciones deberán notificar al usuario mediante un correo sin enviar la nueva contraseña.
	Cualquier modificación o actualización que se realice al perfil de un usuario, deberá notificarse mediante un correo.
	Se deberá mantener un ambiente seguro en el lugar de trabajo de los usuarios de la aplicación, por ejemplo uso de impresoras especiales y bien ubicadas para los reportes de información confidencial.

Tabla No. 3 Mecanismos para lograr el Control de Acceso

Intercambio de datos	
Indispensable	Todas las transacciones de la aplicación deberán ser registradas (bitácora de transacciones) en forma electrónica conteniendo una estampa de al menos los siguientes datos: fecha, hora, solicitante, estatus de la transacción y requerimiento.
	Las aplicaciones clasificadas como críticas y vitales deberán adoptar esquemas de alta disponibilidad o deberán ser tolerantes a fallas.
	Se podrán utilizar mecanismos de transferencia de información segura como túneles, encripción de datos, manejo de firmas y certificados digitales, e incluso infraestructura de llave pública para garantizar la integridad y confidencialidad de la información.

	El manejo de mensajes entre plataformas deberá ser encriptado y además deberán implantarse mecanismos que aseguren que los mensajes fueron recibidos. En ningún momento una aplicación podrá quedarse "sin hacer nada" el usuario deberá conocer el estado de la aplicación. Por ejemplo: errores como fuera de línea, codificación de errores, etc., deberán ser implantados.
Necesario	Todas las conexiones que se establezcan entre los servidores aplicativos y las bases de datos deberán contar con algún esquema de cifrado de canal.
	Las conexiones para las replicaciones de bases de datos deben contar con un túnel construido a partir de una VPN (*Virtual Private Network).*
	En caso de existir réplicas entre bases de datos, debe existir un método de "*Roll back"* y esquemas de "*2 Phase Commit"* para asegurar la consistencia de información. Estos mecanismos aseguran la replicación y sincronización de las bases de datos y garantizan la disponibilidad de la información.
	La conectividad entre plataformas deberá seguir los esquemas de autentificación propuestos para todas las entidades.
Deseable	Todas las conexiones que se realicen entre los usuarios y los servidores aplicativos deberán contar con un canal cifrado.

Tabla No. 4 Controles para intercambio de datos

Operación	
Indispensable	Es necesario contar con una réplica de la información más crítica y/o sensible en una localidad externa al sitio donde se localizan las aplicaciones y/o bases de datos.
	Los servidores de bases de datos y de aplicaciones deben contar con antivirus que previenen la transferencia de archivos infectados y código malicioso.
	La gerencia de desarrollo y Mantenimiento debe efectuar periódicamente análisis de riesgos que le permita identificar el impacto y probabilidad de ocurrencia de riesgos en su infraestructura y aplicaciones.
	Debe existir un proceso de renovación de privilegios y cuentas para usuarios durmientes, ociosos o no utilizados.
	Ningún servidor público (incluyendo Web) debe contener información crítica y/o sensible.
	Se deben efectuar periódicamente pruebas sobre los servidores aplicativos y de bases de datos, con el fin de validar la disponibilidad de los servicios, confidencialidad e integridad de la información. Además todas las aplicaciones deberán ser sometidas a pruebas de seguridad de manera periódica.
	Todas las aplicaciones deberán mantener clara y específicamente separados los módulos de configuración y de función de negocios. El registro de las actividades deberá ser forzoso para ambos módulos.

	El código fuente de las aplicaciones deberá ser protegido de manera adecuada. Se deberán implantar controles que aseguren que la aplicación en producción es realmente la versión liberada por el área de desarrollo de sistemas.
Necesario	La jefatura de desarrollo de sistemas debe contar con planes de continuidad del negocio documentados que describan las instrucciones necesarias para la continuidad de los servicios y la restauración de cualquier servicio que proporcione cada una de las aplicaciones.
	Los planes de contingencia se realizaran tomando como base: la plataforma de hardware, sistema operativo, plataforma de software y aplicaciones.
	Es necesario definir un calendario de pruebas para los planes de contingencia de tal forma que se mejore la eficiencia en la restauración de servicios proporcionados por la Gerencia de Desarrollo y Mantenimiento.
	Debe existir un proceso de implantación de parches, actualizaciones y nuevas configuraciones a nivel de sistema operativo, plataforma de software, plataforma de hardware y aplicaciones.
	Se debe contar con procesos de rotación de contraseñas tanto de los usuarios como de los administradores y operadores.
	Todos los usuarios deberán ser capacitados en el uso de la aplicación. De la misma forma, el personal de TI responsable de la administración y operación de la aplicación deberá recibir una capacitación adecuada de los controles de seguridad incorporados en la aplicación.
	El código fuente de la aplicación deberá atender problemas de seguridad relacionados con: * Manejo de errores. * Nombramiento de activos. * Distribución de software. * Capacidades y rendimiento. * Transferencia de archivos. * Manejo de mensaje. * Transacciones síncronas. * Transacciones asíncronas. * Seguridad en el Middleware.

Tabla No. 5 Controles para garantizar la operación

3.4 RECOMENDACIONES GENERALES:

1 Mantener actualizado el sistema operativo, el navegador y otros programas, haciendo uso de las herramientas de actualización de los distintos sistemas operativos.

2 Crear diferentes cuentas de usuario en el sistema y asignar a ciertos usuarios privilegios limitados para navegar. Con ello se evita que personas no

autorizadas permitan la entrada de software maligno, por medio de sus malos hábitos de navegación.

3 Instalar un firewall de cliente (un programa que evita que un intruso o un programa maligno entre a su PC desde Internet). El sistema operativo Windows XP incluye uno básico, sin embargo existen otros gratuitos que se consiguen en la red. Se recomiendo tener solo uno activo a la vez.

4 Mantener un programa antivirus actualizado.

3.5 RECOMENDACIONES PARA APLICACIONES WEB

Algunas de las recomendaciones de seguridad más básicas son también las más obvias. No obstante, incluso los métodos de seguridad de aplicaciones más elaborados pueden verse comprometidos si un usuario malintencionado logra obtener acceso a los equipos usando medios simples.

1. Realizar copias de seguridad con frecuencia y guardarla en un lugar seguro.

2. Mantener el servidor en un lugar físico seguro, de forma que los usuarios no autorizados no puedan tener acceso a él, apagarlo, llevárselo, etc.

3. Protejer el equipo del servidor Web y todos los demás equipos de la misma red con contraseñas rigurosas.

4. En caso de que el servidor sea bajo Windows, se deben protejer los servicios *Internet Information Service IIS.* De igual forma en caso de ser un servidor bajo Linux o Unix, la mejor defensa contra ataques consiste en simplemente cerrar los servicios que no sean estrictamente necesarios y mantener actualizado el software en las máquinas que se pueda considerar como crítico (núcleo, demonios, ficheros). También se deben utilizar protocolos seguros como Kerberos o SSH .

5. Cerrar los puertos que no se utilicen y desactivar los servicios no usados.

6. Ejecutar un programa antivirus que supervise el tráfico.

7. Establecer y hacer respetar una política que prohíba a los usuarios tener sus contraseñas escritas en una ubicación fácil de localizar. Las contraseñas del administrador preferiblemente debe estar encriptadas y éstas no deben ser sencillas ni de fácil cifrado.

8. Usar un servidor de seguridad (firewall).

9. Manténerse informado sobre las últimas revisiones de seguridad e instálarlas.

10. Usar las funciones de registro de eventos y examinar los registros con frecuencia para detectar actividades sospechosas. Esto incluye los intentos repetidos de iniciar una sesión en el sistema o la existencia de un número extremadamente alto de solicitudes en el servidor Web.

Si la aplicación pertenece a una Intranet, se debe configurar de manera segura, aplicando unas correctas políticas de seguridad, que definan claramente a que usuarios se les debe permitir acceso a la información, así como el debido control de acceso ya que de este modo, las contraseñas de inicio de sesión de los usuarios se pueden usar para obtener acceso a los recursos. Esto se usa para restringir el acceso únicamente a los usuarios que se hayan autenticado. De igual forma se deben dar de alta usuarios que ya no pertenezcan a la Intranet y actualizar el software crítico.

Como regla general, nunca se debe afirmar que la entrada proveniente de los usuarios es segura. A los atacantes les resulta fácil enviar información potencialmente peligrosa desde el cliente a la aplicación. Para protegerse contra las entradas malintencionadas, se debe seguir las siguientes instrucciones:

- En los formularios, se debe filtrar la entrada de los usuarios para comprobar si existen etiquetas HTML, que pueden contener una secuencia de comandos. La mayoría de los ataques mediante secuencias de comandos se producen cuando los usuarios pueden introducir código ejecutable (secuencias de comandos) en la aplicación. De forma predeterminada, ASP.NET proporciona validación de solicitudes, que provoca un error si un formulario recibido contiene código HTML de cualquier tipo. Es posible protegerse contra los ataques mediante secuencias de comandos de los modos siguientes:

    - Aplicar codificación HTML a las cadenas antes de aceptarlas o mostrarlas, de forma que no incluyan ningún elemento ejecutable.
    - Si la aplicación necesita aceptar algún elemento de código HTML, deshabilitar la validación de solicitudes y crear un propio filtro HTML.

- Nunca se debe mostrar la entrada de los usuarios sin filtrar. Antes de mostrar información que no sea de confianza, se deben codificar los elementos HTML para convertir cualquier secuencia de comandos potencialmente peligrosa en cadenas visibles, pero no ejecutables.

- No se debe almacenar nunca información proporcionada por el usuario sin filtrar en una base de datos.

- Si se desea aceptar algún elemento de código HTML de un usuario, se debe filtrar manualmente. En el filtro, hay que definir explícitamente lo que aceptará. No hay que crear un filtro que intente eliminar cualquier entrada malintencionada, ya que es muy difícil anticipar todas las posibilidades.

- No se debe afirmar que la información obtenida del encabezado (normalmente mediante el objeto Request) es segura. Es necesario proteger las cadenas de consulta, cookies, etc. Hay que tener en cuenta que la información que el explorador envía al servidor (información del agente de usuario) puede ser suplantada, en caso de que resulte importante para la aplicación en cuestión.

- De ser posible, no almacenar información confidencial en un lugar accesible desde el explorador, como campos ocultos o cookies. Por ejemplo, no se debe almacenar un nombre de usuario o una contraseña en una cookie.

Normalmente, las bases de datos tienen sus propios sistemas de seguridad. Un aspecto importante de una aplicación Web protegida es diseñar un modo de que ésta pueda tener acceso a la base de datos de forma segura. Para ello, se deben seguir estas instrucciones:

- Usar el sistema de seguridad inherente de la base de datos para limitar quién puede tener acceso a los recursos de dicha base. La estrategia exacta dependerá de la base de datos y de la aplicación:
- Si resulta viable en la aplicación, usar la seguridad integrada de forma que sólo los usuarios autenticados puedan tener acceso a la base de datos. La seguridad integrada es más confiable que utilizar cadenas de conexión.
- Si la aplicación debe utilizar el acceso anónimo, crear un único usuario con permisos muy limitados, y hacer que las consultas se ejecuten iniciando las sesiones como dicho usuario.
- No crear instrucciones SQL concatenando cadenas que contengan información aportada por los usuarios. En su lugar, crear una consulta parametrizada y usar la entrada del usuario para establecer los valores de los parámetros.
- Si debe almacenar un nombre de usuario y una contraseña en alguna parte para usarlos como contraseñas de inicio de sesión con la base de datos, se deben almacenar de forma segura. Si es factible, cifrarlos.

Otra forma de protegerse es crear mensajes de error seguros. Si no se es cuidadoso, un usuario malintencionado puede deducir información importante sobre la aplicación a partir de los mensajes de error que ésta muestra. Para evitarlo, se deben seguir estas instrucciones:

- No escribir mensajes de error que presenten información que pudiera resultar útil a los usuarios malintencionados, como un nombre de usuario.
- Configurar la aplicación para que no muestre errores detallados a los usuarios. Si desea mostrar mensajes de error detallados para la depuración, comprobar primero que quien los recibirá es un usuario local con respecto al servidor Web.
- Crear un sistema de administración de errores personalizado para las situaciones que sean propensas a los errores, como el acceso a las bases de datos.

En términos generales hoy en día los proveedores de servicios de Internet cuentan con las mejores prácticas de seguridad en cuanto a instalación, configuración y aseguramiento de la información, brindando con ello excelentes soluciones a los usuarios. De igual forma esto aplica tanto para sistemas operativos como para leguajes de programación.

3.6 RECOMENDACIONES DE SEGURIDAD PARA SERVIDORES BAJO SISTEMAS OPERATIVOS WINDOWS, UNIX Y LINUX

❖ Características Sistemas Operativos UNIX

Es un sistema operativo multiusuario, con capacidad de simular multiprocesamiento y procesamiento no interactivo, escrito en un lenguaje de alto nivel: C y que además dispone de un lenguaje de control programable llamado SHELL. Entre otras tantas facilidades ofrece el servicio de creación de programas y sistemas y el ambiente adecuado para las tareas de diseños de software. Emplea manejo dinámico de memoria por intercambio y además tiene capacidad de permitir interconexión de procesos. Emplea un sistema jerárquico de archivos, con facilidades de protección, cuentas y procesos, tiene también facilidad para el redireccionamiento de entradas y salidas.

Este sistema operativo cuenta con cuatro aportes importantes que han aumentado la viabilidad de los sistemas UNIX como base para los sistemas distribuidos:

- Conectores Berkely

- Los Streams de AT&T
- El sistema de archivos de red NFS
- El sistema de archivos remoto RFS de AT&T

En cuanto a los aspectos de seguridad, para poder identificar a las personas, UNIX realiza un proceso denominado ingreso (login). Cada archivo en UNIX tiene asociados un grupo de permisos. Estos permisos le indican al sistema operativo quien puede leer, escribir o ejecutar como programa determinado archivo. UNIX reconoce tres tipos diferentes de individuos: primero, el propietario del archivo; segundo, el "grupo"; por último, está el "resto" que no son ni propietarios ni pertenecen al grupo, denominados "otros".

Un computador UNIX ofrece generalmente una serie de servicios a la red, mediante programas que se ejecutan continuamente llamados *daemon* (demonio). Por supuesto, para usar estos programas hay que tener primero permiso para usar tal puerto o protocolo, y luego acceso a la máquina remota, es decir, hay que ''autentificarse'', o identificarse como un usuario autorizado de la máquina. Algunos de estos programas son telnet, rlogin, rsh, ftp, etc.

❖ Características Sistemas Operativos Microsoft Windows NT

Dicho sistema operativo soporta Sistemas Intel y los basados en RISC. Incorpora un NOS (Sistema Operativo de Red) de 32 bits y ofrece una solución de red punto a punto. Requiere un mínimo de 16MB en RAM, por lo que es más caro de instalar que la mayor parte de los NOS. También soporta multitarea simétrica y puede usar hasta 4 procesadores concurrentes. Además de ser multitarea, el Windows NT Server también es de lectura múltiple o multilectura. Soporta la administración centralizada y el control de cuenta de usuarios individuales. Las multitareas, priorizadas permiten que se ejecute simultáneamente varias aplicaciones y las operaciones de red adquieren prioridad sobre otros procesos menos críticos.

Windows como sistema operativo Incluye extensos servicios para Mac. Un computador Mac puede acceder a Windows NT Server, como si accesara al servidor Appleshare.

Windows NT Server soporta integración con otras redes (Con Software adicional), que incluyen: NetWare, VINES, Lan Manager OS/2, UNIX, VMS y redes SNA. Este sistema es tolerante a fallas Proporciona utilidades para la administración y control fácil de usar y además proporciona acceso remoto por marcación telefónica.

En cuanto a seguridad Windows NT ofrece gran firmeza por medio del acceso por cuentas y contraseñas. Es decir un usuario debe tener su cuenta asignada y una contraseña para poder tener acceso al sistema. Contiene además protecciones para directorios, archivos, y periféricos, es decir que todo esto se encuentra con una contraseña para poder ser utilizados.

Maneja además perfiles que manejan ciertos privilegios como:
CONCEPTO DE DERECHOS: Permite a un grupo de usuarios efectuar determinadas operaciones.
CUENTA ADMINISTRADOR: Controla todos los permisos y con ellas se puede: dar de alta, asignar cuentas, cancelar derechos, entre otros.

- **Características Sistema Operativo Novell Netware**

Es un sistema multitarea y multiusuario, que no requiere demasiada memoria RAM. Brinda también soporte y apoyo a la MAC, así como el apoyo para archivos de DOS y MAC en el servidor. Con él el usuario puede limitar la cantidad de espacio en el disco duro y además detectar y bloquear intrusos, soportar múltiples protocolos y acceso remoto y permitir instalación y actualización remota, a la vez que muestra estadísticas generales del uso del sistema. Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios y permite realizar auditorías de acceso a archivos, conexión y desconexión, encendido y apagado del sistema, etc. y en general soporta diferentes arquitecturas

De igual forma NetWare presenta varias desventajas, como que no cuenta con listas de control de acceso (ACLs) administradas en base a cada archivo y que algunas versiones no permiten criptografía de llave pública ni privada. Tampoco carga automáticamente algunos manejadores en las estaciones de trabajo., ni ofrece mucha seguridad en sesiones remotas. No permite el uso de múltiples procesadores, ni de servidores no dedicados. Adicional a esto para la instalación de dicho software se requiere un poco de experiencia.

- **Características sistema operativo Linux**

El sistema operativo Linux, puede considerarse como un clon del sistema operativo UNIX por tanto es Multitarea y Multiusuario, puede además correr la mayoría del software popular para UNIX, incluyendo el Sistema X-Window. Cumple también los estándares POSIX y de Sistemas Abiertos, esto es que tiene la capacidad de comunicarse con sistemas distintos a él.

Adicional a estos el sistema operativo Linux es de distribución gratuita, posee una amplia estabilidad, se puede consideras como libre de virus ya que es muy difícil que sea infectado, es mucho más seguro que otros servidores y compatible con la mayoría de los otros sistemas operativos en una red. Es mucho más veloz para realizar las tareas y posee el apoyo de miles de programadores a nivel mundial. Linux incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades de cada usuario.

Otra ventaja adicional es que se puede instalar en casi cualquier computador desde un 386 y puede manejar múltiples procesadores, incluso hasta 16 procesadores, maneja discos duros de hasta 16 TeraBytes, soporta acceso remoto, es de fácil conexión a Internet y a otras redes.

Dentro de sus principales desventajas se tiene el de que carece de soporte técnico y que no soporta todas las plataformas, y no es compatible con algunas marcas específicas.

Sistema Operativo	Conectividad	Confiabilidad	Estabilidad	Escalabilidad	Multi-usuario	Multi-plataforma
UNIX	Excelente	Muy Alta	Excelente	Muy Alta	Si	Si Múltiple
Windows NT	Muy Buena	Baja	Regular	Media	Inseguro	Parcial
Netware	Excelente	Alta	Excelente	Alta	Si	Si
Linux	Excelente	Muy Alta	Excelente	Muy Alta	Si	Si Múltiple

Tabla No. 6 Resumen características Sistemas Operativos

4. CONCLUSIONES

- La correcta selección de los controles es una tarea que requiere del apoyo de especialistas en seguridad informática y que deben formar parte fundamental de la política de seguridad de cualquier organización. Se deben seguir con especial cuidado todas las normas, estándares y reglamentaciones vigentes con el fin de optimizar los recursos de la empresa y brindar seguridad y confiabilidad a toda la organización.

- El trabajo que todos los días realizamos, el control que tenemos sobre los procesos de las empresas y hasta las comunicaciones que hacen que se mueva el mundo utilizan computadores, equipos y sistemas; es así, que se han convertido estos en algo cotidiano pero de lo cual dependemos, por eso es necesario tener todas las medidas pertinentes para evitar fallas, ataques y fraudes.

- La seguridad ha dejado de ser un problema exclusivo de las áreas informáticas, de una organización para dar lugar a estrategias que permitan enfrentar de manera coordinada y cooperativa las amenazas y vulnerabilidades que acompañan al uso de las tecnologías.

- Durante los últimos años los servidores Web se han convertido en el blanco predilecto de atacantes informáticos. La mayor parte de estos ataques tiene éxito gracias a una configuración incorrecta del servidor o a errores de diseño del mismo: si se trata de grandes empresas, los servidores Web suelen ser bastante complejos y difíciles de administrar correctamente, mientras que si la empresa es pequeña es muy posible que haya elegido un servidor Web simple en su instalación y administración pero en el cual es casi imposible garantizar una mínima seguridad.

- El presente trabajo sirve como marco de referencia a futuras aplicaciones donde se pretenda implementar políticas de seguridad y estructurar un marco de aseguramiento de la información como pilar fundamental de los activos de cualquier organización, garantizando con ello mitigar los riesgos y minimizar sus efectos.

BIBLIOGRAFIA

WEB APPLICATION SECURITY CONSORTIUM. CLASIFICACIÓN DE AMENAZAS. Disponible en Internet: < www.webappsec.org>

MDSN EN ESPAÑOL. Crear aplicaciones asp .net seguras, capítulo 6: seguridad de extranet. Productos y Tecnologías. Disponible en Internet: <http://www.microsoft.com/spanish/msdn/arquitectura/BuildSecNetApps/html/SecurityGuide_Chapter06.asp>

MONOGRAFIAS.COM. Artículo: Análisis de los requerimientos tecnológicos para la implementación de servidores web seguros. Disponible en Internet en: **<**http://www.monografias.com/trabajos12/rete/rete.shtml**>**

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOG (NIST). Guideline on Network Security Testing. Computer Security. Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg. October 2003.

MONOGRAFIAS.COM. Artículo: Hackers: Seguridad Informática. Disponible en Internet en: **<**http://www.monografias.com/trabajos/hackers/hackers.shtml**>**

MONOGRAFIAS.COM. Ataques a aplicaciones Ataques vía Web. Disponible en Internet en: <http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node279.html>

NUÑEZ, Alejandro. Estándares de seguridad en la información. Disponible en Internet en: <http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm>

VILLABON, Antonio. SEGURIDAD EN UNIX Y REDES. Versión 2.1 Julio de 2002.

MONOGRAFIAS.COM. Artículo: En el foco de los hackers: vulnerabilidades de software. Disponible en Internet en: <http://www.monografias.com/trabajos30/vulnerabilidades-software-foco-hackers/vulnerabilidades-software-foco-hackers.shtml>

DISEÑAR APLICACIONES SEGURAS. Disponible en Internet en: <http://msdn.microsoft.com/library/spa/default.asp?url=/library/SPA/vsent7/html/vxconDesigningForSecurability.asp>

ARÁMBULA, Jesús. MONOGRAFIAS.COM. Seguridad en Redes de Computadoras. Disponible en Internet en: <http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml>

MORALES, Carlos. MONOGRAFIAS.COM. Seguridad en una Intranet. Disponible en Internet en; <http://www.monografias.com/trabajos6/sein/sein.shtml>

ELORREAGA, Daniel. MONOGRAFIAS.COM. Firewalls y Seguridad en Internet. Disponible en Internet en: <http://www.monografias.com/trabajos3/firewalls/firewalls.shtml>

GUERRERO, David. Implementación práctica de políticas de seguridad: La S.G.T.I. del MEC Disponible en Internet en: <http://www.rediris.es/rediris/boletin/38/ponencia1.html>

Red Hat Linux 7.1. Oficial Red Hat Linux Referente Guide. Capitulo 7. Elementos básicos de seguridad Red Hat. El desarrollo de políticas de seguridad. Disponible en Internet en: <http://www.europe.redhat.com/documentation/rhl7.1/rhl-rg-es-7.1/s1-security-policies.php3>

AuditoriaSistemas.com. Políticas de Seguridad. Disponible en Internet en: <http://www.auditoriasistemas.com/politicas_de_seguridad.htm>

Crear aplicaciones ASP .NET seguras, Capítulo 4 - Comunicación segura. Disponible en Internet en: <http://www.microsoft.com/spanish/msdn/arquitectura/BuildSecNetApps/html/SecurityGuide_Chapter04.asp>

GLOSARIO

ANSI: Instituto Nacional Americano de Normalización

ANTIVIRUS: programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco duro o disquete.

BACKUP: copia de seguridad. Se hace para prevenir una posible pérdida de información.

CÓDIGO: es un conjunto de símbolos y reglas que sirven para representar datos de forma que puedan ser reconocidos por una máquina.

COMANDO: término que define una instrucción, mandato u orden dado al computador mediante el cual el usuario le informa de las operaciones o tareas que quiere realizar con su ayuda.

CONFIGURAR: establecer, desde un programa especial, las características de un dispositivo periférico; personalizar físicamente dichas características.

DOS: Siglas de Disk Operating System (sistema operativo de disco). Es uno de los tipos de sistema operativo más utilizado en computadores. Se emplea generalmente para el control de las unidades de disco.

FICHERO: unidad mínima de almacenamiento de información. Los archivos son un tipo de ficheros, es decir, son ficheros que pueden albergar otros ficheros. En general, archivo y fichero se consideran sinónimos, a excepción del entorno Windows, donde a los ficheros se les denomina archivos, es decir, todo documento en Windows se almacena en un archivo. Sin embargo, en este entorno se denomina Fichero a una utilidad incluida que es una sencilla base de datos de dos campos.

HACKER: experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

HARDWARE: término que indica todas las partes físicas, eléctricas y mecánicas de un computador. Significa literalmente "partes duras".

HTML: Hyper Text Markup Language. Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar páginas Web. Fue desarrollado en el CERN (Conseil Europeen pour la Recherche Nucleaire. Consejo Europeo para la Investigación Nuclear).

HTTPS: URL creada por Netscape Communications Corporation para designar documentos que llegan desde un servidor WWW seguro. Esta seguridad es dada por el protocolo SSL (Secure Sockets Layer) basado en la tecnología de encriptación y autentificación desarrollada por la RSA Data Security Inc.

INTRANET: redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW.

IP: Protocolo Internet. Es un protocolo de bajo nivel para redes que describe la manera cómo el usuario puede comunicarse con los miembros Internet.

ISO: Organización Internacional para la Normalización

LAN: red de área local, una red de propiedad privada que ofrece canales de comunicaciones de alta velocidad para conectar equipos de procesamiento de información en áreas geográficas limitadas.

PROCESADOR: parte central de un sistema computador que proporciona y controla las funciones aritméticas, lógicas y de transferencias requeridas para comparar, mover, calcular y, de cualquier manera, manipular y procesar datos.

RAM: Random Access Memory. Memoria de Acceso Aleatorio. Se le llama así porque es posible dirigirse directamente a la célula donde se encuentra almacenada la información. Su principal característica es que la información se almacena en ellas provisoriamente, pudiendo ser grabadas una y otra vez, al igual que un casette de sonido. La memoria RAM se puede comparar a un escritorio, donde se coloca los papeles con que se va a trabajar. Mientras más grande el escritorio más papeles soporta simultáneamente para ser procesados.

SHELL: procedimiento mediante el cual se puede acceder temporalmente al sistema operativo desde el interior de un programa.
En Windows es una ventana de aplicación especial que permite lanzar otras aplicaciones.

SERVIDOR DE RED O HOST: servidor de archivos que proporciona las funciones esenciales para ofrecer servicios a los usuarios de la red y para ofrecer funciones de gestión a los administradores de la misma.

SSL: Secure Sockets Layer. Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

TCP/IP: Transmission Control Protocol / Internet Protocol. El término describe dos mecanismos de software empleados para posibilitar la múltiple comunicación entre computadores de manera libre de error. TCP/IP es el lenguaje común de la Internet, el que permite que diferentes tipos de computadores utilicen la red y comuniquen unas con otras, indiferentemente de la plataforma o sistema operativo que usen.

TELNET: Protocolo y aplicaciones que permiten conexión como terminal remota a un computador anfitrion, en una localización remota

URL: Universal Resource Locator. Nombre genérico de la dirección en Internet, Indica al usuario dónde localizar un archivo HTML determinado, en la Web.

WEB SITE: Sitio en el World Wide Web. Conjunto de páginas Web que forman una unidad de presentación, como una revista o libro. Un sitio está formado por una colección de páginas Web
WWW (World Wide Web)