Sistema de Gestión de Seguridad de la Información (SGSI) en el Comando Provincial de Policía “Imbabura No. 12”

Jaime R. Michilena, Paola A. Díaz

***Resumen*— El presente proyecto aborda la problemática que se plantea al momento de implantar y gestionar un SGSI, tal como se define en la norma ISO/IEC 27000, para una Organización. Además, contempla los controles que deben ser implantados y las herramientas de gestión desarrolladas sobre software libre.**

Un Sistema de Gestión de la Seguridad de la Información (SGSI), es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan comparar de manera consciente y objetiva escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos que se invierten dentro de una organización.

***Términos para Indexación*— SGSI, TI, MAGERIT.**

I. INTRODUCCIÓN

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la norma ISO 27001.

Documento recibido el 6 de Febrero de 2013. Esta investigación serealizó como proyecto previo para obtener el título profesional en la carrerade Ingeniería Electrónica y Redes de Comunicación de la Facultad deIngeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica delNorte.

J.R. Michilena, trabaja en la Universidad Técnica del Norte, en la Carrera deIngeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sectorEl Olivo, Ibarra-Ecuador (teléfono: 0990746792; e-mail:jrmichilena@utn.edu.ec).

P.A. Díaz egresada de la Carrera de Ingeniería Electrónica y Redesde Comunicación (teléfono: 0989179176; e-mail:pao_lucho@hotmail.com).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.Este proceso es el que constituye un SGSI, que puede ser considerado, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es prácticamente imposible. El propósito de un sistema de gestión de la seguridad de la información esgarantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

II. CONCEPTOS BÁSICOS

A. Norma ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC, que proporcionan un marco de gestión de seguridad de la información, utilizable por cualquier tipo de organización pública o privada, grande o pequeña.

La norma ISO 27000 comprende un amplio rango de numeración para los estándares, que va desde 27000 a 27019 y de 27030 a 27044.

Contiene términos y definiciones relacionados con la gestión y seguridad de la información que se emplean en toda la serie. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

Los términos más utilizados dentro de la norma ISO 27000 y que se mencionan en los estándares posteriormente descritos, están definidos con la finalidad de no obtener varios conceptos para un mismo término.

- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Confidencialidad:** La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.
- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.
- **Seguridad de información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad. [2]

B. Estándar Internacional ISO/IEC 27001

Este estándar fue publicado el 15 de Octubre de 2005 por la ISO e IEC que conforman un sistema especializado para la estandarización universal. Es la norma principal de la serie ISO 27000 y contiene los requisitos de implementación del sistema de gestión de seguridad de la información.

El estándar ha sido preparado para proporcionar un modelo que permite establecer, implementar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. [4]

Este estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase Actuar lleva de nuevo a la fase de Planificar para iniciar un nuevo ciclo de las cuatro fases.

La Fig. 1. muestra cómo se desarrolla el proceso de implantación de un SGSI.

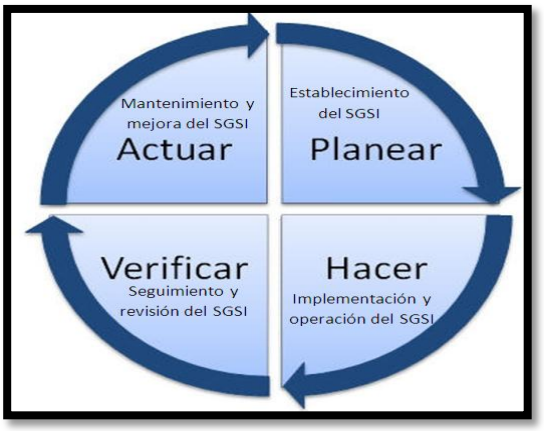

Fig. 1. Modelo de desarrollo PDCA

- **Planificar (Plan):** Dentro de esta fase se establecen políticas, objetivos, procesos y procedimientos relevantes para manejar el riesgo y mejorar la seguridad de la información. Se debe definir una política de seguridad que considere los requerimientos legales relativos a la seguridad de la información; además debe establecerse los criterios con los que se va a evaluar el riesgo y finalmente debe ser aprobada por la dirección o gerencia.
  Aquí se define una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos de la institución, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.
- **Hacer (Do):** En esta fase se seleccionan e implementan los controles que reduzcan el riesgo a los niveles considerados como aceptables.
  Se debe efectuar el cambio y/o las pruebas proyectadas según la decisión que se haya tomado y la planificación que se ha realizado.
- **Verificar (Check):** Una vez realizada la acción e implantado el control, se debe verificar, evaluar y medir el desempeño del proceso en comparación con la política, objetivos, experiencias prácticas y reportar los resultados a la gerencia para su revisión.

- **Actuar (Act):** Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.
  Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar la forma de proceder, además es importante tener la seguridad de que las mejoras introducidas alcanzan los objetivos previstos.

Definición de SGSI

Un SGSI es un Sistema de Gestión de la Seguridad de la Información, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración. Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. [1]

C. Estándar Internacional ISO/IEC 27002

Es una guía de buenas prácticas que fue publicada el 1 de Julio de 2007 basándose en la norma ISO 17799:2005 por lo que mantiene a 2005 como año de edición y describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es una norma certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Los objetivos de control y los controles, deben ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos, de esta manera se logra una práctica eficaz de gestión de la seguridad.

D. Metodología MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT, cumple con el objetivo primordial de garantizar la seguridad los sistemas de información, identificando problemas y definiendo políticas que los eviten. [3]

MAGERIT define los procedimientos que sirven de guía para el establecimiento de la protección necesaria de los sistemas de información de una institución de carácter público. Además, cumple con objetivos adicionales que están enfocados a la realización de un análisis de riesgos dentro de la institución.

Estos objetivos son:

- Analizar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados, mediante la gestión de riesgos. Basado en los resultados del análisis de riesgos, se seleccionan e implantan las medidas o salvaguardas de seguridad adecuadas para reducir al mínimo aceptable los posibles perjuicios.

Administración de riesgos

Es importante asegurar que la institución alcance los objetivos relacionados con la seguridad de la información, para lo cual ésta debe dirigir y administrar las actividades de TI con el fin de lograr un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, los Directivos necesitan identificar las actividades más importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando la manera en la que se desarrollan los procesos de TI. [5]

La Fig. 2. muestra un esquema de administración de riesgos que sirve como base para analizar y gestionar los riesgos de TI.

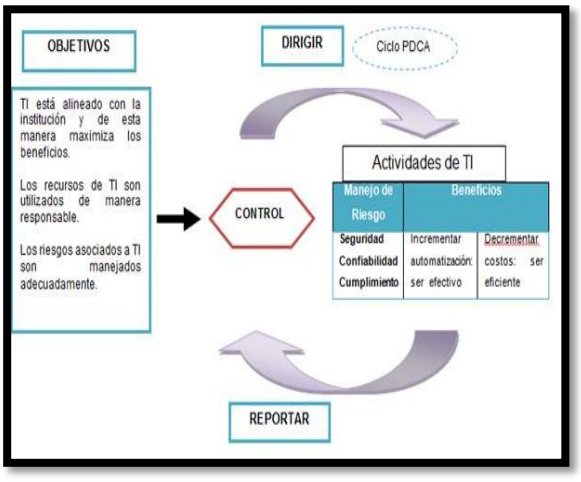

Fig. 2. Esquema base para administración de riesgos

Análisis de riesgos

El análisis de riesgos permite determinar qué tiene la institución y estimar el nivel de exposición a los riesgos presentes.

Este análisis se compone de tres elementos fundamentales:Activos, Amenazas, Salvaguardas.

El primer paso consiste en la valoración de los activos, que son los elementos del sistema de información que aportan valor a la Institución.

En el siguiente paso se tratan las amenazas, esto implica todo aquello que puede provocar una vulnerabilidad. La probabilidad de la amenaza, el grado de vulnerabilidad y la severidad del impacto se relacionan entre sí para emitir un criterio acerca de la evaluación del riesgo.

Finalmente se debe realizar la selección de contramedidas o salvaguardas y una evaluación de su eficacia, que también identifica el riesgo residual. El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones basadas en un fundamento.

- **Control de activos:**Son considerados como activos los recursos del sistema de información o que tengan una relación con éste, y son necesarios para que la Institución funcione correctamente y alcance los objetivos propuestos por su gerencia. La Tabla I muestra el valor que se debe asignar a cada uno de los activos, clasificados según el daño que puedan ocasionar a la Institución en caso de que exista algún daño.

TABLA I
VALORACIÓN DE ACTIVOS

Valoración de activos			
Valor	**Disponibilidad**	**Integridad**	**Confidencialidad**
5	Este nivel abarca toda información, instalación o recurso cuya disponibilidad siempre debe garantizarse. Su pérdida es considerada como catastrófica para la Institución.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es en extremo importante y debe garantizarse bajo cualquier circunstancia. Su pérdida es considerada como catastrófica.	Este nivel abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
4	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
3	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es de importancia media y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
2	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.
1	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por varios días sin causar consecuencias.	Este nivel abarca toda información, instalación o recurso en el cual la pérdida de integridad es insignificante.	Este nivel abarca toda información, instalación o recurso calificado como de uso público.

- **Control de amenazas:** Este proceso consiste en determinar las amenazas que pueden afectar a cada activo perteneciente a la institución. Las amenazas son sucesos que pueden ocurrir causando daños a los activos. Hay accidentes naturales como inundaciones, terremotos, etc., y desastres industriales en los que se encuentran la contaminación, fallos eléctricos, entre otros, ante los cuales el sistema de información es víctima pasiva.
  De la misma manera existen amenazas que pueden ser causadas por las personas, que pueden ser desde un error de usuario hasta un ataque mal intencionado.

Valoración de las amenazas

Para determinar si una amenaza puede ocasionar daños o no a un activo, se debe estimar cuán vulnerable es el activo, para esto es necesario realizar un análisis tomando en cuenta dos criterios:

1) Degradación: cuán perjudicado resulta el activo
2) Frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Se suele caracterizar como una fracción del valor del activo.

La Tabla II muestra los valores en porcentaje (%) de degradación de un activo en el caso de que la falla se materialice.

TABLA II.
VALOR DE DEGRADACIÓN DE UN ACTIVO

DEGRADACIÓN DEL ACTIVO (Si la falla ocurre)		
DESCRIPCIÓN	**DEGRADACIÓN %**	**VALOR**
Baja	25	1
Media	50	2
Alta	75	3
Total	100	4

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de consecuencias fatales pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acumular un daño considerable. La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos.

La Tabla III, muestra los valores representativos de frecuencia de ocurrencia de amenazas basados en una tasa anual, según indica la metodología MAGERIT. La frecuencia está expresada en tiempo (t).

TABLA III.
VALORES REPRESENTATIVOS DE FRECUENCIA DE AMENAZAS EN ACTIVOS

VALOR	TASA	OCURRENCIA	TIEMPO
4	100	muy frecuente	a diario
3	10	Frecuente	mensualmente
2	1	Normal	una vez al año
1	1/10	poco frecuente	cada varios años

Valoración del riesgo

La Tabla IV muestra el nivel del riesgo con su respectivo valor numérico, entendiéndose al valor más alto como el más expuesto a amenazas dentro de la institución. La valoración del riesgo se expresa en porcentaje.

TABLA IV.
NIVELES DE VALORACIÓN DEL RIESGO

Nivel de factor de riesgo	Valor	Porcentaje %
Bajo	1 a 32	1-25
Medio	33 a 63	26-50
Alto	64 a 94	51-75
Extremadamente alto	95 a 125	76-100

- ***Salvaguardas:*** Es necesario planificar el conjunto de salvaguardas pertinentes para disminuir tanto el impacto como el riesgo, reduciendo la degradación del activo (minimizando el daño), o reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

  Para esto es necesario, establecer una política de la Organización al respecto, es decir directrices generales de quién es responsable de cada actividad.

III. DISEÑO E IMPLEMENTACIÓN DEL SGSI

A. Diseño del SGSI

El diseño del SGSI está basado en 11 objetivos de control, cada uno de ellos debe cumplir con los requisitos que se muestran en la Fig.3.

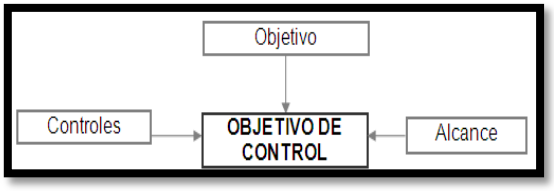

Fig. 3.Requisitos de desarrollo para objetivos de control

Las políticas de seguridad basadas en objetivos de control tienen como finalidad brindar una guía de procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Los beneficios de un sistema de seguridad con políticas claramente concebidas y bien elaboradas son inmediatos, ya que el CP-12 trabajará sobre una plataforma confiable. Con la implementación de las políticas se logran los objetivos de control indicados en el diseño del SGSI.

Las políticas descritas en este documento están enfocadas en dar cumplimiento a los objetivos de control implementados, de igual manera la selección de las herramientas se basa en la funcionalidad que presta cada una de ellas y el soporte que brinda a los controles mencionados en la norma ISO 27002.

A continuación se listan los objetivos de control:

1. **Política de Seguridad:**Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requerimientos de la institución y a las leyes y regulaciones vigentes dentro del CP-12.
2. **Organización de la seguridad de la información:** Gestionar la seguridad de la información dentro del CP-12
3. **Gestión de activos:** Alcanzar y mantener una protección adecuada de los activos de la institución asegurando que se aplica un nivel de protección adecuado a la información.
4. **Seguridad de los recursos humanos:** Asegurar que el personal, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen.
5. **Seguridad física y ambiental (Entorno físico de los activos):** Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
6. **Gestión de las comunicaciones y operaciones:** Asegurar la operación correcta y segura de los recursos de tratamiento de información.
7. **Control de acceso:** Controlar los accesos a la información.
8. **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Garantizar que la seguridad es parte integral de los sistemas de información.
9. **Gestión de incidentes en la seguridad de la información:** Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.
10. **Gestión de la continuidad comercial:** Reaccionar a la interrupción de actividades y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
11. **Cumplimiento:** Evitar incumplimientos de ley, estatuto, regulación u obligación establecida dentro de la institución.

B. Arquitectura de red implementada

Previo a la implementación de herramientas se estructuró la red del CP-12 como se muestra en la Fig. 4.

De acuerdo a las necesidades de la institución y sus debilidades, la solución planteada pretende mejorar los niveles de seguridad reduciendo al máximo las vulnerabilidades.

La arquitectura de red implementada utiliza un servidor UTM desarrollado sobre software libre que controla el acceso de usuarios a los recursos de red del CP-12.Con la implementación de este servidor se reduce la posibilidad de obtención de información de manera no autorizada, además se controla el acceso de los usuarios hacia las aplicaciones necesarias para el desarrollo de sus actividades, de igual manera a los usuarios de la red LAN hacia servicios públicos. Sobre el servidor se encuentran funcionando los servicios firewall, proxy, IDS/IPS y NTOP. Además, la red está dividida en 3 zonas que limitan con el UTM implementado.

- **Zona LAN.-** Es la red interna LAN del CP-12 en donde se encuentran todos los usuarios.
- **Zona de Servidores.-** Esta zona debe ser independiente del resto para poder controlar el acceso tanto de usuarios internos como de usuarios externos a la institución.
- **Zona Wireless.-** Esta zona al ser independiente permite controlar todo el tráfico desde y hacia la subred inalámbrica ya que no se tiene control de los usuarios que intentan acceder de esta manera.

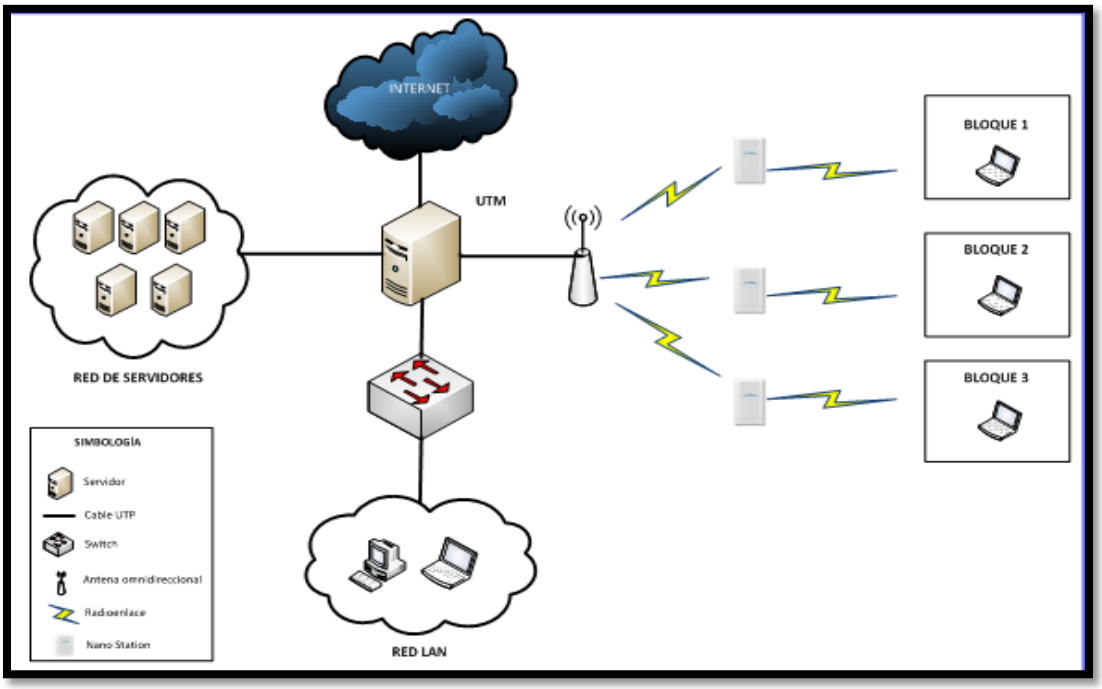

Fig. 4.Arquitectura de red implementada en el CP-12

C. Herramientas implementadas

- **Generador de contraseñas RPG.-** IObit Random Password Generator es una herramienta que permite generar hasta cien contraseñas aleatorias. Únicamente es necesario escoger la longitud (desde seis hasta 64 caracteres), el tipo de caracteres y la cantidad de claves a crear. Dependiendo del tipo y cantidad de caracteres, una contraseña será más o menos fuerte. IObit Random Password Generator indicará en la tabla de claves mediante una leyenda de cuatro colores.

- **Controlador de dominio con Samba 4.-** La implementación del Controlador de dominio se realiza sobre Samba 4 que es un proyecto de código abierto y además es una opción alternativa a Microsoft AD .

Uno de los objetivos de Samba4 es implementar un controlador de dominio compatible con varios sistemas operativos.

- **iTALC.-** Es una aplicación didáctica de monitorización, que ofrece la oportunidad de supervisar e influir en las actividades de los usuarios.Se trata de un software de uso libre y de muy sencilla instalación que permite controlar los equipos de usuarios a distancia.Permite ver el contenido de las pantallas de los usuarios en la propia pantalla del administrador.

- **Nagios3-NCONF.-** Nagios es una aplicación de código abierto para monitoreo de sistemas y redes. Revisa equipos y servicios que se le específica,

alertando cuando el comportamiento de los mismos no sea el deseado.
Para poder añadir de una forma sencilla los sistemas que se desea, se utiliza NCONF como herramienta gráfica de configuración para Nagios.
NConf es una herramienta de código abierto que permite administrar los archivos de configuración de Nagios a través del uso de una interfaz gráfica de usuario, en lugar de mantener los archivos de configuración con un editor de texto.

- **OCS Inventory.-** Open Computer and Software Inventory Next Generation (OCS-NG) es un software libre que permite a los usuarios administrar el inventario de sus activos de TI.
  OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS.

- **OTRS (Open-source Ticket Request System). -** Es una aplicación web Open Source que permite ofrecer servicio on-line con la utilización de tickets soportando multi-usuarios.
  El OTRS permite realizar una gestión integrada de las solicitudes de servicio, información o cualquier requerimiento que realice un usuario a un área, dirección o cualquier entidad o agente que le solicite asistencia.

- **Servidor de archivos con samba 3.-**Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, podrán tener acceso al archivo del servidor en lugar de tener que pasarlo entre distintos equipos.

- **Cobian Backup.-** Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP.
  También soporta SSL. Se ejecuta sobre Windows y una de sus grandes ventajas es que consume muy pocos recursos.

- **Truecrypt.-** Es una aplicación gratuita que permite crear volúmenes cifrados, de manera que todo lo que contengan estos volúmenes pueda ser accedido únicamente si se conoce la contraseña y el fichero clave que se utiliza en su creación.

- **UTM.-** Los sistemas de Gestión Unificada de Amenazas constituyen una solución de seguridad mejorada ya que integran múltiples tecnologías integradas cubriendo las exigencias básicas de protección integral.
  El UTM combina un firewall, un proxy, IDS/IPS y herramientas de monitoreo, todo en un único equipo y a tiempo real.

- **MRTG.-** (Multi Router Traffic Grapher), es una herramienta que permite monitorizar varias características de los servidores reportando la información en gráfica visible por medio de un html.

IV. CONCLUSIONES

El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma ISO/IEC 27001, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua, que consiste en Planificar- Hacer-Verificar-Actuar, de igual manera tiene también su fundamento en la norma ISO/IEC 27002:2005, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información.

Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Una política de seguridad es una forma de comunicarse con los usuarios, ya que las mismas establecen un instructivo de comportamiento del personal, en relación con los recursos y servicios tecnológicos de la organización.

La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para lograrlos objetivos de la institución.

Llegar a tener seguridad total en una red es inalcanzable pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.

El uso de software libre en instituciones públicas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las tecnologías de la información.

RECONOCIMIENTOS

Se expresa un especial reconocimiento al Departamento de Sistemas del CP-12, en especial al Ing. Ángel Núñez, director del mismo e Ing. Israel Cevallos, por el apoyo y colaboración brindada para desarrollar este trabajo.

REFERENCIAS

[1] ISO/IEC, ISO 27000.(2011). Normativa ISO y estándares referentes. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

[2] Bitberry Software ApS. (2012). Seguridad de la información. Disponible en: http://www.bitzipper.com/es/aes-encryption.html

[3] Consejo Superior de Informática. (2012) MAGERIT. Versión 1.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

[4] Gestión de calidad, Implantación ISO 27001:2005. (2011). Disponible en: http://www.gestion-calidad.com/implantacion-iso-27001.html

[5] Mendoza Rosendo A., SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.CASO: CENTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN. Venezuela. 2008. Disponible en http://www.slideshare.net/mmujica/mi-defensa

Jaime R. Michilena C.

Jaime Roberto Michilena Calderón, nació el 19 de febrero de 1983, en la ciudad de Atuntaqui, Provincia de Imbabura. Ingeniero en Electrónica y Telecomunicaciones de la Escuela Politécnica Nacional (2006), Egresado Maestría en Redes de Comunicación de la PUCE (2012).

Actualmente se desempeña como docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la FICA en la Universidad Técnica del Norte.

Además ha colaborado de manera constante e incondicional en el voluntariado del Instituto de Ingenieros Eléctricos y Electrónicos-IEEE como Consejero de la Rama Estudiantil IEEE-UTN a partir del año 2011.

Paola A. Díaz P.

Nació en Quito-Ecuador el 7 de Septiembrede 1987. Hija de Ramiro Díaz y Soledad Parco. Realizó sus estudios primarios en laEscuela Fiscal de Niñas "María Angélica Idrobo".

En el año 2005 obtuvo su título de Bachilleren Ciencias con especialización Físico Matemático en el Colegio Nacional de Señoritas "Ibarra". Actualmente, es egresada de laCarrera de Ingeniería Electrónica y Redes deComunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.