Auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP ISO/IEC 17799:2007 y la metodología OSSTMM v2.

Edgar A. Maya, Daniel D. Jaramillo

***Abstracto*— El presente proyecto expone el proceso de la realización de una auditoria de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP ISO/IEC 17799:2007 y OSSTMM v2 con el objetivo de detectar las vulnerabilidades y posibles deficiencias que pueda tener la red y de esta manera determinar con efectividad las medidas necesarias a tomar.**

Se presenta una serie de recomendaciones estableciendo acciones a emprender, que contribuyan a mejorar el nivel de seguridad de la información, incluyendo políticas de seguridad, para reducir al mínimo los riesgos que pudieran darse en el futuro, para evitar ataques y mejorar la eficiencia de la red.

I. INTRODUCCIÓN

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar las operaciones, reduciendo significativamente el uso del papel, a su vez reduciendo los costos al compartir información. Sin embargo, el éxito de muchos de estos esfuerzos depende, en gran parte, de la capacidad de la organización para proteger la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos.

Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la seguridad de la información debe convertirse en una de las principales preocupaciones de una empresa.

Documento recibido el 14 de julio de 2014. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.

E. A. Maya, trabaja en la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (teléfono: 5936-2955-413; e-mail: eamaya@utn.edu.ec).

D. D. Jaramillo, egresado de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono: 5936-2635160; e-mail: ddjaramillo@utn.edu.ec).

II. SEGURIDAD INFORMÁTICA

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad está garantizada.

En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto necesita ser protegido adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio han vuelto más comunes, y cada vez son más sofisticadas.

A. Auditoria

Con la explotación en el uso del Internet en los últimos 10 años, tanto las empresas grandes como las pequeñas, se han visto obligadas en asegurar su componente vital que es la tecnología de la información. Actualmente las empresas, cuenta con el valioso recursos de TI, tales como computadoras, redes de datos, sistemas informáticos, etc. Para la protección de los activos de una empresa, se sugiere que haya tenido al menos una auditoría de seguridad, con el fin de obtener una imagen clara de los riesgos de seguridad que enfrentan y saber la mejor manera de tratar con esas amenazas.

El propósito de una auditoría de seguridad no es para culpar o desmerecer el diseño de una red, sino para garantizar la eficacia, integridad y el cumplimiento de las políticas de seguridad de la empresa. La auditoría ofrece la habilidad de probar los sistemas, encontrar riesgo y comprobar si los controles son los apropiados para mitigar la exposición a los diferentes riesgo, cabe recalcar que la auditoría de seguridad no sólo trata de cómo ejecutar un sin número de herramientas

de hackers, en un intento de entrar en la red.

Características de la auditoría de seguridad informática

La auditoría es sistemática esto quiere decir que los resultados obtenidos son debidos a un análisis meticuloso, metódico y planificado por parte del auditor, que garantiza un grado de fiabilidad.
La auditoría es totalmente independiente ya que es imposible para una empresa autoevaluarse en forma objetiva.
Evalúa si las acciones preventivas tendentes al control de los riesgos de ataques o falencias detectados en la empresa, son eficaces o no, en función de los resultados obtenidos.
La auditoría se encarga de analizar el estado actual de la empresa para dar soluciones a futuro, sin la necesidad de encontrar un culpable de las posibles falencias de la tecnología de la información.
Las características se las puede resumir gráficamente en este esquema.

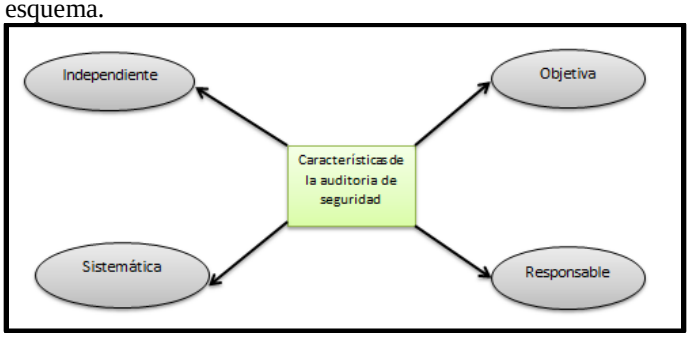

Fig. 1. Características de la auditoria de seguridad informática

B. NTP ISO/IEC 17799

Si ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Estructura y campo de aplicación

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo. Las clausulas son las siguientes:

- Política de seguridad;
- Organizando la seguridad de información;
- Gestión de activos;
- Seguridad en recursos humanos;
- Seguridad física y ambiental;
- Gestión de comunicaciones y operaciones;
- Control de acceso;
- Adquisición, desarrollo y mantenimiento de sistemas de información;
- Gestión de incidentes de los sistemas de información;
- Gestión de la continuidad del negocio;
- Cumplimiento;

Dentro de cada clausula, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. Para este proyecto se considera previamente cuantos son realmente los aplicables según las necesidades.

C. Metodología OSSTMM

El OSSTMM fue creado por Peter Herzog de la organización ISECOM en Diciembre del año 2000, este manual el único y el más extenso estándar certificado disponible para el desarrollo de pruebas de Seguridad en Sistemas de Internet y Redes. Con el fin de que el manual este siempre actualizado, la organización se asegura de estar al tanto de los cambios que ocurren y de los nuevos progresos en materia de seguridad Informática.

El OSSTMM funciona como una guía completa, con respecto a los aspectos principales de la seguridad de la información de una empresa, de esta manera permite que el personal autorizado en realizar auditorías, puedan consultar información relevante sobre sus propias políticas de seguridad, esto muestra la gran flexibilidad del manual.

Estructura

Las pruebas de seguridad abarcan seis secciones que corresponden a las seis secciones que contiene este manual. Cada sección consta de varios módulos y cada módulo indica una serie de tareas o pruebas a realizar; las cuales cubren las siguientes áreas.

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

El esquema de este manual es como muestra la figura 2.

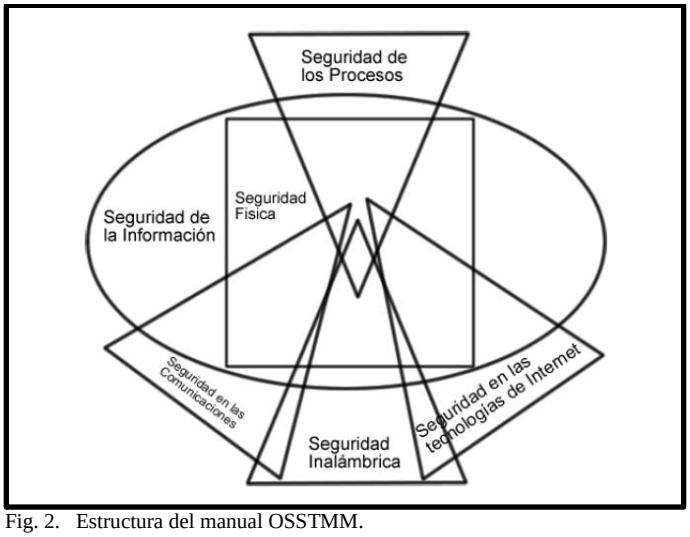

Fig. 2. Estructura del manual OSSTMM.

El OSSTMM cuida de las condiciones límites tales como los procesos de prueba, ética, análisis de los resultados de las pruebas y la seguridad IT con respecto a la ley, regulaciones y estándares.

III. Análisis de la situación actual

En este capítulo se describe la infraestructura actual de la red de datos del Gobierno Municipal de Santa Ana de Cotacachi hasta octubre del 2013, los datos obtenidos son el resultado de la información recolectada con la colaboración del departamento de informática y el reconocimiento de las instalaciones físicas de la red.

A. Descripción general

La estructura organizacional del Gobierno Municipal de Santa Ana de Cotacachi es el vehículo, que vincula la misión y los objetivos institucionales con la prestación de servicios a la comunidad cotacacheña, y se basa en un enfoque de procesos, productos y servicios para garantizar el ordenamiento orgánico y la continuidad de los servicios públicos municipales.

B. Especificaciones Técnicas

El GAD Municipal de Santa Ana de Cotacachi es una institución pública sin fines de lucro se encuentra en la Provincia de Imbabura en la ciudad del mismo nombre, ubicado en las calles Gonzales Suarez y García Moreno
En este punto se describe la ubicación física, la estructura de la red de datos tanto interna como externa, los recursos informáticos, y los enlaces de red hacia las instituciones relacionadas con el municipio.

C. Administración del sistema de red

En este ítem se analiza la gestión del software, del hardware de los equipos del GAD municipal así como también la gestión del antivirus y la administración del departamento de informática.

D. Responsabilidad de los funcionarios del departamento de informática

El Departamento de Informática está conformada por el Jefe de informática, jefe de conectividad, y dos analistas de informática; las responsabilidades asignadas a cada funcionario, están de la siguiente manera: los analistas informáticos realizan el mantenimiento de software, mantenimiento de hardware, soporte al usuario, administración de cuentas de usuarios, inventarios, etc. Los jefes de informática por lo general se encargan de la parte administrativa, desarrollo de aplicaciones, etc.

IV. Pruebas de vulnerabilidad

En este capítulo se describe las vulnerabilidades encontradas en la red de datos del Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi, para lo cual se ha utilizado el software Backtrack, y se ha tomado como base los preceptos de la metodología OSSTMM.

A. Seguridad de la información

La seguridad de la información describe la inteligencia competitiva del GAD Municipal de Santa Ana de Cotacachi, misma que detalla la infraestructura que se posee en el área de informática y la información intelectual de cada uno de las personas que son parte del soporte en el departamento de informática.

B. Seguridad de procesos

Consiste en la realizar una serie de testeos para obtener privilegios de acceso a la organización y a sus activos desde una posición fraudulenta, haciendo uso de teléfono, chat, boletines, entrevistas, mail, etc.

C. Seguridad en las tecnologías de internet

Se realiza un análisis de la seguridad de las tecnologías de la información como es el sondeo de red, la identificación de los servicios de los sistemas, aplicaciones de internet, enrutamiento, cifrado de contraseñas, testeo de denegación de servicios, y la evaluación de políticas de seguridad.

D. Seguridad en las comunicaciones

El testeo de la seguridad en las comunicaciones consiste en chequear el funcionamiento de la central telefónica, el modem y el FAX, con el objetivo de encontrar alguna anomalía.

E. Seguridad inalámbrica

Consiste en verificar la seguridad de las redes inalámbricas como por ejemplo las redes WIFI, bluetooth, RFID, infrarrojos etc.

F. Seguridad física

Consiste en evaluar la seguridad física del GAD Municipal de Santa Ana de Cotacachi y sus bienes informáticos, verificando las medidas de seguridad de su perímetro físico, y

evaluar las condiciones de la región respecto a los desastres naturales.

V. Medidas específicas de corrección

Este capítulo trata de una serie de recomendaciones estableciendo acciones a emprender, de cómo mejorar la seguridad de la información, incluyendo políticas de seguridad, para reducir al mínimo los riesgos que pudieran darse en el futuro, basado en la norma NTP-ISO/IEC 17799:2007.

A. Políticas de seguridad

Una vez revisado el diagnóstico del cual fue objeto el capítulo 4, se observó que la seguridad de la información es escaza, vulnerable a fallas, y considerando que el objetivo principal del departamento de Informática del GAD Municipal de Santa Ana de Cotacachi es tener continuidad en el servicio que día a día presta a la Ciudadanía del cantón se ha elaborado una serie de recomendaciones que permitan mejorar la calidad en el servicio que se presta en el GAD Municipal de santa Ana de Cotacachi.

B. Aspectos organizativos para la seguridad

Considerando que en el GAD Municipal de Santa Ana de Cotacachi, al momento no se cuenta con proceso para el manejo de la información se sugiere al departamento de Información elaborar una panificación que permita a los usuarios conocer la importancia de seguir procesos y procedimientos al momento de procesar la información para que esta sea confiable, para lo cual se ha establecido un cronograma en el cual se podría difundir las políticas anteriormente mencionadas , que sean de importancia para los empleados.

TABLA I
CRONOGRAMA DE DIFUSIÓN DE POLÍTICAS DE SEGURIDAD

CRONOGRAMA DE DIFUSION DE POLITICAS DE SEGURIDA		
Fecha	***Departamento***	***Horas***
4-08-14	Alcaldía y Concejales	15:00
5-08-14	Coordinación General	15:00
6-08-14	Secretaria General	15:00
7-08-14	Dir. Gestión financiera	15:00
8-08-14	Dir. Gestión Administrativa	15:00
11-08-14	Dir. Planificación para el Desarrollo Local	15:00
12-08-14	Dir. Obras y Servicios Públicos	15:00
13-08-14	Dir. Gestión Social e Interculturalidad y Derechos Humanos	15:00

C. Gestión de activos

Para tener un control de los activos que se manejan en la red del GAD Municipal de Santa Ana de Cotacachi, el departamento de Informática en conjunto con inventario y bodega, etiquete, cada uno de los equipos entregados, así también se registrara información como el nombre del responsable del activo, ubicación, descripción física, a más del número de serie otorgada.

La información recogida se almacenara de manera física, y digital, para lo cual el departamento de informática deberá diseñar un programa que permita el ingreso y almacenamiento de la información, para que esta pueda ser procesada de manera fácil y rápida por el personal encargado de llevar el registro.

D. Seguridad en recursos humanos

El personal que labora en el departamento técnico, lo ha venido haciendo desde hace varios años, cada uno cuenta con la experiencia necesaria, para el cargo que desempeña, el trabajo lo realizan a tiempo completo, y únicamente tienen firmado el contrato por prestación de servicios.

Se recomiendo, incluir en el contrato de trabajo, un acuerdo de confidencialidad, mismo que asegure que los empleados, no revelaran información concerniente a la institución, además de recordar que de violar este acuerdo pudieren ser sometidos a las leyes que se encuentren vigentes.

E. Seguridad física y ambiental

Concerniente a la seguridad física, los equipos que utilizados los usuario de la red del GAD Municipal de Santa Ana de Cotacachi, no se encuentran visibles para el público, cada uno de estos están protegido por un escritorio, la mayoría se encuentran dentro de oficinas, misma que para el ingreso es necesario tener la llave la cual permite el acceso.

Los servidores, que permiten la ejecución de los diferentes servicios informáticos que se maneja en el GAD Municipal de Santa Ana de Cotacachi, se encuentran en un cuarto que cuenta con una puerta que la única seguridad que este ofrece es la de la chapa.

Se recomienda que en la puerta de ingreso se implemente seguridad de acceso, a través sistemas biométricos, código de acceso, entre otros, además de cambiar la puerta, por otra que brinde seguridad pudiendo ser una puerta de acero diseñada para cuartos de quipos, puesto que en la que en la actualidad la puerta es de vidrio y aluminio.

F. Gestión de comunicaciones y operaciones

Administración y Gestión de Red de GAD Municipal de Santa Ana de Cotacachi

En la actualidad los sistemas informáticos que se manejan en el GAD Santa Ana de Cotacachi, se pueden evaluar como buenos, pero el rendimiento de la red, tiende a presentar inconvenientes porque los equipos de red como ruteadores y switch no tiene una administración y configuración ideal de red, actualmente la red del GAD Municipal de Santa Ana de Cotacachi se encuentra configurada como se muestra en la Figura 3.

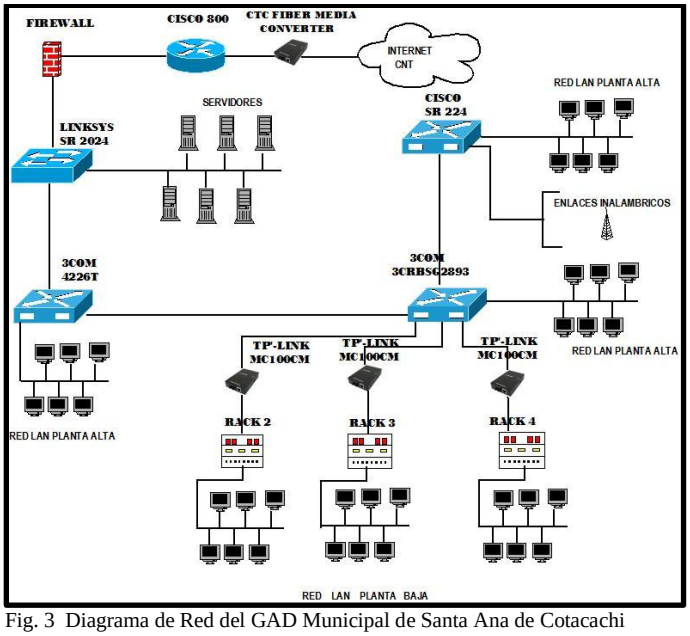

Fig. 3 Diagrama de Red del GAD Municipal de Santa Ana de Cotacachi

Se sugiere un reorganización en los equipos de red para así tener una mejor administración de los equipos, y que el performance de la red se vea reflejado en la excelencia del servicio prestado a los ciudadanos del cantón Cotacachi, evitando que los sistemas de recaudación, cobranzas entre otros estén fuera de línea, para ellos se ha rediseñado la red, con la implementación de VLANs y la realización de subredes, tomando en cuenta los niveles jerárquicos que deben tener los equipos de red.

Se ha tomado la red de clase C 192.168.0.0/24 de la cual se pueden obtener 254 ordenadores con el fin de optimizar el número de redes y host utilizables, considerando que es una red relativamente pequeña.

La segmentación de la red se realiza haciendo uso de la herramienta VLSM con el objetivo de no desperdiciar direcciones de red, obteniendo subredes que permitirán al administrador de la red brindar contención de broadcast y seguridad de bajo nivel en la LAN. Para realizar esta segmentación se ha tomado en cuenta el número de host por cada rack y el número de servidores.

Se diseña siete VLANs, con el objetivo de reducir el dominio de colisión, las peticiones constantes de mensajes de ARP, que pueden saturar una red, con un significativo número de host, para ello se crea dominios de difusión más pequeños. A cada una de las VLANs se le ha asignado diferente dependencias de acuerdo a su función, información que maneja y lugar donde se encuentran.

Una vez diseñado la segmentación de las subredes y las vlans por cada dependencia se realiza la distribución correcta de los dispositivos de red, como switchs y router, para mantener la red operativa y funcionando correctamente, en la Figura 4, se puede visualizar la configuración idónea para la red del GAD Municipal de Santa Ana de Cotacachi.

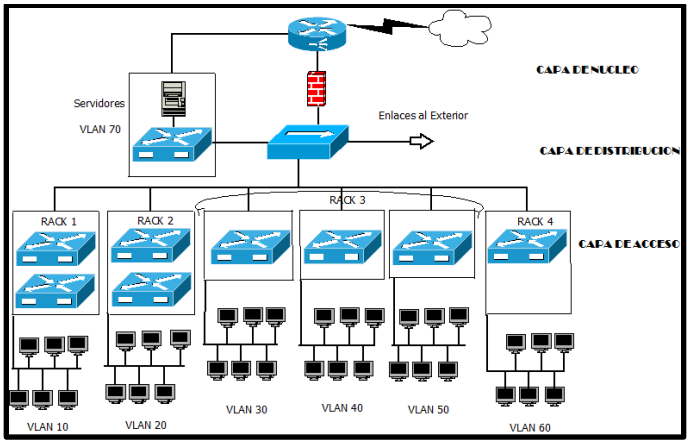

Fig. 4. Diagrama de Reorganización de GAD Municipal de Santa Ana de Cotacachi

Como se puede observar en la figura del rediseño de la red, los dispositivos de red como router y switch están distribuidos jerárquicamente, esto permite tener una red fácilmente entendible y a definir funciones en cada capa, además permita una fácil configuración en el caso de que sea necesario.

Gestión De Seguridad De Redes Inalámbricas

Del Acces Point con SSID Santa Ana de Cotacachi se recomienda usar una contraseña segura, misma que debe tener ocho caracteres como mínimo y estar compuesta por letras minúsculas y mayúsculas, números y símbolos como ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /; La contraseña se la debe cambiar con regularidad, de esta manera se evitara obtenerla fácilmente en caso de que sea víctima de un ataque.

Del Acces Point con SSID Sistemas se recomienda configurar una clave de seguridad que tengan características parecidas a las mencionadas previamente ya que al momento no cuenta con contraseña. Los usuarios que deseen conectarse a esta red deberán solicitar su contraseña en el Departamento de Informática.

Del Acces Point con SSID Wifi_Parque_MC se recomienda asignarle a un puerto del Rack 3, a este puerto se le debe asignar una nueva VLAN 80, para mantener a los usuarios que se conectan desde el parque aislados de la red municipal y de esta manera evitar cualquier intrusión a través de esta red inalámbrica a la red interna del Municipio

Protección Contra Amenazas

Sitio Web cotacachi.gob.ec

En el análisis de la página web cotacachi.gob.ec detalla la vulnerabilidad llamada falsificación de petición en sitios cruzados, después de realizar un ataque a este sitio a través de esta vulnerabilidad se comprueba que es un falso positivo como indica el mismo resultado del escaneo del sitio Web.

Sitio Web cotacachienlinea.gob.ec

Según el resultado del escáner de vulnerabilidades para este sitio web, visto en la sección 3.4.1.1 del trabajo de grado, la página tiene la vulnerabilidad que se la conoce como adivinación de contraseña en inicio de sesión, para ello se recomienda implementar el siguiente tipo de seguridad.

El sitio Web se encuentra diseñado en la plataforma joongla, para parchar esta vulnerabilidad se recomienda seguir los siguientes pasos:

- Ingresar a la página Web como administrador
- Ir a Extensiones – Gestor de plug-ins.
- Buscar el plug-in: System - Brute Force Stop
- Activar el plug-in
- Aparece la ventana donde permite cambiar el número de intentos para iniciar sesión, tiempo de bloqueo de la ip, y la opción de enviar un correo electrónico en caso de que sea bloqueada la página web.
- Guardar cambios y cerrar

Se recomienda colocar un número de intentos menor a 5 y que el tiempo de bloqueo sea al menos de una hora, de esta manera se puede decir que la página web se considerará segura.

G. Control de accesos

Para brindar la seguridad necesaria a la información que circula dentro de la red del GAD Municipal de Santa Ana de Cotacachi se deberá tener un registro de quienes utilizan los sistemas informáticos, que privilegios tienen, y en caso de que el cargo que desempeñado en la municipalidad se culmine, eliminar de los usuarios privilegiados, para evitar posibles accesos indebidos a la red.

Conociendo la información que circula por la red del GAD Municipal de Santa Ana de Cotacachi, es de carácter confidencial, se recomienda que todos quienes tengan acceso a los sistemas de información, firmen un compromiso, mismo que les obliga a no revelar las contraseñas personales, a terceros, así también las contraseñas grupales, más aun a los profesionales que trabajen en el departamento de Informática que estará en la facultad de acceder todos los sistemas y conocerá la contraseña de todos los usuario.

H. Adquisición desarrollo y mantenimiento de sistemas

Se debe considerar para la adquisición de software la garantía ofrecida por el fabricante, así también que cumpla con normas y recomendación que garanticen la seguridad en la información.

Con anterioridad a la adquisición se recomienda realizar un estudio de los beneficios y desventajas que cada uno presta, para así poder acoplarlo a los sistemas que se encuentran operativos.

Es necesario que el software desarrollado con recursos del GAD Municipal de Santa Ana de Cotacachi, sea sometido a pruebas, que permitan comprobar la seguridad del mismo, para lo cual el departamento de Informática será el responsable de comprobar que cumpla con las normas con las reglas de seguridad internacionales, puesto que la información que se maneja en la red de la municipalidad también está en la Internet.

I. Gestión de incidentes de la información

Es necesario llevar un registro de cada uno de los eventos suscitados dentro de la municipalidad, esto será útil para detectar las vulnerabilidades existentes en la red, y prevenir posibles ataques a la seguridad de la misma, para llevar un correcto registro se ha recomendado la utilización de la platilla que se indica en la Tabla 2.

TABLA II
PLANTILLA PARA REGISTRO DE EVENTOS

Plantilla para registro de Eventos	
Numero de Evento	
Equipo o Sistema Afectado	
Departamento	
Oficina	
Número de Serie del equipo	
Hora	
Fecha	
Personal que reporta el daño	
Observaciones	
Firma del responsable	

VI. CONCLUSIONES

La elaboración de este proyecto ha supuesto un gran esfuerzo de trabajo y tiempo, ya que se ha tenido que investigar temas como, gestión de seguridad y auditoria de seguridad, así como diferentes estándares de seguridad informática, con lo cual se pudo analizar que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se puede estar preparado y dispuesto a reaccionar con rapidez a las amenazas y las vulnerabilidades que pueden presentarse en el campo de la informática.

Se pudo constatar que los activos informáticos que posee el GAD municipal manejan información que es de mucha importancia para los ciudadanos del cantón, esto es debido a que cada vez más, los servicios principales que presta esta dependencia dependen de los sistemas informáticos, es por eso la necesidad de una auditoria de seguridad al sistema de red, además el manejo eficiente de las TICs es uno de los principales objetivos estratégicos de la municipalidad.

El buen ejercicio de una empresa obedece a la eficiencia de sus sistemas informáticos; una empresa puede tener gente de primera, pero si posee un sistema informático propenso a fallos, vulnerable e inestable y si no hay un equilibrio entre estas dos cosas, la empresa nunca podrá brindar un servicio de calidad. En cuanto al trabajo de la auditoría en sí, se puede remarcar que se precisa de conocimiento de seguridad informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de seguridad informática debe hacerse por gente altamente responsable, ya que una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada.

VII. RECOMENDACIONES

Es menester poner en marcha las recomendaciones redactadas en el capítulo cuatro de este proyecto de tesis con

el fin de mejorar el nivel de seguridad de la información y optimizar los recursos de las tecnologías de la información.

Se recomienda que el personal del departamento de informática tenga capacitación en aspectos de seguridad y control de tecnología para que en base a los conocimientos obtenidos expongan nuevas estrategias adecuadas para mantener segura las tecnologías de la información, que a diario se maneja en la municipalidad.

Se recomienda que el departamento de informática con apoyo del GAD municipal de Santa Ana de Cotacachi adopte como una buena práctica la planificación y realización de auditorías periódicas tomando en cuenta que los estándares van evolucionando y cambiando para asegurar que los objetivos relacionados a la seguridad de la información se estén cumpliendo.

VIII. Referencias

[1] Aldaz, K. (Julio, 2011). Normas de Auditoria. Alcance de la auditoría informática. Recuperado de: http://normasauditoria.blogspot.com/2011/07/alcance-de-la-auditoria-informatica.html

[2] Antonio Villalón Huerta *El sistema de gestión de seguridad de la información* Recuperado de: http://www.shutdown.es/ISO17799.pdf

[3] Apaza, G. (Junio, 2011). Seguridad en Servicios TCP/IP. Recuperado de: http://www.sistemas.edu.bo/mreynolds/Redes2/SEGURIDAD%20TCP - IP_2.pptx

[4] Benavidez, E. (Junio, 2011). Seguridad Informatica: Que es la seguridad Informatica Recuperado de: http://seguridadinformaticaais.wordpress.com

[5] Bisogno, M (Octubre, 2004). Metodología para el Aseguramiento de Entornos Informatizados" Proyecto de titulacion: Universidad de Buenos Aires

[6] Cerra, M. (2010). *200 respuestas de seguridad*. Argentina: USERSHOP

[7] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de: Datos, (2007). Perú. *Norma Técnica Peruana NTP-ISO/IEC 17799. Reseña Histórica*. (p. iv).Lima (2a ed.).

[8] Daniel. Sf. Vulnerabilidades en las redes TCP/IP. Recuperado de: http://dnl-skm.blogspot.com/2011/07/vulnerabilidad-tcpip.html

[9] Del Peso, E. Ramos. M. (2010). *El documento de seguridad: Análisis técnico y jurídico*. Madrid: Díaz de Santos como se realiza la auditoria

[10] Dias, G. (2010). *Redes de Computadoras*. Recuperado de: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/08_capaTransporteUDP.pdf

[11] Economia, sf. Economia Aida. Estandares auditoría informática. Recuperado de: https://sites.google.com/site/economiaaida/estandares-auditoria- informatica

[12] Eleclibre. (Enero, 2011). Sistemas y mecanismos de proteccion. Recuperado de: http://eleclibre.blogspot.com/

[13] Flores, B. (Noviembre, 2010). Riesgos de Auditoria. Cuando se debe aplicar una auditoria informatica. Recuperado de: http://dfloresysbonilla.blogspot.com/

[14] Galisteo, D. Moya, R. sf. Seguridad en TIC. Man in the middle Ataque y deteccion. Recuperado de: http://issuu.com/arrayl/docs/mitm

[15] García, J. (2008). *Ataques contra redes TCP/IP*. Recuperado de: http://www.intercambiosvirtuales.org/tag/ataques-contra-les-redes-tcpip

[16] Gonzáles, H. (2013). UTTN-TICS. Unidad III Auditoria. Recuperado de: http://uttn-tics.wikispaces.com/Unidad+III.+Auditoria

[17] Jauregui, I. (2009). *SNIFFING DE REDES*. Recuperado de: http://toma37.blogspot.es/1241710200/

[18] Jiménez, E. (sf). Riesgos potenciales en los servicios de red. Recuperado de: http://esperanza7989.files.wordpress.com/2011/11/6-riesgos-potenciales-en-los-servicios-de-red.pdf

[19] Kioskea (Diciembre, 2012). Ataques por desbordamiento de buffer. Recuperado de: http://es.kioskea.net/contents/19-ataques-por-desbordamiento-de- bufer

[20] Martínez, J. E. Giraldo, C. A. (2009). *Auditoría de seguridad Informática*. Recuperado de: http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf

[21] Tony, (febrero, 2011). Gestión de servicios de tecnologías de la información. Recuperado de: http://mymusicismydrug.blogspot.com/2011/02/unidad-1gestion-de-servicios-de.html

[22] Victoria, M. (2011). *Metodología para el Aseguramiento de Entornos Informatizados*. Recuperado de: http://es.scribd.com/doc/36819948/32/Vulnerabilidades-a-nivel-fisico

IX. BIOGRAFÍAS

Edgar A. Maya A. Nació en Ibarra provincia de Imbabura el 22 de abril de 1980. Ingeniero en Sistemas Computacionales, Universidad Técnica del Norte-Ecuador en 2006. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra- Ecuador, y cursa la Maestría en Redes de Comunicación (3do Semestre), Pontificia Universidad Católica del Ecuador, Quito- Ecuador.

Daniel D. Jaramillo R. Nació en Otavalo – Ecuador. Hijo de Rosa Remache y Alfonso Jaramillo. En el año de 1992, realizó sus estudios primarios en la Escuela Libertador Simón Bolívar. En el año de 1998 ingresó al Instituto Técnico Superior Otavalo ITSO, en donde finalizó su educación media. En el año de 2004 obtuvo su título de Bachiller Técnico en "Electrónica" y en el año 2005 ingresó como estudiante a la Universidad Técnica del Nortel. Tiene aprobado los cursos de Matlab, Simuladores de circuitos, Domótica. Actualmente es egresado de la carrera de ingeniería en electrónica y redes de comunicación de la universidad Técnica del Norte.