ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROCEDIMIENTO PARA EVALUAR EL RENDIMIENTO Y SEGURIDADES DE SERVIDORES WINDOWS

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

MANOBANDA CAZA GABRIELA ALEXANDRA

gabyale22@hotmail.com

DIRECTOR: MSC. JAIME NARANJO

naranjojf@epn.edu.ec

Quito, diciembre 2009

DECLARACIÓN

Yo, Gabriela Alexandra Manobanda Caza, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

Gabriela Alexandra Manobanda Caza

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Gabriela Alexandra Manobanda Caza, bajo mi supervisión.

Msc. Ing. Jaime Naranjo

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por guiar mi camino y darme siempre la fortaleza para alcanzar esta tan deseada meta.

A mis padres por apoyarme incondicionalmente a lo largo de toda mi vida. Gracias por todo su amor y paciencia.

A mis hermanos, Lore y Willy, quienes a pesar de habernos separado físicamente, siguen estando en mi corazón. Les agradezco mucho por todas sus palabras de apoyo, los quiero mucho loquitos.

A mis tías y tíos por su cariño, consejos y respaldo. Han sido y serán mi ejemplo de lucha a seguir. Gracias por mantener vivo el recuerdo de la Chelita.

A mi esposo Edison, quien me ha brindado su amor y compresión desde el día que lo conocí. Te amo mucho.

A la familia de mi esposo, quienes me han tratado como uno de ellos, brindándome consejos y apoyo.

A mi tutor Jaime Naranjo por su paciencia durante el desarrollo de esta tesis.

A mis amigos y amigas con quienes viví buenos y malos momentos durante el tiempo que pudimos compartir en la Universidad.

Gracias.

Gaby

DEDICATORIA

El presente proyecto, lo dedico con mucho cariño a las siguientes personas, ya que sin ellos no hubiese podido llevarse a cabo.

A mi papi, por comprender y apoyar todas las decisiones que he tomado. Le quiero mucho.

A mi mami, por su tiempo y dedicación que le ha brindado a nuestro Juanito José. Mami, sin usted no hubiese podido lograrlo. Gracias de todo corazón por todo. Le quiero mucho.

A mi hijo hermoso, quien es la luz que llena mi vida y es la principal motivación que tengo para salir adelante. Gracias por tu hermosa sonrisa que en los momentos más difíciles me han fortalecido.

A mis hermanos, para que sepan que con dedicación y sacrificio, se puede obtener alcanzar las metas propuestas.

A mi esposo, quien ha comprendido y soportado mi malos ratos.

A mis primos, quienes han empezado a darse cuenta del arduo camino que tienen por vivir. Nunca se rindan y luchen por ser felices siempre.

Gaby

CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE TABLAS

RESUMEN

El presente procedimiento, ha sido desarrollado con la finalidad de apoyar y facilitar el trabajo de los profesionales de TI en las actividades de evaluación y monitoreo de los sistemas de información. Tiene como objetivo evaluar el rendimiento y las seguridades de los servidores Windows.

El rendimiento de un servidor puede verse afectado no solo por sus componentes internos sino también por los diferentes procesos del sistema en el que trabaja. El presente trabajo muestra un estudio de las principales herramientas de evaluación, además incluye un listado de plantillas con las características básicas de las funciones con las que debe cumplir un servidor Windows.

Para evaluar de forma general a una organización se tomó como referencia la Metodología para la Evaluación del Desempeño de una Unidad Informática desarrollada por el Ingeniero Jaime Naranjo; y para la evaluación de las seguridades se tomó como referencia lo módulos de los estándares de mejores prácticas como: COBIT, ITIL y la Norma ISO/IEC 27001.

Finalmente, este procedimiento fue aplicado en el Servidor de Autenticación RADIUS de los Laboratorios DICC de la Facultad de Ingeniería de Sistemas. Los resultados se detallan en el Informe Técnico.

INTRODUCCIÓN

En la actualidad, la información es el activo más importante de una organización, aunque en ciertos lugares es el menos atendido. La continua evaluación del desempeño y de las seguridades del mismo mejora su porcentaje de disponibilidad, ayudando a la organización a alcanzar sus objetivos.

El siguiente trabajo hace una recopilación de las mejores prácticas existentes, para la creación de un procedimiento de evaluación que tiene como objetivo el obtener resultados rápidos que permitan a una organización tomar las decisiones estratégicas a tiempo.

La estructura del presente trabajo se resume de la siguiente manera:

Capítulo 1: Presenta una parte de la base teórica a utilizarse para la elaboración del procedimiento, se desarrolla en primera instancia el planteamiento del problema en cual se realiza una comparación de las plataformas Windows 2003 y 2008 Server. Se definen las herramientas de evaluación a utilizarse en la aplicación del procedimiento.

Capítulo 2: Presenta un estudio de los parámetros de evaluación y valores umbrales establecidos para cada recurso; relacionando de esta manera, las herramientas de evaluación con los parámetros que pueden medir.

Capítulo 3: Es la recopilación teórica para desarrollar el procedimiento de evaluación con respecto a la seguridad. Se establecen los componentes de seguridad, las políticas y procesos para la evaluación de riesgos e incidentes que deben administrarse en la organización.

Capítulo 4: Corresponde a la elaboración del procedimiento, en el que se establecen los pasos a seguir para realizar la evaluación tanto del rendimiento como de las seguridades. Presenta además, los resultados obtenidos al validar el procedimiento en el Servidor RADIUS perteneciente a los Centro de Gestión de los Laboratorios DICC.

Capítulo 5: Se detallan las conclusiones y recomendaciones originadas a partir de la ejecución del presente proyecto de titulación; tanto de la elaboración del procedimiento como de la aplicación del mismo.

CAPÍTULO 1

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad la red de computadores se ha convertido en el principal medio de comunicación de una organización ya que a través de esta se obtienen varios servicios que los miembros de la empresa requieren, dichos servicios son provistos por un servidor o conjunto de servidores, los mismos que deben ser seguros, confiables, rápidos y deben asegurar un buen rendimiento; por tal motivo es necesario realizar evaluaciones periódicas que ayuden a mantener un buen rendimiento tanto de los servidores como de los demás elementos de la red.

Las bajas en el rendimiento de un servidor pueden darse por varias causas, algunas de ellas pueden ser tratadas por simple intuición solucionando de esta forma el o los problemas que los generan, pero dicha solución puede ser temporal si no se aplica un correctivo definitivo; con este antecedente nace la realización del presente procedimiento que apoya a la persona que está a cargo del servidor o los profesionales de TI[1], en la toma de decisiones proporcionándoles criterios claros para realizar la evaluación.

El rendimiento del sistema puede ser evaluado en cualquier etapa de su ciclo de vida dependiendo del objetivo con el que se haga la evaluación, por lo general lo que se busca es que el sistema cumpla con las metas de rendimiento deseadas y de no ser así, la evaluación permitirá tomar decisiones estratégicas. Para el presente proyecto se realizará la evaluación en un sistema que ya esté en funcionamiento, en el que se pueda aplicar los conocimientos aprendidos en clase permitiendo establecer conclusiones y recomendaciones que ayuden al evaluador la tarea de administrar la red.

---

[1] TI [Tenology Information, Tecnología de la Información]

Es importante destacar que el rendimiento de un sistema depende más de la relación entre sus componentes y de cómo se combinan estos entre sí que del funcionamiento de cada uno de ellos por separado. Por tal motivo, el rendimiento del sistema puede mejorar no solo combinando los mejores elementos lógicos, físicos y de recursos humanos; sino por una adecuada coordinación de estos.

Las falencias que pueden estar afectando el rendimiento de la red pueden tener relación directa con el rendimiento del servidor; por tal motivo se debe realizar evaluaciones periódicas, en las que los datos tomados permitan determinar las posibles causas de los problemas con el objetivo de solucionarlos. Es importante poder determinar con que efectividad administra los recursos un sistema operativo determinado, actualmente existe una mejora en el uso de los recursos, pero, muchas organizaciones realizan muy poco o ningún control o evaluación. Además, cuando se hacen controles específicos se generan grandes cantidades de datos que no se sabe como interpretar porque muy pocas veces se cuenta con personal instruido en lo que se refiere a técnicas de análisis de rendimiento.

"El rendimiento expresa la manera o la eficiencia con que un sistema de computación cumple con sus metas"[2]*,* es una cantidad relativa más que absoluta pero suele hablarse de medidas absolutas de rendimiento. Algunas medidas son difíciles de cuantificar, por ejemplo, la facilidad de uso; otras medidas son fáciles de cuantificar, por ejemplo, acceso a un disco en una unidad de tiempo. Las mediciones de rendimiento se pueden orientar hacia el usuario, por ejemplo, tiempos de respuestas; o hacia el sistema, por ejemplo, utilización de la Unidad de Procesamiento.

El rendimiento se evalúa mediante técnicas entre las que se destacan:

---

[2] Fuente: H. M. Deitel, Introducción a los Sistemas Operativos, Addison-Wesley, México, 1987

- Tiempos: Proporcionan los medios para realizar comparaciones rápidas del hardware.

- Mezclas de instrucciones: Se usa un promedio ponderado de varios tiempos de las instrucciones más apropiadas para una aplicación determinada; los equipos pueden ser comparados con mayor certeza de la que proporcionan los tiempos por sí solos. Son útiles para comparaciones rápidas del hardware.

- Programas del núcleo: Un programa núcleo es un programa típico que puede ser ejecutado en una instalación. Se utilizan los tiempos estimados que suministran los fabricantes para cada máquina para calcular su tiempo de ejecución.

- Modelos analíticos: Son representaciones matemáticas de sistemas de computación o de componentes de sistemas de computación. Requieren un gran nivel matemático del evaluador y son confiables solo en sistemas sencillos, ya que en sistemas complejos los supuestos simplificadores pueden invalidar su utilidad y aplicabilidad.

- Puntos de referencia: Llamados también programas de comparación del rendimiento, son programas reales que el evaluador ejecuta en la máquina que se está evaluando. El programa completo se ejecuta en la máquina real con datos reales. Se deben seleccionar cuidadosamente los puntos de referencia para que sean representativos de los trabajos de la instalación. Los efectos del software pueden experimentarse directamente en vez de estimarse.

- Programas sintéticos: Combinan las técnicas de los núcleos y los puntos de referencia. Son programas reales diseñados para ejercitar características específicas de una máquina.

- Simulación: Es una técnica con la cual el evaluador desarrolla un modelo computarizado del sistema que se está evaluando. Es posible preparar un

modelo de un sistema inexistente y ejecutarlo para ver cómo se comportaría en ciertas circunstancias; se puede evitar la construcción de sistemas mal diseñados.

- Control del rendimiento: Es la recolección y análisis de información relativa al rendimiento del sistema existente. Permite localizar embotellamientos con rapidez, ayuda a decidir la forma de mejorar el rendimiento y puede ser útil para determinar la distribución de trabajos de varios tipos. El control del rendimiento puede hacerse por medio de herramientas de hardware o de software llamadas monitores. Un Monitor es una herramienta diseñada para observar la actividad de un sistema informático mientras es utilizado por los usuarios; entre las acciones típicas de un monitor están:

    - Observar el comportamiento
    - Recoger datos estadísticos
    - Analizar estos datos
    - Mostrar los resultados

  Los monitores producen grandes cantidades de datos que indican con precisión cómo está funcionando un sistema; por tal motivo son de mucha ayuda al momento de evaluar su rendimiento cuando estos ya están en funcionamiento; ayudando además a tomar las decisiones de diseño adecuadas.

En general, en cualquier sistema es difícil valorar el rendimiento, debido a que intervienen algunas variables, y no existe un único parámetro que indique el resultado de su funcionamiento, por tal motivo y con la ayuda de los monitores de rendimiento mencionados en la técnica de control de rendimiento, se realizará la evaluación del rendimiento de los sistemas operativos Windows Server 2003 y Windows Server 2008; permitiendo de esta manera reducir el tiempo en la búsqueda de posibles cuellos de botella presentes en el sistema.

Cabe mencionar que el rendimiento general del sistema, como se explicará en temas posteriores, puede verse limitado por la velocidad de acceso a los discos

duros físicos, la cantidad de memoria disponible para ejecutar procesos, la velocidad máxima del procesador o el rendimiento máximo de las interfaces de red. Una vez que se ha identificado las limitaciones de rendimiento del hardware, se procede a supervisar aplicaciones y procesos individuales para valorar qué uso hacen de los recursos disponibles. Los profesionales de TI pueden usar un análisis amplio del rendimiento tanto del efecto de las aplicaciones como de la capacidad global para ayudar a planear implementaciones y aumentar la capacidad del sistema según aumenta la demanda.

Para facilitar la tarea de analizar el rendimiento, los sistemas operativos estudiados en este proyecto de tesis incluyen herramientas de evaluación de rendimiento. Windows Server 2003 tiene herramientas individuales de gran ayuda como son: el Monitor del Sistema, Registro y alertas de rendimiento y Server Performance Advisor.

Windows Server 2008 incluye nuevas características en su Monitor de Confiabilidad y Rendimiento, el mismo que combina la funcionalidad de las herramientas antes mencionadas en una misma interfaz gráfica con métodos comunes para personalizar conjuntos de recopiladores de datos y sesiones de seguimiento de eventos; complementando de esta forma, el análisis del rendimiento con un análisis de la confiabilidad del sistema, permitiendo determinar posibles eventos que pueden estar afectando la estabilidad general del sistema.

Otro aspecto importante que se toma en cuenta para establecer el procedimiento, es la seguridad que brindan los sistemas operativos de la familia Windows Server ya que al ser Microsoft la plataforma más difundida y comercializada la hace más vulnerable; por tanto es necesario identificar los riesgos y amenazas que pueden presentarse tanto en el sistema operativo en sí como en su entorno. Cuando se habla de seguridad, lo primero que se necesita establecer es: qué se va a proteger, de qué se lo va a proteger y cómo se lo va a hacer, encontrando de esta forma,

posibles fallas en la seguridad que pueden estar afectando el funcionamiento del sistema o los resultados que se obtienen del mismo.

Una de las metas que busca este procedimiento es el establecer las mejores prácticas de seguridad que faciliten la tarea de protección de los servidores Windows.

El ámbito de las seguridades es muy amplio por tal motivo se ha tomando como base la Norma ISO 27001, la misma que permite realizar una adecuada evaluación de la seguridad de los sistemas de información; se sugiere que la aplicación de la norma se la realice mediante la aplicación de checklists, lo que permitirá determinar con mayor certeza el nivel de seguridad y posibles falencias que pueden tener los sistemas operativos servidor Windows 2003 y Windows 2008.

La norma ISO 27001 comprende una metodología dedicada a la seguridad de la información, puede ser aplicada a todo tipo de organizaciones independientemente de su tamaño o actividad; y se la puede dividir en dos grandes áreas:

- Un conjunto de controles que materializan las mejores prácticas en seguridad de la información.

- Un proceso para evaluar, implantar, mantener y administrar un Sistema de Gestión de Seguridad de la Información (SGSI).

El objetivo que busca este SGSI es orientar todos los esfuerzos hacia la protección de la información, facilita además la administración de los riesgos priorizando los controles necesarios a ser aplicados y permite mantener un nivel de seguridad adecuado para que la organización funcione eficientemente.

Esta norma adopta el modelo PDCA (Plan - Do - Check - Act), el cual es aplicado a toda la estructura de procesos del SGSI; a continuación se describe un breve resumen del modelo:

- Como primer punto este modelo pretende establecer el SGSI (Plan): Implica, establecer la política SGSI, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- A continuación hay que implementar y operar el SGSI (Do): Representa la forma en que se debe operar e implementar las políticas, controles, procesos y procedimientos.

- Luego se debe monitorizar y revisar el SGSI (Check): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados para su revisión.

- Finalmente hay que mantener y mejorar el SGSI (Act): Realizar las acciones preventivas y correctivas, basados en auditorias internas y revisiones del SGSI o cualquier otra información relevante para permitir la mejora continúa del SGSI. [3]

Parte fundamental de este procedimiento es el de trabajar conjuntamente con la norma 27001 y demás elementos de apoyo como las herramientas de seguridad propias de cada sistema operativo, que ayuden a mantener la seguridad de los sistemas operativos estudiados en el presente proyecto de tesis.

Microsoft ofrece continuamente nuevas o mejoradas herramientas de seguridad que permiten mitigar en parte las amenazas tecnológicas que cada vez son más sofisticadas, haciendo posible que las organizaciones sigan operando con la misma

[3] Fuente: Estándar Internacional ISO/IEC 2700, Primera Edición, año 2005, Pág. 6

eficiencia y brindando el mayor nivel de productividad posible. Los sistemas operativos Windows Server 2003 y Windows Server 2008 incluyen dichas herramientas y tecnologías de seguridad.

Windows Server 2008 integra una serie de nuevas tecnologías de seguridad que aumentan la protección del sistema operativo, permitiendo reducir la exposición a ataques, lo que produce un entorno de servidor más seguro y estable. El sistema de protección de servicios de Windows ayuda a mantener más seguros los sistemas al evitar que servicios críticos de servidor estén en riesgo por actividades anormales en el sistema de archivos, registro, o red. La seguridad también se mejora por medio de la protección de acceso a redes (NAP) que incluye este sistema operativo, incluye también un controlador de dominio de sólo lectura, mejoras en la infraestructura de clave pública, un nuevo firewall de Windows bidireccional y compatibilidad con criptografía de última generación.

Windows Server 2003 es el sistema operativo más seguro que ha comercializado Microsoft. Proporciona una infraestructura integrada que ayuda a afirmar que la información estará segura y también proporciona fiabilidad, disponibilidad, y escalabilidad, haciendo de este el sistema de red que los usuarios solicitan. Entre las funciones de seguridad clave están las relacionadas a la confianza entre bosques del servicio Microsoft Active Directory, integración Microsoft .NET Passport. La administración de identidades en Active Directory abarca la totalidad de la red, ayudando a consolidar la seguridad en toda la organización. El cifrado de datos confidenciales es muy sencillo y las directivas de restricción de software pueden usarse para prevenir los daños causados por virus u otro tipo de código malintencionado. Permite además implantar una infraestructura de claves públicas y las funciones de inscripción y de renovación automáticas facilitan la distribución de tarjetas inteligentes y certificados en la empresa.

Dado que el procedimiento de evaluación del rendimiento y seguridades de servidores será aplicado a los sistemas operativos Windows Server en sus ediciones Windows 2003 Server y Windows 2008 Server, que en la actualidad son los más utilizados, se describe a continuación en resumen sus principales características.

Windows Server 2003

Se basa en los sólidos fundamentos de Windows 2000 Server; superando a este en fiabilidad, escalabilidad, rendimiento, facilidad de uso y administración; hay quienes lo consideran como un XP modificado ya que tiene deshabilitadas algunas de las funciones que en Windows Server 2003 permiten mejorar su rendimiento y centrar el uso de procesador en las características de servidor. Ofrece todas las funciones que todo cliente espera de un servidor como son: rapidez, seguridad, confiabilidad y escalabilidad. Entre las principales características se tiene:

- El sistema de archivos es de tipo NTFS lo que permite entre otras cosas, el cifrado y compresión de archivos, carpetas y no unidades completas.

- Permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo Unix.

- Incluye una gestión jerárquica de almacenamiento.

- Su Directorio Activo se basa en LDAP lo que permite gestionar de forma centralizada la seguridad de una red.

- Incluye DNS con registro de IP's dinámicamente.

- La autentificación la hace mediante el protocolo Kerberos5.

- Provee políticas de seguridad.

- Incluye Windows Driver Model, lo que permite una implementación básica de los dispositivos más utilizados, con lo que los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware.

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una amplia gama de funciones de servidor, en base a las necesidades de cada organización, tanto de manera centralizada como distribuida. Incorpora

innumerables ventajas, mejoras y nuevas tecnologías, orientadas todas ellas a cubrir las necesidades de organizaciones de cualquier tamaño. Entre las funciones de servidor están:

- Servidor de archivos e impresión.
    - Servidor Web y aplicaciones Web.
    - Servidor de correo.
    - Terminal Server.
    - Servidor de acceso remoto/red privada virtual (VPN).
    - Servicio de Directorio Activo.
    - Sistema de dominio (DNS), y servidor DHCP.
    - Servidor de transmisión de multimedia en tiempo real (Streaming).
    - Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

A continuación se describen algunos aspectos básicos de Windows Server 2003

- Confiable: lo que hace a este sistema operativo altamente confiable son la disponibilidad, escalabilidad y seguridad.

    - La disponibilidad se consigue gracias a la compatibilidad de organización de clústeres, lo que se ha convertido en un elemento fundamental para las organizaciones especialmente para aquellas que distribuyen aplicaciones empresariales vitales, aplicaciones de comercio electrónico y aplicaciones de línea de negocios específica.

    - Con respecto a la escalabilidad Windows Server 2003 la proporciona a través del escalado vertical, habilitado por el multiproceso simétrico (SMP) y el escalado horizontal, habilitado por la organización de clústeres.

    - En lo referente a la seguridad: Windows Server 2003 proporciona diversas funciones y mejoras nuevas en la seguridad, como por

ejemplo: The common language runtime, motor de software, elemento clave de Windows Server 2003 que mejora la confiabilidad y facilita un entorno informático seguro. Y provee un Internet Information Services 6.0 que está configurado para obtener la máxima seguridad de forma inmediata; con la finalidad de aumentar la seguridad del servidor Web.

- Productividad: Este sistema operativo provee ciertos elementos que ayudan a mejorar la productividad como son: servidor de archivos e impresión, directorio activo, administración de servicios, administración del almacenamiento y servicio de Terminal.

- Conectividad: Tiene funciones y mejoras que permiten que las organizaciones y los usuarios permanezcan conectados; entre las que están:

    - Servicios Web XML para administradores y desarrolladores de aplicaciones Web. La seguridad se incrementa gracias a que el administrador del sistema habilita o deshabilita las funciones del sistema en función de los requisitos de las aplicaciones necesarias.

    - Redes y comunicación: Las mejoras en las redes y las nuevas funciones de la familia de Windows Server 2003 amplían la versatilidad, la capacidad de administración y la confiabilidad de las infraestructuras de red.

    - Servicios de Windows Media: Windows Server 2003 incluye los servicios digitales de multimedia de transmisión por frecuencias más potentes del sector.

- Ahorro de Costos: Este sistema operativo al incluir múltiples componentes y servicios ofrece un bajo costo total de la propiedad, facilitando que las organizaciones sean más productivas y eficaces. Por otro lado, Como la tecnología PC proporciona la plataforma de chips de costo más razonable, el simple hecho de estar basado en PC proporciona un incentivo económico.

Resumiendo, Windows Server 2003 incluye toda la funcionalidad que los clientes esperan de un sistema operativo de servidor de gran trascendencia, como son: la seguridad, la confiabilidad, la disponibilidad y la escalabilidad. Además, Microsoft ha mejorado y ampliado los sistemas operativos de servidor Windows para que las organizaciones puedan beneficiarse de las ventajas de Microsoft .NET, un software para conectar información, personas, sistemas y dispositivos.

Windows Server 2008

Conocido como Windows Server Longhorn hasta el anuncio de su título oficial en mayo del 2007. Sucesor de Windows Server 2003, incluye mejoras especialmente en el área de funcionamiento de redes, funciones de seguridad avanzadas, acceso remoto a aplicaciones, administración centralizada de roles del servidor, herramientas de monitoreo en términos de rendimiento y confiabilidad, mejoras en el sistema de archivos, fácil instalación, todas estas mejoras permiten maximizar la flexibilidad, disponibilidad y control de servidores; adicionalmente esta plataforma es mucho más segura y de fácil administración. Entre las principales características están:

- Incluye un proceso en segundo plano que permite reparar archivos dañados de sistemas NTFS.

- Permite crear sesiones de usuario en paralelo, con un inicio de sesión único lo que elimina la necesidad de especificar las credenciales varias veces.

- Protección contra malware en la carga de controladores en memoria.

- Ofrece una tecnología eficaz de virtualización con sólidas características de administración y seguridad.

- El núcleo del sistema se ha renovado con muchas nuevas y mejoras que permiten a los administradores instalar únicamente los servicios de Windows Server requeridos.

- Incluye una consola mejorada con soporte GUI que permite controlar de manera más fácil y segura la administración y automatización de tareas rutinarias, en especial a través de varios servidores.

- Ofrece dos nuevas funcionalidades que permiten maximizar el control del acceso a los servidores en red como son: Internet Information Server 7.0 y Network Access Protection.

- Incluye una nueva opción de configuración del controlador de dominio para que sea solo de lectura (Read Only Domain Controler, RODC), que se puede instalar en sitios remotos con niveles muy bajos de seguridad física.

- Cierre limpio de servicios, es decir ya no hay que esperar para la finalización de servicios.

- Incluye un protocolo mejorado y estandarizado de reporte de errores llamado Windows Hardware Error Architecture (WHEA).

Windows 2008 Server es una nueva plataforma que cubre con los actuales requerimientos de las organizaciones enfocándose en sus necesidades críticas; este sistema operativo ofrece la mejor base para cualquier servidor e infraestructura de red de la organización, entre las funciones de servidor se tienen:

  - Windows Server Virtualization
  - Servidor del protocolo de configuración dinámica de host (DHCP)
  - Servidor del sistema de nombres de dominio (DNS)
  - Servidor de archivos
  - Servidor de aplicaciones
  - Servicios de dominio de Active Directory (AD DS)
  - Servicios de directorio ligero de Active Directory (AD LDS)
  - Servicios de Windows Media
  - Administración de impresión
  - Servidor de fax

Los puntos centrales en que este sistema operativo basa su funcionamiento son: el control, la flexibilidad y la seguridad. Control sobre el servidor y sobre la infraestructura de red, protección sobre la totalidad del ambiente, flexibilidad para crear un centro de datos dinámico y ágil que pueda cumplir con las necesidades cambiantes de los negocios.

- Control: Windows 2008 Server ofrece más control sobre sus servidores e infraestructura de red a través de:

    - Windows Power Shell que ofrece más de 130 herramientas y lenguaje scripting integrado lo que ayuda a los profesionales de TI a automatizar tareas comunes de TI.

    - Plataforma unificada para publicación Web que permita satisfacer las necesidades de publicación Web actuales.

    - Un nuevo tipo de configuración del controlador de domino, lo que mejora la seguridad y los tiempos de autenticación.

    - Nuevo esquema de configuración de la consola de Administrador del servidor que facilita la tarea de administrar y proteger las múltiples funciones de servidor.

- Flexibilidad: Este sistema operativo permite a los administradores modificar la infraestructura para adaptarla a las cambiantes necesidades del negocio y continuar siendo ágiles, entre las funciones que ofrecen flexibilidad se tienen:

    - Sever Core que permite instalar únicamente las funciones de servidor necesarias lo que implica menos mantenimiento y actualizaciones y también mayor protección.

    - Servicios de Terminal que permiten tener una integración que llega al punto en que prácticamente no hay diferencias entre un usuario local y uno remoto.

- Tecnologías de virtualización que están incorporadas dentro del sistema operativo lo que permite un despliegue de aplicaciones seguro y sencillo que no requiere conexiones mediante VPNs.

- Seguridad: Windows 2008 Server incorpora una serie de mejoras para la seguridad y refuerzo del sistema operativo entre las que se puede mencionar:

  - Protección de acceso a la red (NAP), bloqueando de este modo, accesos que podrían poner en riesgo la seguridad de la red.

  - Failover Clustering que permite realizar pruebas del sistema, almacenamiento y red para verificar si la computadora está apta o no para actuar como cluster, por medio de esta función los administradores pueden maximizar la disponibilidad de servicios, almacenan más eficientemente y mejoran incluso la seguridad de las instalaciones.

Windows 2008 Server es una plataforma versátil, confiable, segura ya que protege al sistema operativo en sí y al entorno de red; responde además a las necesidades de las organizaciones y ofrece a los administradores de TI mayor flexibilidad gracias a las herramientas de administrativas que son mucho más intuitivas; ofreciendo la mejor base para cualquier servidor e infraestructura de red. En cuanto a rendimiento se refiere, Windows Server 2008 incluye el Monitor de confiabilidad y rendimiento que permite hacer un seguimiento del efecto que tienen las aplicaciones y servicios sobre el rendimiento y puede genera alertas o realizar acciones cuando se superan los umbrales de rendimiento óptimo definidos por el usuario.

Dado que estos dos sistemas operativos tienen innumerables características que los convierten en los más comerciales actualmente al ofrecer alta disponibilidad, seguridad, mayor rendimiento y muchos otras cualidades; se presenta a continuación un cuadro comparativo en el que se podrá ver las funciones de servidor que tiene cada sistema operativo con sus respectivas mejoras:

Funciones	Windows Server 2003	Windows Server 2008
Directorio Activo	Si, incluye renombrado de directorios y replicación más eficiente	Si, incluye servicios de directorio ligero, servicios de federación, servicios de dominio y servicios de certificado
Servidor DHCP	Si	Si
Servidor DNS	Si	Si
Servidor de aplicaciones	Si	Si
Servidor de fax	No	Si
Servidor Web	Si	Si
Servidor de archivos y de impresión	Si	Si
Servidor de correo	Si	No
Servicios de Terminal Services	Si	Si
Servidor de acceso remoto	Si	Si, no necesidad de creación de una VPN
Internet Information Server	Si, IIS 6.0	Si, IIS 7.0
Network Access Protection	No	Si
Servicios de Administrar el Servidor	Si, Gestiona tu Servidor/configura tu servidor	Si, Server Manager
Windows Power Shell	No	Si

Read Only Domain Controler RODC	No	Si
Server Core	No	Si
Windows Deployment Services WDS	No	Si
Failover Clustering	No	Si
Políticas de Grupo	Si	Si, creación de políticas inteligentes y reglas inteligentes
Consola de Gestión de Políticas de Grupo	Si	No
Recuperación automática del sistema (ASR)	Si	Si
.NET Framework	Si, Plataforma completamente integrada	Si
Servicios de Balanceo de Carga	Si	Si, funcionalidad mejorada con ISA Server
Monitor de Rendimiento del Sistema	Si	Si, Monitor de Confiabilidad y rendimiento

Tabla 1:1 Comparativa de Funciones y Tipos de Servidores entre Windows Server 2003 y Windows Server 2008 [4]

[4] Elaborado por: La Autora

1.1. ANÁLISIS Y DEFINICIONES DE LAS HERRAMIENTAS DE EVALUACIÓN

1.1.1. Análisis de los principales factores que ayudan a evaluar el rendimiento

Para realizar la evaluación del rendimiento de los servidores Windows se debe analizar cuales son los principales factores que permiten revelar posibles cuellos de botella que pueden provocar una ralentización del rendimiento de todo el sistema. Los cuellos de botella suelen producirse cuando un recurso alcanza el límite de su capacidad y son provocados normalmente por recursos insuficientes o configurados incorrectamente, componentes que no funcionan debidamente o solicitudes incorrectas de recursos realizadas por un programa.

El rendimiento del servidor puede verse afectado por cuellos de botella presentes en cinco áreas principales: disco, memoria, proceso, red y CPU; si se hace uso excesivo de cualquiera de estos recursos puede llegar al punto de bloquearse; por tanto las herramientas que se utilicen para realizar una adecuada evaluación del rendimiento deben contener por lo menos uno de los factores que se describen a continuación para las cinco áreas antes mencionadas:

- Disco: % de tiempo inactivo, promedio de segundos de lectura y escritura, promedio de la cola de disco, Bytes de caché.
- Memoria: % de bytes confirmados en uso, % de bytes disponibles, entradas libres de la tabla de páginas del sistema, bytes de bloqueo no paginado, bytes de bloqueo paginado, páginas por segundo, % de uso, lectura de página por segundo.
- Procesador: % de tiempo de procesador, % de tiempo de usuario, % de tiempo de interrupción, longitud de la cola del procesador.
- Red: total de bytes/s, longitud de la cola de salida, % de uso.
- Procesos: recuento de identificadores, número de subprocesos, bytes privados.[5]

[5] Fuente: http://technet.microsoft.com/es-es/magazine/2008.08.pulse.aspx

- Servidor: Inicio de sesión por segundo, errores de permisos de acceso, longitud de la cola, sesiones cerradas debido a un error.

En el capítulo 2 del presente proyecto de tesis se estudiarán con mayor énfasis los parámetros de evaluación mencionados.

1.1.2. Definición de las herramientas de evaluación

Existen varias herramientas de software tanto comercial como libre, que tienen uno o varios de los contadores mencionados anteriormente, que ayudan a evaluar el rendimiento del servidor, muchas de estas herramientas se las puede encontrar en Internet, a continuación se listan las más usadas y recomendadas:

- Monitor del sistema: Herramienta propia de los sistemas Windows, en Windows Server 2008 llamada Monitor de confiabilidad y rendimiento.

- Task Manager: Herramienta propia de los sistemas Windows.

- PRTG Network Monitor: Herramienta enfocada hacia el monitoreo de la red, disponible tanto en su edición libre como comercial, distribuida por la compañía PAESSLER. [6]

- Advanced Host Monitor: Herramienta que monitorea continuamente la disponibilidad y rendimiento de los servidores, distribuido por Network Management Solutions, KS-Soft. [7]

- ServerAssist: Herramienta basada en agentes, provee un monitoreo detallado de los servidores sin necesidad de un sistema de monitoreo central. Desarrollado por Aldebaran Systems. [8]

---

[6] http://www.paessler.com
[7] http://www.ks-soft. net
[8] http://www.serverassist.com

- Speed Test: Herramienta que permite monitorear el rendimiento del sistema con la posibilidad de exportar los datos a Excel. Distribuido por Absolute Futurity. [9]

- GFI Network Server Monitor: Herramienta que permite monitorizar automáticamente la red y los servidores en busca de fallos. Desarrollado por GFI Software. [10]

- PCMark05: Herramienta que informa sobre los puntos débiles y fuertes del sistema, las pruebas que realiza dan como resultado una calificación real de los parámetros que evalúa. [11]

- VISUAL Control for Windows: Herramienta de monitorización y gestión multiplataforma en tiempo real de la infraestructura informática. [12]

- ManageEngine OpManager: Herramienta que utiliza características avanzadas, tolerancia a fallas integrada y administración del desempeño. Distribuido por ManageEngine. [13]

La mayoría de las herramientas mencionadas tienen varias funciones que están habilitadas cuando se adquiere la licencia comercial, mientras que en las ediciones libres tienen únicamente funciones básicas. A continuación se presenta una tabla que resume las funciones que tiene cada herramienta, permitiendo así determinar cuándo usar cada una de ellas.

[9] http://www.speedtestpro.net
[10] http://www.gfi.com
[11] http://www.futuremark.com/products/pcmark05
[12] http://www.tango04.es/productos/vcw/index.php
[13] http://www.manageengine.com

	Monitor del Sistema	**PRTG Network Monitor**	**Task Manager**	**Advanced Host Monitor**	**Server Assist**	**Speed Test**	**GFI Network Server Monitor**	**PC Mark05**	**VISUAL Control for Windows**	**OpManager**
Detecta cuellos de botella de disco duro	Si	No	No	Si	Si	Si	No	Si	Si	Si
Detecta cuellos de botella de memoria	Si	Si	Si	Si	Si	Si	No	Si	Si	Si
Detecta cuellos de botella de procesador	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Detecta cuellos de botella de red	Si	Si	Si	Si	Si	Si	Si	No	Si	Si
Detecta cuellos de	Si	No	Si	Si	No	Si	No	No	Si	No

botella de proceso										
Permite establecer umbrales	No	No	No	No	No	No	No	No	No	Si
Permite agregar varios equipos de la red para ser analizados al mismo tiempo	No	No	No	Si	No	No	No	No	No	Si
Windows 2003 Server	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Windows 2008 Server	Si	Si	Si	No	No	No	No	Si	Si	No
Mide el uso del ancho de banda	Si	Si	No	Si	No	Si	Si	No	No	No

Permite agregar contadores	Si	Si	Si	No	No	No	No	No	Si	Si
Presenta los datos en varias vistas como: histograma, informe o gráfico	Si	Si	Si	Si	Si	Si	Si	No	Si	Si
Auto detecta la red	No	No	No	No	Si	No	No	No	No	Si
Notifica fallas mediante correo electrónicos o SMS	No	Si	No	Si	Si	Si	Si	No	Si	Si

Tabla 1:2 Comparativa de las herramientas para evaluar el rendimiento [14]

[14] Elaborado por: La Autora

1.2. JUSTIFICACIÓN DEL USO DE LA METODOLOGÍA

La metodología utilizada para el presente proyecto de tesis se basa en un conjunto de normas, técnicas y herramientas que permiten realizar una adecuada evaluación del rendimiento y las seguridades de los servidores Windows; sirviendo así, de ayuda para los ingenieros en sistemas y en general para administradores y especialistas en TI.

Los marcos de trabajo como: la Norma 27001, COBIT e ITIL son estándares para el uso común, que al ser aprobadas por organismo internacionales reconocidos, proveen reglas, métodos, y procesos que permiten el aseguramiento de la información y de los sistemas que la procesan; por lo que serán el soporte del procedimiento desarrollado en este Proyecto de Tesis.

Las técnicas analizadas en el presente proyecto, se basan en la Metodología para la Evaluación del Desempeño de una Unidad Informática desarrolla por el Ingeniero Jaime Naranjo[15], lo que permite plasmar un enfoque más práctico al momento de evaluar el rendimiento y las seguridades de los servidores.

Finalmente, las herramientas utilizadas para el desarrollo del procedimiento son reunidas de varios sitios de Internet, que al ser las más utilizadas facilitan la tarea de evaluar el rendimiento de los sistemas.

Todos los aspectos mencionados forjan una metodología útil para la evaluación tanto del rendimiento como de las seguridades; haciendo que, de las muchas formas

[15] Fuente: Metodología para la Evaluación del Desempeño de una Unidad Informática; Naranjo Anda, Jaime Fabián, año 2000

que existe para efectuar esta tarea, sea este, el procedimiento facilitador en la administración de servidores Windows.

CAPÍTULO 2

2. EVALUACIÓN DEL RENDIMIENTO EN PLATAFORMAS WINDOWS

La evaluación del rendimiento consiste en examinar el valor de los parámetros que se registran cuando el sistema realiza varias operaciones; mediante este tipo de análisis de datos de rendimiento se puede comprender el modo en que el sistema responde a las exigencias de las cargas de trabajo.

Como resultado de este análisis se puede observar que el sistema funciona satisfactoriamente en algunas ocasiones y de manera no satisfactoria en otras, dependiendo de las causas de estas variaciones y del grado de importancia, se puede optar por tomar las acciones correctivas necesarias.

2.1. PARÁMETROS DE EVALUACIÓN

Los parámetros son características de los recursos del sistema que deben ser seleccionados en función del trabajo que realizará el sistema, la buena o mala selección de estos condicionará la precisión de los resultados al momento de realizar las mediciones; en el presente capítulo se analiza con mayor profundidad los parámetros necesarios para realizar la evaluación del rendimiento.

En un servidor existen cinco áreas importantes en las que se refleja el rendimiento y son: disco duro, memoria, CPU, proceso, red y servidor, si se hace uso excesivo de alguno de estos recursos el servidor o aplicación puede ralentizarse notablemente o puede llegar a bloquearse, a continuación se describe cada una de las áreas mencionadas y los principales parámetros útiles en la medición del rendimiento.

2.1.1. Disco duro

La función del disco duro es la de almacenar y controlar los datos y los programas del servidor, por tal motivo si se presenta un cuello de botella que afecte al uso y a la velocidad del disco tendrá repercusión en el rendimiento general del servidor, para analizar el estado del disco del servidor se mide los parámetros siguientes:

- Disco lógico

Parámetro	Descripción	Unidad de medida
Espacio libre	Mide el porcentaje de espacio libre existente en la unidad de disco lógica seleccionada.	Porcentaje

Tabla 2:3 Parámetros de evaluación del disco lógico [16]

- Disco físico

Parámetro	Descripción	Unidad de medida
Tiempo inactivo	Mide el porcentaje de tiempo en el que el disco ha permanecido inactivo durante el intervalo de medida.	Porcentaje
Tiempo de lectura de disco	Mide el tiempo que necesita el disco para leer los datos.	Porcentaje, segundos

[16] Elaborado por: La Autora

Tiempo de escritura de disco	Mide el tiempo que se tarda en escribir datos en el disco.	Porcentaje, segundos
Longitud promedio de la cola de disco	Indica el número de operaciones E/S que permanecen a la espera de que la unidad de disco duro esté disponible.	Operaciones

Tabla 2:4 Parámetros de evaluación del disco físico[17]

- Memoria

Parámetro	Descripción	Unidad de medida
Bytes de caché	Indica la cantidad de memoria en uso para la memoria caché del sistema de archivos.	Porcentaje, bytes, MB

Tabla 2:5 Parámetros de evaluación del disco duro [18]

2.1.2. Memoria

Una escasez de memoria es normalmente debida a una cantidad insuficiente de RAM, pérdida de memoria o un modificador de comandos de memoria insertado en el archivo boot.ini; por tanto cuando se trata de determinar la memoria que se utiliza,

[17] Elaborado por: La Autora

[18] Elaborado por: La Autora

es necesario examinar la memoria física y el archivo de paginación; y para detectar problemas específicos se analizan los parámetros siguientes:

- Memoria Física

Parámetro	Descripción	Unidad de medida
Bytes confirmados en uso	Mide la proporción de bytes confirmados respecto al límite de confirmación, es decir, la cantidad de memoria virtual en uso.	Porcentaje
MB disponibles	Mide la cantidad de memoria física, disponible para los procesos que se están ejecutando.	Porcentaje, MB

Tabla 2:6 Parámetros de evaluación de la memoria física [19]

- Memoria Lógica

Parámetro	Descripción	Unidad de medida
Entradas libres de la tabla de páginas del	Indica el número de entradas de la tabla de páginas que no está usando actualmente el sistema.	Entradas

[19] Elaborado por: La Autora

sistema		
Bytes de bloque no paginado	Se trata de un área de la memoria del sistema para aquellos objetos que no pueden escribirse en el disco, sino que deben permanecer en la memoria física mientras estén asignados. Mide el tamaño en bytes del bloque no paginado	MB, Bytes
Bytes de bloque paginado	Mide el tamaño en bytes del bloque paginado. Se trata de un área de la memoria del sistema empleada para los objetos que pueden escribirse en el disco cuando no se usan.	MB, Bytes
Páginas por segundo	Mide la velocidad a la que se leen las páginas desde el disco o se escriben en éste para resolver errores severos de página.	Páginas/s

Tabla 2:7 Parámetros de evaluación de la memoria lógica [20]

2.1.3. Procesador

La presencia de cuellos de botella en el procesador puede deberse a que el propio procesador no ofrece un rendimiento suficiente o bien que exista alguna aplicación ineficaz; se puede verificar si el procesador está invirtiendo mucho tiempo en la paginación a consecuencia de no disponer de suficiente memoria física. Los parámetros que ayudan a determinar problemas en el procesador son:

- Procesador

[20] Elaborado por: La Autora

Parámetro	Descripción	Unidad de medida
Tiempo de procesador	Mide el porcentaje de tiempo transcurrido que invierte el procesador en ejecutar un subproceso no inactivo.	Porcentaje
Tiempo de usuario	Mide el porcentaje de tiempo transcurrido que el procesador invierte en el modo de usuario.	Porcentaje
Tiempo de interrupción	Mide el tiempo que el procesador invierte en recibir y atender interrupciones de hardware durante intervalos específicos de medición.	Porcentaje

Tabla 2:8 Parámetros de evaluación del procesador [21]

- Sistema

Parámetro	Descripción	Unidad de medida
Longitud de la cola del procesador	Indica el número de subprocesos que contiene la cola del procesador.	Subprocesos

Tabla 2:9 Parámetros de evaluación de procesador [22]

[21] Elaborado por: La Autora

[22] Elaborado por: La Autora

2.1.4. Red

Un cuello de botella de red, por supuesto, afecta a la capacidad del servidor para enviar y recibir datos a través de la red. Puede tratarse de un problema con la tarjeta de red del servidor, o quizás que la red se haya quedado saturada; se puede usar los siguientes parámetros para diagnosticar los posibles problemas:

- Interfaz de red

Parámetro	Descripción	Unidad de medida
Total de bytes por segundo	Mide la velocidad a la que se envían y reciben bytes a través de cada adaptador de red, incluidos los caracteres de tramas.	B/s
Longitud de la cola de salida	Mide la longitud de la cola de paquetes de salida. Teniendo en cuenta que las peticiones son puestas en la cola por la especificación de interfaz de controlador de red en esta aplicación, este contador deberá ser cero.	Paquetes
Ancho de banda actual	Es una estimación del ancho de banda actual de la interfaz de red en bits por segundo.	bps

Tabla 2:10 Parámetros de evaluación de la interfaz de red [23]

[23] Elaborado por: La Autora

Fuente: Texto explicativo de Microsoft Management Console, Windows 2003 Server

2.1.5. Proceso

El rendimiento del servidor se verá gravemente afectado si tiene un proceso que no funciona de la manera prevista o procesos que no están optimizados, las pérdidas de subprocesos e identificadores podrían incluso llegar a bloquear un servidor, mientras que un uso excesivo del procesador ralentizará notablemente su rendimiento. Los siguientes parámetros son imprescindibles para diagnosticar cuellos de botella relacionados con procesos.

Parámetro	Descripción	Unidad de medida
Recuento de identificadores	Mide el total de identificadores abiertos actualmente por un proceso.	Identificadores
Número de subprocesos	Mide el número de subprocesos activos en ese momento en un proceso	Subprocesos
Bytes privados	Indica la cantidad de memoria que ha asignado el proceso en cuestión y que no puede compartirse con otros procesos.	Bytes

Tabla 2:11 Parámetros de evaluación de los procesos [24]

2.1.6. Servidor

[24] Elaborado por: La Autora

A más de los parámetros descritos anteriormente se puede realizar también una medición de los parámetros del Recurso Servidor que miden la comunicación entre el equipo local y la red; entre estos tenemos:

Parámetro	Descripción	Unidad de medida
Inicios de sesión por segundo	Mide la frecuencia de inicios de sesión en todos los servidores	Porcentaje
Errores de permiso de acceso	Indica el número de veces que ha fracasado alguna operación de apertura para algún cliente	Número de errores
Errores de acceso concedido	Indica el número de veces que se ha denegado el acceso a archivos abiertos correctamente.	Número de errores
Sesiones cerradas debido a un error	Mide el número de sesiones que se han cerrado debido a condiciones de error imprevistas.	Número de sesiones

Tabla 2:12 Parámetros de evaluación de servidor [25]

2.2. VALORES UMBRALES

[25] Elaborado por: La Autora

Fuente: Texto explicativo de Microsoft Management Console, Windows 2003 Server

Los parámetros descritos anteriormente tienen un valor límite determinado, con los cuales el sistema trabaja sin problemas pero si alguno de ellos no es el determinado ocasionará cuellos de botella que pueden afectar al rendimiento del sistema. En esta sección se establecen los valores umbrales para cada uno de los parámetros.

Cabe mencionar que dependiendo de la función del servidor existen valores umbrales, por ejemplo, si es un servidor Web debe cumplir con ciertos valores umbrales establecidos, de igual manera si es un servidor de base de datos, servidor de impresión, y así con todos los demás servidores existentes.

Área	**Parámetro**	**Valor Umbral**
Disco lógico	Espacio libre	Mayor que 15%
Disco físico	Tiempo inactivo	Mayor de 20%
Disco físico	Tiempo de lectura de disco	Menor de 25 ms
Disco físico	Tiempo de escritura de disco	Menor a 25 ms
Disco físico	Longitud promedio de la cola de disco	Menor al número de ejes + 2
Disco - Memoria	Bytes de caché	Menor a 200 MB
Memoria física	Bytes confirmados en uso	Menor al 80%
Memoria física	MB disponibles	Mayor al 5% de la memoria RAM física total
Memoria lógica	Entradas libres de la tabla de páginas del sistema	Mayor a 5000
Memoria lógica	Bytes de bloque no paginado	Menor a 175 MB
Memoria lógica	Bytes de bloque paginado	Menor a 250 MB

Memoria lógica	Páginas por segundo	Menor a 5 (deseado) Mayor a 10 (cuello de botella) Mayor o igual a 20 (sistema degradado)
Procesador	Tiempo de procesador	Menor al 85%
Procesador	Tiempo de usuario	Mayor al 75%
Procesador	Tiempo de interrupción	Menor al 15%
Procesador - Sistema	Longitud de la cola del procesador	2 veces del número de unidades CPU
Red	Total de bytes por segundo	Menor al 70% de la interfaz
Red	Longitud de la cola de salida	Menor a 2
Proceso	Recuento de identificadores	10000
Proceso	Número de subprocesos	500
Proceso	Bytes privados	250
Servidor	Inicios de sesión por segundo	Menor al 1% de los reingresos
Servidor	Errores de permiso de acceso	0
Servidor	Errores de acceso concedido	0
Servidor	Sesiones cerradas debido a un error	Menor al 1% de las sesiones activas

Tabla 2:13 Valores Umbrales [26]

Como se puede ver en la tabla, existen algunos parámetros útiles para analizar el rendimiento de un servidor, no obstante existen herramientas que permiten crear conjuntos de parámetros acordes a las necesidades específicas del usuario; una de ellas es la herramienta Monitor del Sistema propia del sistema operativo Windows, que permite crear plantillas con los contadores preferidos del usuario para usarlos en futuras ocasiones; lo que ayuda a ahorrar tiempo cada vez que se desea supervisar los servidores.

2.3. HERRAMIENTAS DE EVALUACIÓN

Como se explicó en el capítulo I, existen muchas herramientas que ayudan a estudiar el funcionamiento de un servidor ya que disponen de contadores útiles para medir el rendimiento del mismo. No todos los parámetros pueden ser analizados con las herramientas planteadas ya que tienen enfoques diferentes; pero fueron seleccionadas porque a más de detectar cuellos de botella tienen otras cualidades que las hacen útiles al momento de realizar la evaluación del rendimiento.

Por otro lado, el éxito de la evaluación no solo depende de la acertada selección de la herramienta sino que además depende de la adecuada configuración de la misma y el correcto establecimiento de los períodos de medición; de tal forma que los datos generados provean de la información necesaria que revelen el verdadero estado de servidor.

[26] Elaborado por: La Autora

A continuación se asocian los parámetros de evaluación a las herramientas descritas en el capítulo 1 de acuerdo a las áreas principales de evaluación que son: disco duro, memoria, CPU, proceso, red y servidor.

Área	Contador	Monitor del Sistema	PRTG Network	Task Manager	Advance Host	Server Assist	Speed Test	GFI Network	PC Mark	Visual Control	Op Manager
Disco lógico	Espacio libre	Si	Si	No	Si	Si	Si	Si	Si	Si	Si
Disco físico	Tiempo inactivo	Si	No	No	Si	Si	No	Si	Si	Si	No
Disco físico	Tiempo de lectura de disco	Si	Si	No	No	Si	Si	Si	No	Si	Si
Disco físico	Tiempo de escritura en disco	Si	Si	No	No	Si	Si	Si	No	Si	Si
Disco físico	Longitud promedio de la cola de disco	Si	Si	No	Si	Si	No	Si	No	Si	Si

Disco Memoria	Bytes de caché	Si	No	Si	No	Si	No	Si	No	No	No
Memoria física	Bytes confirmados (asignados) en uso	Si	No	No	Si	Si	No	Si	Si	Si	No
Memoria física	Bytes disponibles	Si	No	Si	Si	Si	Si	Si	Si	Si	Si
Memoria lógica	Entradas libres de la tabla de páginas del sistema	Si	No	No	No	Si	No	Si	No	No	No
Memoria lógica	Bytes de bloque no paginado	Si	Si	Si	No	Si	No	Si	No	No	No

Memoria lógica	Bytes de bloque paginado	Si	No	Si	No	Si	No	Si	No	No	No
Memoria lógica	Páginas por segundo	Si	Si	No	No	Si	No	Si	Si	Si	Si
Procesador	Tiempo de procesador	Si	Si	Si	Si	Si	No	Si	Si	Si	Si
Procesador	Tiempo de usuario	Si	Si	No	Si	Si	No	Si	No	Si	No
Procesador	Tiempo de interrupción	Si		No	Si	Si	No	Si	No	No	No
Procesador - Sistema	Longitud de la cola del procesador	Si	Si	No	Si	Si	No	Si	No	Si	Si

Red	Total de bytes por segundo	Si	Si	No	No	Si	No	Si	Si	No	No
Red	Longitud de la cola de salida	Si	No	No	No	Si	No	Si	No	No	No
Proceso	Recuento de identificadores	Si	No	Si	Si	Si	No	No	No	No	No
Proceso	Número de subprocesos	Si	No	Si	No	Si	No	Si	No	No	No
Proceso	Bytes privados	Si	No	No	No	Si	No	Si	No	No	No

Tabla 2:14 Herramientas de evaluación y sus contadores [27]

[27] Elaborado por: La Autora

CAPÍTULO 3

3. COMPONENTES Y POLÍTICAS DE SEGURIDAD

En la actualidad el principal activo de una organización es la información ya que tiene una importancia fundamental para el funcionamiento de la misma llegando incluso a ser decisiva para su continuidad; es por eso que se busca la forma de gestionar y proteger la información, su aseguramiento y el aseguramiento de los sistemas que la procesan, es por tanto un objetivo de primer nivel para la organización.

Como se manifiesta en los marcos de trabajo utilizados en la actualidad y que son mencionados en el presente capítulo en lo que a la seguridad de la información se refiere, todo empieza por un compromiso desde los altos niveles de la organización hacia los demás miembros de la misma, para que el objetivo de proteger la información se cumpla.

Entre los marcos de referencia como: COBIT, ITIL, OCTAVE; o estándares como las normas ISO/IEC 27001, 27002, que ayudan a gestionar la seguridad de la información existe un punto en común, y es que utilizan el ciclo PDCA[28] como estrategia de mejora continua para sus procesos.

---

[28] PDCA [Plan, Do, Check, Act]

Fuente: http://es.wikipedia.org/wiki/PDCA

En el presente capítulo se establecerán los componentes de seguridad, políticas, gestión de riesgos e incidentes según las normas y estándares mencionados; lo que será de mucha ayuda al momento de realizar la evaluación de las seguridades por parte del equipo de TI.

COBIT

"COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de TI. "[29]

En los siguientes dominios de COBIT se analizan aspectos tanto de la administración de la seguridad, como de la gestión de riesgos e incidentes:

---

[29] COBIT [Control Objectives for Information and related Technology]

Fuente: CobiT4_Espanol.pdf; IT Governance Institute; Pág. 9

Dominio	Proceso
Planear y Organizar	PO9 – Evaluar y administrar riesgos de TI
Entregar y Dar Soporte	DS5 – Garantizar la seguridad de los sistemas DS8 – Administrar la mesa de servicio y los incidentes

OCTAVE

El método OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), se basa en un conjunto de criterios que definen los elementos esenciales para una integral evaluación de los riesgos de seguridad de una organización. Requiere de un equipo interdisciplinario formado tanto por gente de la organización como del departamento de TI con diversas habilidades y experiencias ya que es un método complejo. Mediante este método se evalúan las amenazas y vulnerabilidades de los recursos tecnológicos y operacionales importantes de la organización.[30]

ITIL

Information Technology Infrastructure Library, es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de TI, incluyen opciones que

[30] OCTAVE [Operationally Critical Threat, Asset, and Vulnerability Evaluation]

Fuente: OCTAVE Method Implementation Guide Versión 2.0 Volumen 1; Pág. I.1

pueden ser adoptadas y adaptadas según las necesidades, circunstancias y experiencia del proveedor del servicio.

LIBRO	Proceso
Soporte a Servicios	- Función Service Desk - Administración de incidentes
Gestión de la seguridad	- Administración de la seguridad

NORMAS ISO/IEC 27001 y 27002

Proporcionan un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI31. La implantación del SGSI es una decisión estratégica para la organización y se ve afectado por sus necesidades, objetivos, requerimientos de seguridad, procesos empleados, tamaño y estructura de la misma.

NORMA ISO	COMPONENTE
27001	Implantación de un SGSI
27002	Código de buenas prácticas
27005	Gestión de riesgos

[31] SGSI [Sistema de Gestión de Seguridad de la Información]

Fuente: Estándar Internacional ISO/IEC 27002-2005, primera edición, 2005

En la Figura 1 se establecen los procesos comunes de COBIT, ITIL, OCTAVE y las Normas 27000 en lo que al tratamiento de la seguridad de la información se refiere:

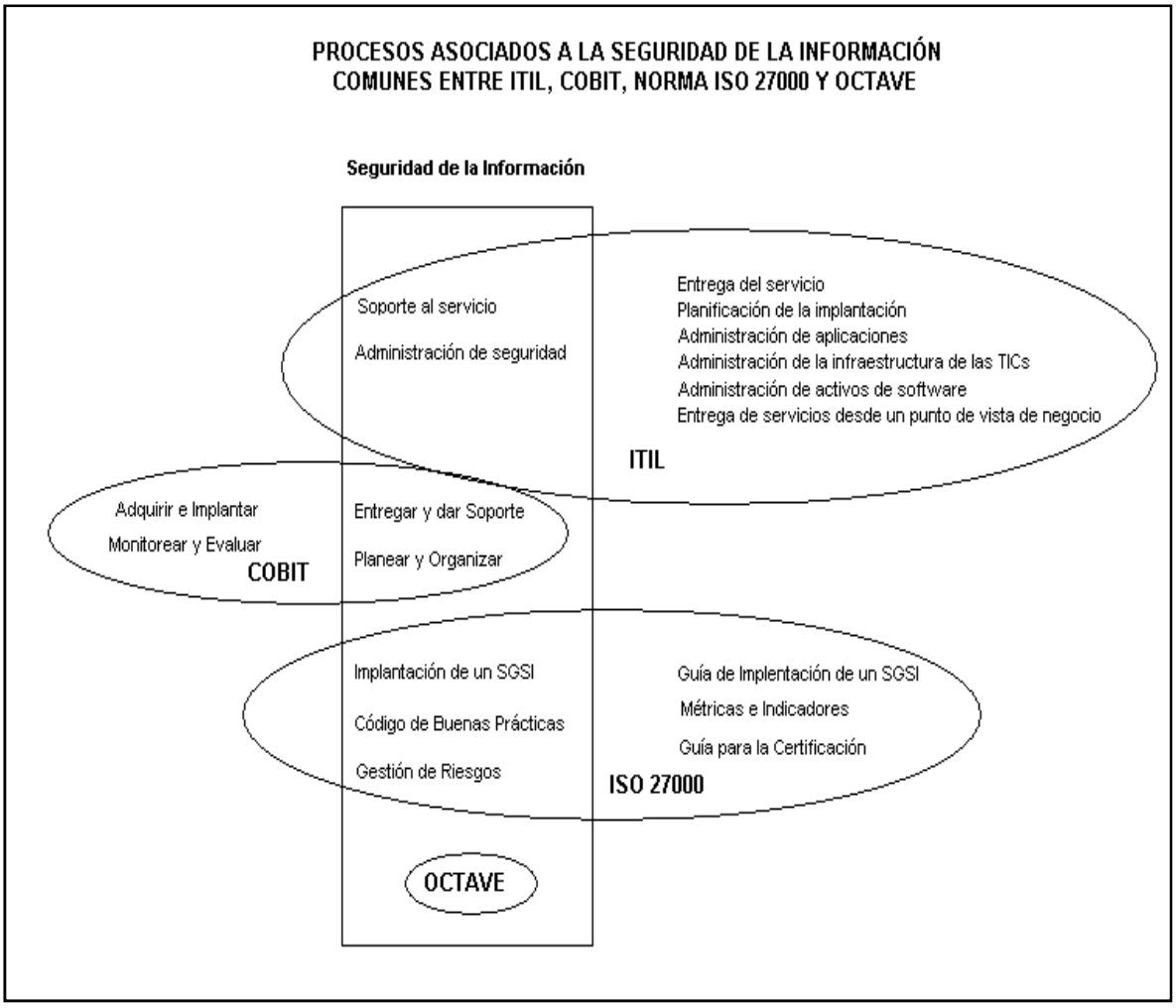


Figura 3:1 PROCESOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN [32]

3.1. POLÍTICAS INTERNAS Y EXTERNAS A LA RED

3.1.1. Visión General

[32] Elaborado por: La Autora

Las decisiones en cuanto a medidas de seguridad de un sitio determinan, que tan segura será la red y, además, qué nivel de funcionalidad ofrecerá y qué tan fácil será de usar.

Estas decisiones deben ser antecedidas por la determinación de los objetivos de seguridad, que permitirán resolver la selección de las herramientas que harán efectivos tales objetivos. Estos objetivos serán diferentes para cada organización porque dependen de sus necesidades. Están muy relacionados con algunos puntos de equilibrio claves tales como:

- Servicios ofrecidos vs. La seguridad provista: cada servicio ofrecido a un cliente tiene su propio riesgo de seguridad.

- Facilidad de uso vs. Seguridad: Un sistema muy fácil de usar permitirá el acceso a casi todos los clientes y por lo tanto será menos seguro.

- Costo de la seguridad vs. Riesgo de pérdida: existen muchos costos de seguridad: monetarios, de desempeño y facilidad de uso. Los riesgos de pérdida pueden ser de privacidad, de datos, y servicios. Cada tipo de costo debe ser balanceado con respecto a cada tipo de perdida.

Una vez definidos los objetivos, deben ser comunicados a todos los clientes de la red de la organización e implementados a través de un conjunto de reglas de seguridad llamadas política de seguridad.

"Una política de seguridad es un enunciado formal de las reglas que los clientes que acceden a los recursos de la red de una organización deben cumplir." [33]

Una política de seguridad debe asegurar cuatro aspectos fundamentales en una solución de seguridad: autenticación, control de acceso, integridad y confidencialidad. A partir de estos, surgen los principales componentes de una política de seguridad:

- Una política de privacidad: define expectativas de privacidad con respecto a funciones como monitoreo, registro de actividades y acceso a recursos de la red.

- Una política de acceso: que permite definir derechos de acceso y privilegios para proteger los objetivos clave de una perdida o exposición mediante la especificación de guías de uso aceptables para los clientes con respecto a conexiones externas, comunicación de datos, conexión de dispositivos a la red, incorporación de nuevo software a la red, etc.

- Una política de autenticación: que establece un servicio de confiabilidad mediante alguna política de contraseñas o mecanismos de firmas digitales, estableciendo guías para la autenticación remota y el uso de dispositivos de autenticación.

- Un sistema de TI y una política de administración de la red: describe como pueden manipular las tecnologías los encargados de la administración interna y externa. De aquí surge la consideración de si la administración externa será soportada y, en tal caso, como será controlada.

[33] Fuente: Estándar Internacional ISO/IEC 27002-2005, primera edición, 2005

Al diseñar la política de seguridad de una red se deben responder algunas cuestiones claves para poder llevar a cabo una sólida definición. Las preguntas básicas sobre la cual desarrollar la política de seguridad son las siguientes:

- ¿Que recursos se tratan de proteger? (objetivos clave)
- ¿De quién se trata de proteger los recursos?
- ¿Cuáles y cómo son las amenazas que afectan a tales recursos?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas pueden ser implementadas para proteger el recurso?
- ¿Cuál es el costo de tal medida y en qué tiempo puede ser implementada?
- ¿Quién autoriza a los clientes? [34]

3.1.2. Fundamentos de las Políticas de Seguridad Internas y Externas a la Red

Las políticas internas y externas a la red deben proteger todos los elementos tanto de la red interna como de la red externa, dichas políticas de seguridad están englobadas en 2 tipos:

- Todo está prohibido a menos que se permita explícitamente.
- Todo está permitido a menos que se prohíba explícitamente.

En ocasiones se utilizan combinaciones de éstas, para diferentes partes del sistema, tomando en cuenta las siguientes estrategias de seguridad:

---

[34] Fuente: http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad

- Mínimos privilegios: Consiste en asignar a cada cliente el mínimo de privilegios que necesite. El objetivo es minimizar los daños en caso de que la cuenta de un cliente sea invadida. En caso de que un cliente quiera realizar actividades diferentes tiene que solicitar que se le asignen los privilegios correspondientes.

- Defensa en profundidad: Consiste en usar tantos mecanismos de seguridad como sea posible, colocándolos uno tras otro. Puede hacer muy compleja la utilización del sistema.

- Check Point: Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto. Puede disminuir el rendimiento.

- Falla en posición segura: Los sistemas deben estar diseñados para que en caso de falla queden en un estado seguro. Por ejemplo en redes, en caso de falla se debe suspender el acceso a Internet.

- Seguridad por Oscuridad: La estrategia es mantener un bajo perfil y tratar de pasar desapercibido, de modo que los atacantes no lo detecten.

- Simplicidad: Los sistemas muy complejos tienden a tener fallas y huecos de seguridad. La idea es mantener los sistemas tan simples como sea posible, eliminando funcionalidad innecesaria. Sistemas simples que tienen mucho tiempo, han sido tan depurados que prácticamente no tienen huecos de seguridad.

- Seguridad basada en hosts: Los mecanismos de seguridad están en los hosts. Puede ser diferente en cada host, lo cual hace difícil su instalación y mantenimiento. Si un host es atacado con éxito, peligra la seguridad de la red (muchos clientes tienen el mismo login y password en todos los hosts a los que tienen acceso).

- Seguridad basada en la red: La seguridad se basa en controlar los accesos a los hosts desde la red. El método más común es la implementación de firewalls.

3.2. COMPONENTES DE SEGURIDAD

Los componentes de seguridad que existen en un SI dependen de la actividad de la organización, y de la importancia que tengan; es decir, deben cumplir con los requerimientos de negocio y aunque resulte complejo precisar cuales son los componentes de seguridad de la información a continuación se establecen los que deberían ser tomados en cuenta para garantizar la seguridad de la información. Dichos componentes son mencionados en tanto en COBIT, ITIL como OCTAVE y en las normas ISO/IEC 27001 y 27002.

3.2.1. Gobierno de TI

Se adopta el término gobierno de TI utilizado en COBIT ya que describe de mejor manera los aspectos y elementos gerenciales que debe existir en la organización para garantizar la seguridad de la información. De aquí nace la estructura organizativa necesaria para gestionar la seguridad.

3.2.2. Política y Plan de Seguridad

Otro componente importante para gestionar adecuadamente la seguridad de la información es el establecimiento de una política acorde a los objetivos de la organización.

La implementación de una Política de Seguridad de la Información, permite a las organizaciones cumplir con una gestión efectiva de los recursos de información críticos e instalar y administrar los mecanismos de protección adecuados, determinando qué conductas son permitidas y cuáles no.

Esto causará una efectiva reducción de los niveles de riesgo y de las vulnerabilidades, lo cual, en definitiva, se traduce en ahorro de tiempo y dinero, genera mayor confianza y un fortalecimiento de la imagen de la organización.

La política no es más que el compromiso del gobierno de TI formalizado por medio de una Política Formalmente escrita, aprobada y comunicada.

Para mantener una visión clara e integral de las políticas de seguridad a definir, es útil establecer un Plan de Seguridad que ofrezca un marco de guías generales para tales políticas. De esta forma, las políticas individuales serán consistentes con toda la arquitectura de seguridad.

Un plan de seguridad debe definir entre otras cosas:

- La lista de servicios que serán ofrecidos por la red de la organización
- Qué áreas de la organización proveerán tales servicios
- Quién tendrá acceso a esos servicios
- Cómo será provisto el acceso
- Quién administrará esos servicios
- Cómo serán manejados los incidentes

Al igual que un plan de seguridad ofrece un marco de diseño para una política de seguridad, éstas se definen a diferentes niveles de especificación o abstracción lo que ofrece una visión más clara y coherente del esquema de seguridad.

3.2.3. Requerimientos de Seguridad

Se debe establecer los requerimientos de seguridad que satisfagan los objetivos del negocio buscando siempre proteger los atributos de la seguridad de la información como la integridad, disponibilidad y confidencialidad:

- Integridad: Propiedad de salvaguardar la exactitud e integridad de los activos.

- Disponibilidad: Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.

- Confidencialidad: Se refiere que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

3.2.4. Procesos y Procedimientos

Un importante componente para la gestión de la seguridad de la información es el establecimiento de un conjunto estructurado de actividades que deben ser realizadas para asegurar la información, ya que debido a su criticidad se hace necesario llevar a cabo la implantación de medidas de protección y el establecimiento de un sistema de gestión de seguridad de la información apoyándonos en procesos y procedimientos bien definidos.

3.2.5. Recursos

Denominados también activos que tienen mucho valor para la organización y que deben ser protegidos de las amenazas constantes a la que están expuestos, dichos recursos pueden ser críticos o no dependiendo de la actividad de la organización, de sus estrategias y objetivos.

En los marcos de trabajo utilizados en el presente proyecto de tesis mencionan a las personas, información, tecnología o infraestructura y aplicaciones, como los recursos que (gestionan o procesan información.

- Personas: Son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

- Información: Son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

- Infraestructura: Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

- Aplicaciones: las aplicaciones incluyen tanto sistemas de cliente automatizados como procedimientos manuales que procesan información. [35]

3.3. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

La evaluación del riesgo es el proceso de identificar, cuantificar y priorizar los riesgos en base a un criterio de aceptación del riesgo y los objetivos relevantes para la Organización. El resultado debe guiar y determinar las acciones y prioridades adecuadas para administrar los Riesgos de Seguridad y los Controles a implementar. ***[36]***

El proceso de evaluar el riesgo está inmerso dentro del enfoque de Análisis y Gestión de Riesgos ya que no es suficiente con identificarlos y evaluarlos; se

---

[35] Recursos de TI según COBIT

Fuente: CobiT4_Espanol.pdf; IT Governance Institute; Pág. 14

[36] Fuente: Estándar Internacional ISO/IEC 27001-2005, primera edición, 2005

necesita implementar los controles apropiados para reducir los riesgos encontrados y recomendados en el proceso de Evaluación del Riesgo.

Tomando como referencia la Norma ISO/IEC 27001 con respecto a la evaluación de riesgos de seguridad, se debería realizar las actividades siguientes para realizar dicha evaluación:

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

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

- Calcular los niveles de riesgo.

- Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecidos por el Gobierno de TI.

Con mayor o menor detalle, con diferencias terminológicas los principales marcos de referencia existentes presentan una estructura común para el Análisis y Administración de Riesgos de Seguridad, en la que se establece un nivel estratégico relacionado con la integración del gobierno de TI y el compromiso de llevar a cabo la gestión y análisis de riesgo; y un nivel táctico referente al proceso en sí de análisis y evaluación del riesgo.

En la figura 3:2 se presenta en resumen un enfoque gráfico del Proceso de Análisis y Evaluación del Riesgo:

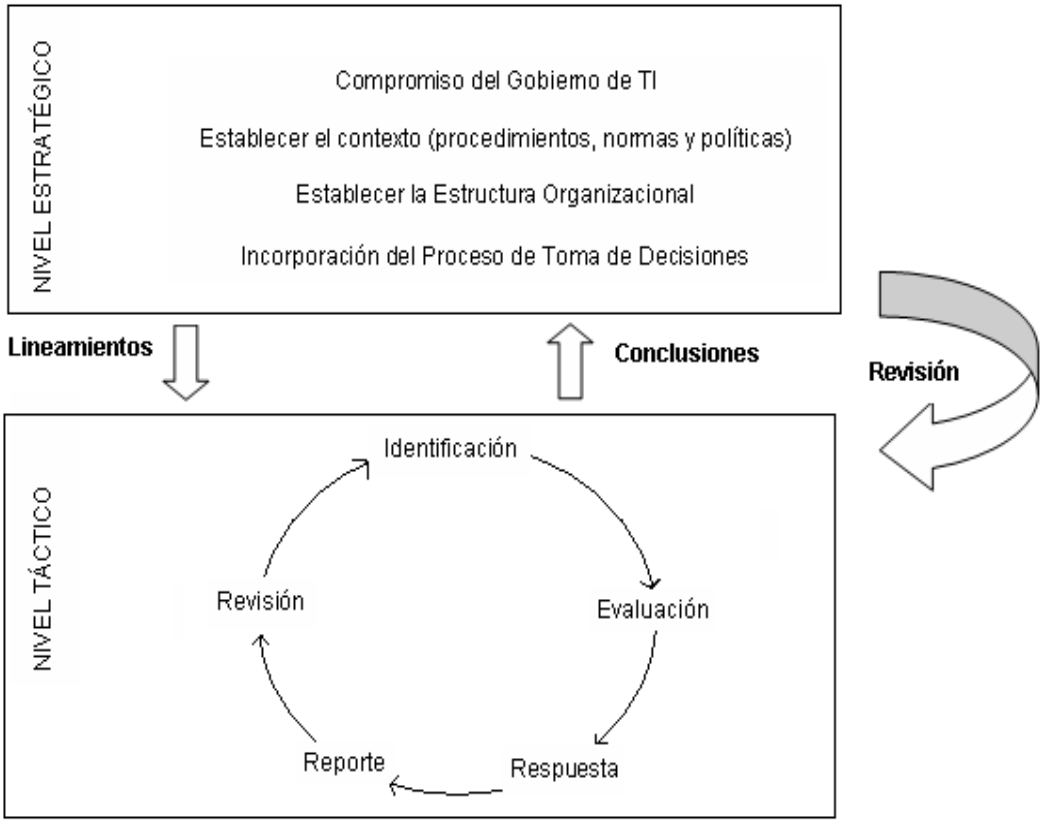


Figura 3:2 PROCESO DE ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD [37]

3.4. GESTIÓN DE INCIDENTES DE SEGURIDAD

ITIL es un marco referencial de mejores prácticas aplicadas en organizaciones a nivel mundial, por lo que se sugiere llevar a cabo la gestión de los incidentes de seguridad de acuerdo a los procesos y procedimientos que en esta se definen. Una

[37] Elaborado por: La Autora

de estas organizaciones es OSIATIS[38], grupo especializado en la ingeniería de servicios e integración de soluciones para las Infraestructuras Informáticas, que en su sitio Web presenta los fundamentos de ITIL para la Gestión de Servicios TI[39], a continuación se toma como referencia la Gestión de Incidentes[40] descrita en dicho sitio.

3.4.1. Introducción y Objetivos

Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA[41] correspondiente.

La Gestión de Incidentes requiere un estrecho contacto con los clientes, por lo que el Centro de Servicios (Service Desk) debe jugar un papel esencial. La Figura 3 resume el proceso de gestión de incidentes:

---

[38] Fuente: http://www.osiatis.es/

[39] Fuente:

http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/vision_general_gestion_servicios_TI/vision_general_gestion_servicios_TI.php

[40] Fuente:
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

[41] SLA [Service Level Agreement, Acuerdo de nivel de servicio]

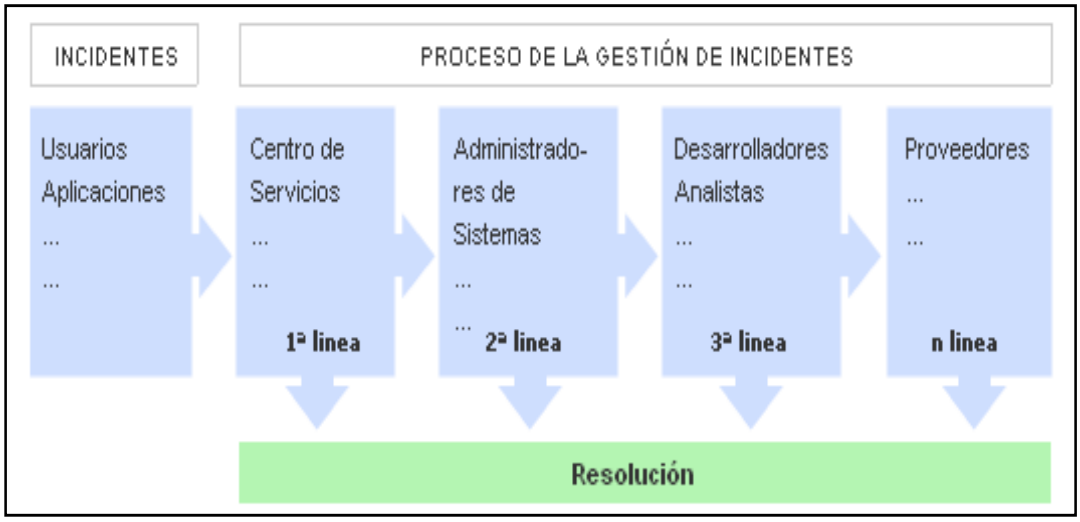


Figura 3:3 PROCESO DE LA GESTIÓN DE INCIDENTES [42]

Aunque el concepto de incidencia se asocia naturalmente con cualquier malfuncionamiento de los sistemas de hardware y software; según el libro de Soporte del Servicio de ITIL un incidente es:

"Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo".[13]

Por lo que casi cualquier llamada al Centro de Servicios puede clasificarse como un incidente, lo que incluye a las Peticiones de Servicio tales como concesión de nuevas licencias, cambio de información de acceso, etc. siempre que estos servicios se consideren estándar.

---

[42] Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introducción_objetivos_gestion_de_incidentes/introducción_objetivos_gestion_de_incidentes.php

Cualquier cambio que requiera una modificación de la infraestructura no se considera un servicio estándar y requiere el inicio de una Petición de Cambio que debe ser tratada según los principios de la Gestión de Cambios.

Entre los principales beneficios de llevar una correcta Gestión de Incidentes se tienen:

- Mejorar la productividad de los clientes.
- Cumplimiento de los niveles de servicio acordados en el SLA.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Una CMDB[43] más precisa, pues se registran los incidentes en relación con los elementos de configuración.
- Mejorar la satisfacción general de los clientes.

Por otro lado una incorrecta Gestión de Incidentes puede acarrear efectos adversos tales como:

- Reducción de los niveles de servicio.
- Se dilapidan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución del incidente.
- Se pierde valiosa información sobre las causas y efectos de los incidentes para futuras reestructuraciones y evoluciones.
- Se crean clientes insatisfechos por la mala y/o lenta gestión de sus incidentes.

[43] CMDB [Configuration Management Database, Base de datos de la gestión de configuraciones]

Las principales dificultades a la hora de implementar la Gestión de Incidentes se resumen en:

- No se siguen los procedimientos previstos y se resuelven las incidencias sin registrarlas o se escalan innecesariamente y/o omitiendo los protocolos preestablecidos.

- No existe un margen operativo que permita gestionar los “picos” de incidencias por lo que éstas no se registran adecuadamente e impiden la correcta operación de los protocolos de clasificación y escalado.

- No están bien definidos los niveles de calidad de servicio ni los productos soportados. Lo que puede provocar que se procesen peticiones que no se incluían en los servicios previamente acordados con el cliente.

3.4.2. Procesos implicados en la Gestión de Incidentes

El siguiente diagrama muestra los procesos implicados en la correcta Gestión de Incidentes:

Figura 3:4 PROCESOS RELACIONADOS CON LA GESTIÓN DE INCIDENTES [44]

- CMDB - Gestión de Configuraciones: La CMDB juega un papel clave en la resolución de incidentes pues, por ejemplo, nos muestra información sobre los responsables de los componentes de la configuración implicados. La CMDB también permite conocer todas las implicaciones que pueden tener en otros servicios el malfuncionamiento de un determinado CI (elemento de configuración). Por otro lado, al resolver el incidente se deberá actualizar la CMDB en caso de que haya sido necesario cambiar o modificar ciertos elementos de configuración.

- Gestión de problemas: ofrece ayuda a la gestión de incidentes informando sobre errores conocidos y posibles soluciones temporales. Por otro lado, establece controles sobre la calidad de la información registrada por la

[44] Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/proceso_gstion_de_incidentes/proceso_gestion_de_incidentes.php

Gestión de Incidentes para que esta sea de utilidad en la detección de problemas y su posible solución.

- Gestión de cambios: La resolución de un incidente puede generar una RFC (petición de cambio) que se envía a la gestión de cambios. Por otro lado, un determinado cambio erróneamente implementado puede ser el origen de múltiples incidencias y la Gestión de Cambios debe mantener cumplidamente informada a la Gestión de Incidencias sobre posibles incidencias que los cambios realizados pueden causar en el servicio.

- Gestión de Disponibilidad: Utilizará la información registrada sobre la duración, el impacto y el desarrollo temporal de los incidentes para elaborar informes sobre la disponibilidad real del sistema.

- Gestión de capacidad: se ocupara de incidentes causados por una insuficiente infraestructura TI (insuficiente ancho de banda, capacidad de proceso, etc.).

- Gestión de Niveles de Servicio: La gestión de incidentes debe tener acceso a los SLA acordados con el cliente para poder determinar el curso de las acciones a adoptar. Por otro lado, la Gestión de Incidentes debe proporcionar periódicamente informes sobre el cumplimiento de los SLAs contratados.

3.4.3. Proceso General

La Gestión de Incidentes, según ITIL, tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible. Este proceso no debe confundirse con la Gestión de Problemas, pues a

diferencia de esta última, no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas. A continuación se presenta el proceso de Gestión de Incidentes.

En ITIL la Gestión de Incidentes está relacionada por un lado con la función Service Desk ya que las dos requieren un estrecho contacto con los clientes; y por otro se relaciona con la Administración de Problemas ya que si el incidente se convierte en problema deberá ser tratado por este proceso.

La Administración de Incidentes trata con todos los incidente; esto puede incluir fallas, preguntas o necesidades reportadas por los clientes (usualmente por teléfono a través del Service Desk), a través del equipo técnico, o detectado automáticamente por alguna herramienta de monitoreo de eventos. Las actividades o subprocesos de la Gestión de Incidentes son:

- Monitoreo, seguimiento y comunicación del manejo de incidentes.
- Detección y registro de incidentes
- Clasificación y soporte inicial del incidente
- Investigación y diagnóstico del incidente
- Cierre del incidente

En la Figura 5 se presenta un esquema de funcionamiento del proceso de Gestión de Incidentes propuesta por ITIL:

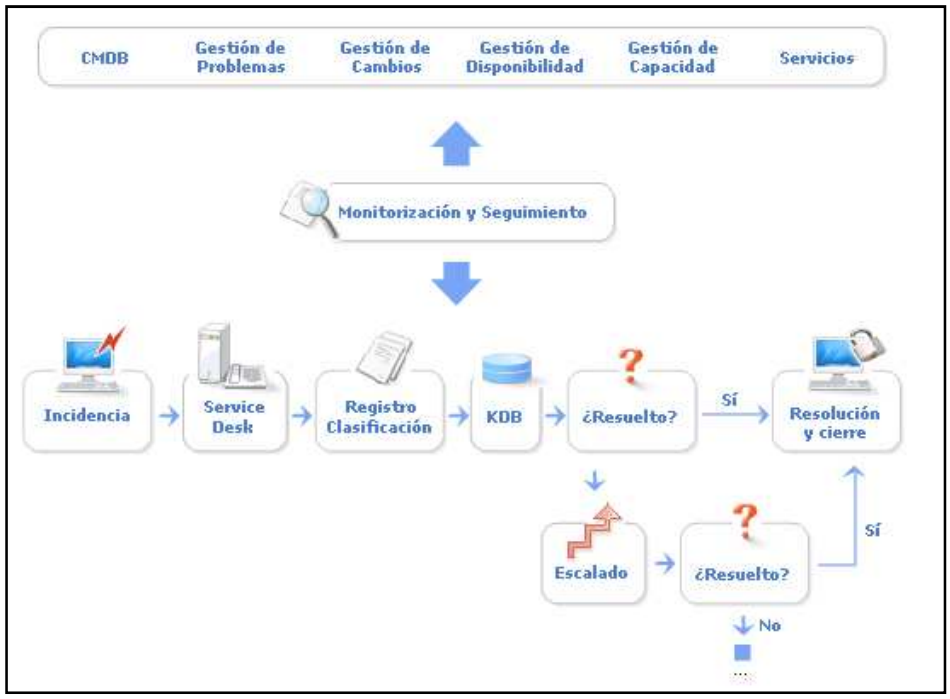


Figura 3:5 PROPIEDADES Y FUNCIONALIDADES DE LA GESTIÓN DE INCIDENTES [45]

A continuación se describen con mayor detalle la secuencia sugerida por ITIL para realizar una adecuada Gestión de Incidentes:

- Monitorización y Seguimiento: Todo el proceso debe ser controlado mediante la:

  - Emisión de informes

[45] Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

- Actualización de las bases de datos asociadas
- Monitorización de los niveles de servicio

- Incidencia: Una incidencia es una Interrupción de los servicios TI o petición de un servicio que es:

  - Comunicada por el cliente
  - Generada automáticamente por aplicaciones

- Service Desk: Este proceso es el responsable directo de la gestión de las incidencias, es:

  - Centro de contacto de la organización TI
  - Primera línea de soporte

- Registro y Clasificación: Se crea un registro de incidente acorde a la prioridad y categorización:

  - Prioridad = Impacto * Urgencia
  - Categorización: Asignación de tipo y personal de soporte

- KDB: Se encarga del Análisis y diagnóstico

  - Consulta BDD de conocimiento.
  - Evalúa si ha una solución preestablecida

Una vez que se realiza el análisis y diagnóstico se evalúa si es que se conoce el método de solución, si es así, se asignan los recursos necesarios. Si no se conoce el método de solución, se escala la incidencia a un nivel superior de soporte

- Escalado: Existen dos tipos de escalado en el proceso de resolución de una incidencia:

  - Escalado funcional: se recurre a técnicos de nivel superior.
  - Escalado jerárquico: entran en juego los más altos responsables de la organización TI.

- Resolución y Cierre: Cuando se ha resuelto el incidente satisfactoriamente:

  - Registro del proceso en el sistema y, si es de aplicación, en la BDD de conocimiento.
  - Si fuera necesario, generar una RFC[46] a la gestión de cambios.

- Interrelaciones: Debe existir una estrecha relación entre la Gestión de Incidentes y otros procesos TI con el objetivo de:

  - Mejorar el servicio y cumplir adecuadamente los SLAs
  - Conocer la capacidad y disponibilidad de la infraestructura TI
  - Planificar y realizar los cambios necesarios para la optimización y desarrollo del servicio TI.

[46] RFC [Request For Change, Petición de Cambio]

- Registro y Clasificación de Incidentes
  - Registro

La admisión y registro del incidente es el primer y necesario paso para una correcta gestión del mismo. Las incidencias pueden provenir de diversas fuentes tales como clientes, gestión de aplicaciones, el mismo Centro de Servicios o el soporte técnico, entre otros.

El proceso de registro debe realizarse inmediatamente pues, resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

- La admisión a trámite del incidente: el Centro de Servicios debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el SLA del cliente y en caso contrario reenviarlo a una autoridad competente.
- Comprobación de que ese incidente aún no ha sido registrado: es común que más de un cliente notifique la misma incidencia y por lo tanto han de evitarse duplicaciones innecesarias.
- Asignación de referencia: al incidente se le asignará una referencia que le identificará unívocamente tanto en los procesos internos como en las comunicaciones con el cliente.
- Registro inicial: se han de introducir en la base de datos asociada la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados, etc.).
- Información de apoyo: se incluirá cualquier información relevante para la resolución del incidente que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia CMDB (hardware interrelacionado, etc.).

- Notificación del incidente: en los casos en que el incidente pueda afectar a otros clientes estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.

- Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo. El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- Categorización: se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.
- Establecimiento del nivel de prioridad: dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de prioridad.
- Asignación de recursos: si el Centro de Servicios no puede resolver el incidente en primera instancia designara al personal de soporte técnico responsable de su resolución (segundo nivel).
- Monitorización del estado y tiempo de respuesta esperado: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.

En la clasificación del incidente es común que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basa esencialmente en dos parámetros:

- Impacto: determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de clientes afectados.
- Urgencia: depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el SLA.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes. Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. La figura siguiente muestra un posible Diagrama de Prioridades en función de la urgencia e impacto del incidente:

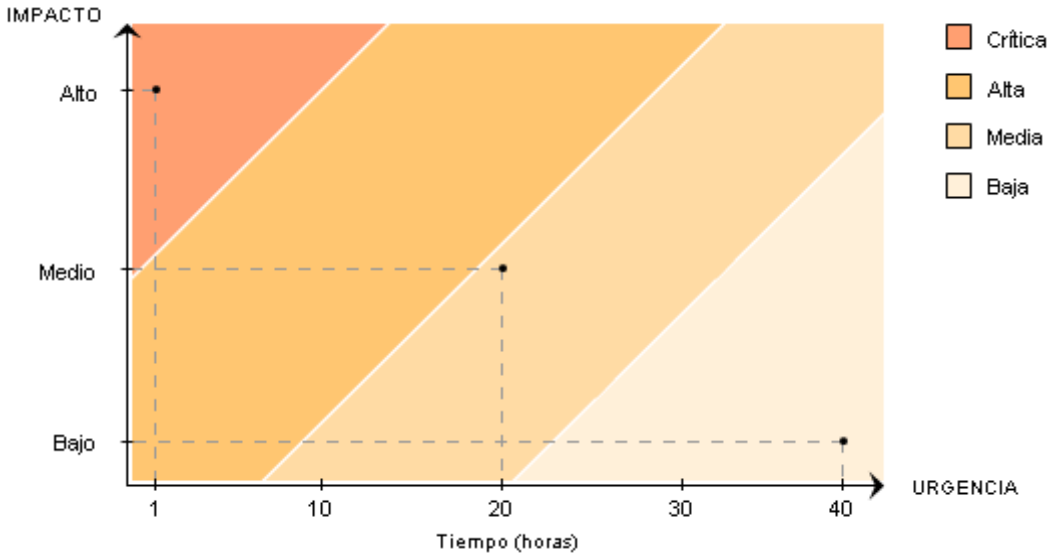


Figura 3:6 DIAGRAMA DE PRIORIDADES [47]

- Escalado y Soporte

Es frecuente que el Centro de Servicios no se vea capaz de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado. Básicamente hay dos tipos diferentes de escalado:

- Escalado funcional: Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.

[47] Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/clasificacion_y_registro_de_incidentes.php

- Escalado jerárquico: Se debe acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.

El proceso de escalado puede resumirse gráficamente como sigue:

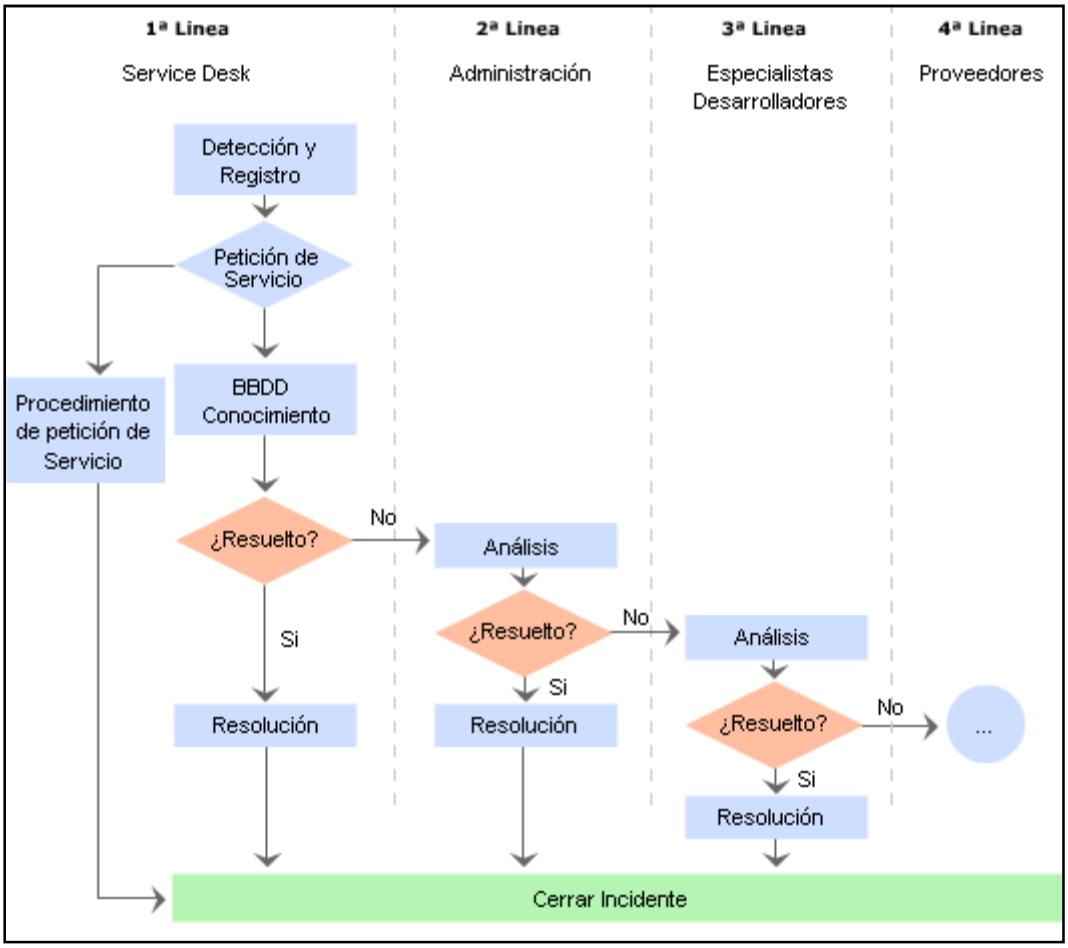


Figura 3:7 ESCALADO DE UN INCIDENTE [48]

[48] Fuente: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/escalado_de_incidentes.php

El escalado puede incluir más niveles en grandes organizaciones, o por el contrario, integrar diferentes niveles en el caso de PYMES (Pequeñas y Mediana Empresas).

- Análisis, Resolución y Cierre de Incidentes

En primera instancia se examina el incidente con ayuda de la KB[49] para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

Si la resolución del incidente se escapa de las posibilidades del Centro de Servicios éste redirecciona el mismo a un nivel superior para su investigación por los expertos asignados. Si estos expertos no son capaces de resolver el incidente se seguirán los protocolos de escalado predeterminados.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo.

En caso de ser necesario se puede emitir una Petición de Cambio. Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la Gestión de Problemas para el estudio detallado de las causas subyacentes. Cuando se haya solucionado el incidente se:

- Confirma con los clientes la solución satisfactoria del mismo.

[49] KB: Knowledge Base: Base de conocimiento

- Incorpora el proceso de resolución a la KB.
- Reclasifica el incidente si fuera necesario.
- Actualiza la información en la CMDB sobre los CI[50] implicados en el incidente.
- Cierra el incidente.

- Control del Proceso

La correcta elaboración de informes forma parte esencial en el proceso de Gestión de Incidentes. Estos informes deben aportar información esencial para, por ejemplo:

- La Gestión de Niveles de Servicio: es esencial que los clientes dispongan de información puntual sobre los niveles de cumplimiento de los SLAs y que se adopten medidas correctivas en caso de incumplimiento.
- Monitorizar el rendimiento del Centro de Servicios: conocer el grado de satisfacción del cliente por el servicio prestado y supervisar el correcto funcionamiento de la primera línea de soporte y atención al cliente.
- Optimizar la asignación de recursos: los gestores deben conocer si el proceso de escalado ha sido fiel a los protocolos preestablecidos y si se han evitado duplicidades en el proceso de gestión.

[50] CI [Configuration Item, Elemento de configuración]

- Identificar errores: puede ocurrir que los protocolos especificados no se adecuen a la estructura de la organización o las necesidades del cliente por lo que se deban tomar medidas correctivas.
- Disponer de Información Estadística: que puede ser utilizada para hacer proyecciones futuras sobre asignación de recursos, costes asociados al servicio, etc.

Por otro lado una correcta Gestión de Incidentes requiere de una infraestructura que facilite su correcta implementación. Entre ellos cabe destacar:

- Un correcto sistema automatizado de registro de incidentes y relación con los clientes.
- Una Base de Conocimiento que permita comparar nuevos incidentes con incidentes ya registrados y resueltos. Una KB actualizada permite:
    - Evitar escalados innecesarios.
    - Convertir el conocimiento de los técnicos en un activo duradero de la empresa.
    - Poner directamente a disposición del cliente parte o la totalidad de estos datos (a la manera de FAQs[51]) en una Extranet. Lo que puede permitir que a veces el cliente no necesite siquiera notificar la incidencia.

[51] FAQs [Frequently Asked Questions, Preguntas frecuentes]

- Una CMDB que permita conocer todas las configuraciones actuales y el impacto que estas puedan tener en la resolución del incidente.

Para el correcto seguimiento de todo el proceso es indispensable la utilización de métricas que permitan evaluar de la forma más objetiva posible el funcionamiento del servicio. Algunos de los aspectos clave a considerar son:

- Número de incidentes clasificados temporalmente y por prioridades.
- Tiempos de resolución clasificados en función del impacto y la urgencia de los incidentes.
- Nivel de cumplimiento del SLA.
- Costos asociados.
- Uso de los recursos disponibles en el Centro de Servicios.
- Porcentaje de incidentes, clasificados por prioridades, resueltos en primera instancia por el Centro de Servicios.
- Grado de satisfacción del cliente.

CAPÍTULO 4

4. FORMULACIÓN DEL PROCEDIMIENTO

4.1. CONSIDERACIONES PARA EL USO DEL PROCEDIMIENTO

4.1.1. Alcance y Objetivos del procedimiento

4.1.1.1. Alcance

El procedimiento pretende brindar un soporte al evaluador ya que cubrirá los aspectos de evaluación tanto del rendimiento como de las seguridades de un servidor Windows considerados los más relevante según el criterio de las mejores prácticas utilizadas en la actualidad y mediante el uso de herramientas destinadas para ello. El procedimiento es aplicable en organizaciones medianas y pequeñas.

En este procedimiento se muestran tablas de ayuda que servirán de guía para el evaluador; con lo que se conseguirá analizar de mejor manera los datos obtenidos en la evaluación.

Se establecen además, las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los sistemas operativos en base a las mejores prácticas y marcos de trabajo analizados en el Capítulo 3, en cuanto a la seguridad de la información se refiere.

El procedimiento no abarcará el desarrollo de todas las actividades que se pueden llevar a cabo dentro de un trabajo de evaluación de las seguridades y el rendimiento de servidores mediante la aplicación de Auditorias Informáticas.

4.1.1.2. Objetivos

El principal objetivo es el de formalizar un documento con criterios claros que permitan al Ingeniero en Sistemas evaluar las seguridades y el rendimiento de servidores Windows.

El procedimiento busca además facilitar la tarea de evaluación y protección de los servidores mediante el establecimiento de un conjunto de pasos sencillos y adecuados que permitan disminuir el tiempo en la aplicación de procesos que corresponden a un trabajo de Evaluación del Rendimiento y las Seguridades.

El evaluador encontrará el soporte necesario para poder identificar posibles problemas presentes en el servidor o en su entorno apoyándose en las herramientas para monitorización de sistemas mencionadas en capítulos anteriores.

El procedimiento permitirá determinar la efectividad y cumplimiento de los procesos informáticos dictados en las metodologías y marcos de trabajo analizados en el capítulo 3.

4.1.2. Destinatarios del procedimiento

Este procedimiento ha sido diseñado principalmente para profesionales de TI que sean responsables de la administración de servidores Windows o que tengan a su cargo planear el desarrollo y la implementación de aplicaciones o infraestructuras en cuanto al tema de seguridad y rendimiento de sistemas se refiere. Otras personas que podrían encontrar útil el presente procedimiento son:

- Estudiantes Informáticos: A quienes este procedimiento les servirá como un documento de consulta en donde pueden encontrar algún tipo de información sobre este tema, lo que permitirá ampliar sus conocimientos sobre la materia Auditoria y Evaluación de Sistemas.

- Responsables en la toma de decisiones empresariales: Quienes son los encargados de gestionar los procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización.

- Auditores informáticos: A quienes el procedimiento les permitirá incluir en sus procesos de Auditoría nuevos conocimientos con relación a los marcos de trabajo y mejores prácticas utilizadas actualmente para la realización de Auditorias Informáticas.

4.1.3. Factores claves para el éxito del procedimiento

Existen algunos factores que permiten lograr una implementación satisfactoria del procedimiento de evaluación del rendimiento y las seguridades de servidores Windows en una organización y son:

- Patrocinio ejecutivo ya que sin su apoyo y compromiso no se puede llevar a cabo la evaluación. Cuando este tipo de tareas se lleva a cabo desde la cúpula de la organización se pueden articular la seguridad en términos de valor para la misma.

- Lista bien definida de los participantes en la tarea de evaluación tanto de las seguridades como del rendimiento de los servidores. Una definición clara de funciones y responsabilidades resulta fundamental para el éxito del procedimiento.

- Ambiente de comunicaciones abiertas.

- Espíritu de trabajo en equipo.

- Visión holística de la organización.

- Autoridad de equipo para realizar la evaluación.

4.2. ELABORACIÓN DEL PROCEDIMIENTO

4.2.1. Aspectos Generales

Para la elaboración del procedimiento se tomaron como criterios los parámetros y herramientas de evaluación aplicados a un servidor Windows analizados en el capítulo 1 y 2 del presente proyecto de tesis; y los estándares internacionales como COBIT, ITIL y Normas ISO/IEC 27001 y 27002, como marcos referenciales para la evaluar las seguridades de los sistemas Windows. Así como también la información expuesta en sitio Web oficial de Microsoft.

Otro aspecto importante para realizar la evaluación es determinar los elementos que se quieren proteger de un servidor, ya que la función es la de proveer servicios de forma eficiente y eso se consigue evaluando constantemente los recursos del sistema mediante una adecuada selección de los principales parámetros que permiten medir su rendimiento.

A continuación se exponen algunas tablas que permite analizar los diferentes roles de los servidores estableciendo sus fortalezas y debilidades así como las características comunes entre cada uno de ellos.

Al establecer el rol y las características del servidor se podrá saber qué elementos de este se deben evaluar; las fortalezas permitirán conocer los elementos que se deben proteger y asegurar con mayor énfasis. Por otro lado, las debilidades dirán en donde se debe aplicar más controles tanto de las seguridades como para el mejoramiento del rendimiento del servidor.

SERVIDOR DE BASE DE DATOS	
Rol	Coordinar los programas, procedimientos, lenguajes, etc.; que suministran a los clientes, los medios necesarios para almacenar, manipular y recuperar los datos almacenados en la base de datos manteniendo integridad, confidencialidad y seguridad.
Características	▪ Controla el lugar de almacenamiento de la información. ▪ Reduce el tiempo de acceso del cliente a la base de datos. ▪ Provee seguridad de la información. ▪ Realiza tareas tales como: respaldo, recuperación, revisión de espacio ocupado, entre otras.

Fortalezas	▪ Es el soporte que necesitan las aplicaciones Web para almacenar o recuperar información de forma rápida y eficaz.
Debilidades	▪ Requiere de un adecuado nivel de seguridad ya que es la información de la organización la que está expuesta a constantes amenazas.
Área de Evaluación Clave	Disco Duro Procesador Memoria Servidor

Tabla 4:15 Servidor de Base de Datos [52]

SERVIDOR DE WEB	
Rol	Se encarga de contestar las peticiones de ejecución que le hará un cliente; de forma adecuada, entregando como resultado una página Web o información de todo tipo de acuerdo a los comandos solicitados.
Características	▪ Permite publicar un sitio Web sin necesitad de contratar hosting. ▪ Permite acceder remotamente a archivos de un equipo específico. ▪ Mediante los virtual hosts permite almacenar varios sitios Web en el mismo sistema. ▪ Permite proveer servicios de un servidor Proxy, servidor de

[52] Elaborado por: La Autora

	correo o servidor Web de aplicación.
Fortalezas	▪ Es fundamental para el desarrollo de aplicaciones ya que se ejecutarán en él.
Debilidades	▪ El problema de usar un computador como servidor Web es que conviene tenerlo encendido permanentemente (para que esté accesible de forma continua como la mayoría de los sitios Web), con el consiguiente coste debido al consumo de electricidad. ▪ La utilización de protocolos como el http aumentan los riesgos de permitir procesar datos de los clientes de los servicios.
Área de Evaluación Clave	Disco lógico Memoria Red - Ancho de banda Hardware

Tabla 4:16 Servidor Web [53]

SERVIDOR DE APLICACIONES	
Rol	Permite conectar computadoras que trabajan con diversos sistemas operativos en un entorno de red, autorizando a los usuarios a compartir archivos y recursos del sistema como: periféricos, impresoras y datos en el disco duro. Permite también ejecutar aplicaciones distribuidas utilizando arquitectura cliente/servidor.

[53] Elaborado por: La Autora

Características	▪ Controla los eventos presentados en las aplicaciones. ▪ Controla las transacciones realizadas. ▪ Controla las solicitudes según llegan al servidor. ▪ Realiza la medición de acceso de usuarios, control de estado y de sesión
Fortalezas	▪ La principal ventaja de la tecnología de los servidores de aplicación es la centralización y la disminución de la complejidad del desarrollo de aplicaciones, puesto que proveen infraestructura para que las aplicaciones no sean programadas en su totalidad y solo requieran ser ensambladas. [54]
Debilidades	▪ El Servidor de Aplicaciones debe proveer una alta disponibilidad, la misma que no resulta gratuita ya que se penaliza el uso de recursos o muchas veces penaliza el rendimiento.
Área de Evaluación Calve	Memoria Procesador Red Servidor

Tabla 4:17 Servidor de Aplicaciones [55]

[54] Fuente: Diccionario Informático: Definición de Servidor de Aplicaciones; http://www.alegsa.com.ar/Dic/servidor%20de%20aplicaciones.php

[55] Elaborado por: La Autora

SERVIDOR DE IMPRESIONES	
Rol	Debe ser capaz de gestionar una o varias impresoras y además debe ser capaz de administrar impresoras remotas
Características	▪ Reduce el número de impresoras en la organización ▪ Incorpora una cola de impresión ▪ Comparte impresoras ▪ Computariza la transmisión y recepción de imágenes de fax
Fortalezas	▪ Permite que todos los usuarios de la red, independientemente de la ubicación física del computador y de la plataforma utilizada, puedan imprimir en una impresora determinada. Con lo que se puede saber quién imprimió y cuando lo hizo.
Debilidades	▪ La cola de impresión suele utilizar memoria para el almacenamiento debido a que puede mover datos más rápido que un disco duro y cuando la cola se llena, los documentos se envían al disco duro del servidor a esperar su turno; por lo que se necesita tener suficiente espacio en disco.
Área de Evaluación Clave	Procesador Red Disco

Tabla 4:18 Servidor de Impresiones [56]

[56]Elaborado por: La Autora

SERVIDOR DE ARCHIVOS	
Rol	Es un dispositivo de almacenamiento de archivos en una LAN o en Internet, al mismo que pueden acceder los distintos usuarios de la red.
Características	▪ Realizar transferencia de archivos ▪ Permite la migración y almacenamiento de datos ▪ Sincroniza la actualización de archivos ▪ Controla el acceso a los archivos ▪ Conserva los permisos de red ▪ Facilita la administración y exploración de la red ▪ Organiza los recursos en estructura de árbol ▪ Administra varias carpeta compartidas desde una única ubicación
Fortalezas	▪ Puede prestar sus servicios desde cualquier tipo de servidor ▪ La localización de archivos compartidos es transparente para los clientes.
Debilidades	▪ Puede ser un reto reforzar las seguridades de los servidores de archivos Windows ya que utilizan ciertos protocolos que proporcionan mucha información a usuarios no autenticados.
Área de Evaluación Clave	Disco Memoria

Tabla 4:19 Servidor de Archivos [57]

[57]Elaborado por: La Autora

SERVIDOR DE DOMINIO	
Rol	Controla el dominio raíz y conoce todos los servidores autorizados para los dominios de primer nivel
Características	▪ El servidor de Dominio es el servidor que autentica a los usuarios en la red. ▪ Contiene los programas encargados de agrupar y mantener disponible la información asociada a un espacio de nombres de dominio.
Fortalezas	▪ Permite administrar de mejor manera los recursos y usuarios de la red, brindando un adecuado nivel de seguridad si se lo configura bien.
Debilidades	▪ El servidor de dominio es muy propenso a sufrir ataques de intrusos; los mismos que podrían modificar datos, crear ataques por servicio denegado o efectuar ataques de redireccionamiento.[58] ▪ Necesita estar siempre en línea afectando al consumo eléctrico.
Área de Evaluación Clave	Red Memoria Servidor

Tabla 4:20 Servidor de Dominio [59]

[58] Amenaza para la Seguridad DNS

Fuente: http://technet.microsoft.com/es-es/library/cc783606(WS.10).aspx

[59]Elaborado por: La Autora

De acuerdo a la información detallada en las tablas se puede decir que todo servidor puede ser víctima de ataques, unos en mayor grado que otros; las amenazas no solamente pueden provenir de fuera de la organización sino también pueden estar dentro de esta; de allí que todos los servidores requieren una adecuada protección.

Por tal motivo se desarrolla el procedimiento para evaluar tanto las seguridades como el rendimiento de los servidores Windows; para lo cual, en el primer capítulo se estudiaron las 10 herramientas de evaluación más utilizadas y recomendadas en la actualidad las mismas que facilitarán la tarea de evaluación del servidor acorde a los recursos descritos en las tablas anteriores.

El profesional de TI encargado de realizar evaluaciones a los servidores encontrará en el presente documento información que le facilitará dicha evaluación; ya que de acuerdo al tipo de servidor que desee evaluar, puede encontrar una herramienta acorde a las necesidades; tomando en cuenta los parámetros y valores umbrales que permiten medir el pulso del servidor.

Finalmente, en cuanto a la seguridad se refiere, mediante algunas de las herramientas de evaluación descritas en el capítulo 1 se puede bloquear puertos y servicios no utilizados; ya que puede significar un problema, puesto que se pueden instalar servicios innecesarios con configuraciones por defecto y activados por defecto; lo cual en consecuencia puede causar tráfico indeseado al servidor.

4.2.2. Pasos para realizar la evaluación del Rendimiento

4.2.2.1. Paso 1 Plantear los objetivos de la evaluación del servidor

Mediante el establecimiento de los objetivos que se desean alcanzar con la evaluación se puede visualizar de forma clara los elementos que podrían estar influyendo en la variación del rendimiento del servidor; y que de una u otra manera afectan al desarrollo de la organización. La consecución de los objetivos planteados ayudará en el proceso de toma de decisiones de la organización.

4.2.2.2. Paso 2 Determinar las funciones que cumple el servidor a ser evaluado

La red de la organización puede estar conformada por un conjunto de servidores los mismos que deben tener sus funciones bien definidas, lo que ayudará a mantener un buen control del rendimiento y de las seguridades. Un ejemplo claro de lo antes mencionado es que en algunas organizaciones tienden a combinar las funciones de un servidor en una misma máquina por ejemplo la base datos la ubican en el servidor de aplicaciones, lo que nunca se debe hacer ya se pone en peligro uno de los activos más importantes de la organización que es la información. Por lo tanto, es imprescindible analizar al servidor a ser evaluado y a su entorno.

Antes de determinar las funciones del servidor es necesario primero conocer a la organización realizando una breve descripción de esta en la que se señalen las actividades que realiza, estructura, organización y otros aspectos que permitan conocer el entorno en el que trabaja el servidor. Esto ayudará a determinar si el rendimiento del servidor se alinea con la consecución de los objetivos de la organización.

Por otro lado, la realización de este paso ayudará a establecer los activos de información presentes en el servidor, los mismos que serán de mucha utilidad para realizar la evaluación de las seguridades en lo posterior.

4.2.2.3. Paso 3 Determinar los recursos del servidor que necesitan ser evaluados

Una vez definidas las funciones que cumple el servidor es necesario realizar un análisis de los recursos que dicho servidor utiliza; para lo cual se puede tomar como referencia los datos de las tablas 1 a la 6 de los Tipos de Servidores descritas anteriormente. Se sugiere realizar la evaluación de acuerdo al rol de servidor que cumple; por ejemplo, si el servidor actúa como servidor de base de datos debería evaluarse el espacio físico en disco, el procesador, memoria, etc.

4.2.2.4. Paso 4 Seleccionar la herramienta de evaluación

Al definir el o los recursos a ser evaluados, se selecciona la(s) herramienta(s) que mejor se adapten a las necesidades de evaluación; para lo cual se puede tomar como referencia la tabla 11 de Herramientas de Evaluación y sus Contadores correspondiente al capítulo 2.

4.2.2.5. Paso 5 Medir el recurso en conflicto y analizar los resultados obtenidos

Mediante el uso de la herramienta se procede a evaluar los recursos; tomando como referencia los parámetros de evaluación clave de cada servidor en base a la información provista en las tablas de los Parámetros de Evaluación desarrolladas en el Capítulo 2.

Una vez que se obtienen los resultados de la medición se procede a realizar el análisis respectivo de los datos ya sea de forma escrita o con la ayuda de gráficos. Los valores obtenidos pueden ser comparados con los descritos en la tabla 10 de Valores Umbrales correspondiente al capítulo 2. Determinando de esta forma, en donde se encuentran los cuellos de botella que están ocasionando una variación en el rendimiento del servidor.

4.2.2.6. Paso 6 Elaborar los Informes

Como se menciona en la Metodología de Evaluación de Sistemas[60] desarrollada por el Ingeniero Jaime Naranjo, los informes deben contener lo realmente esencial, así se haya utilizado gran cantidad de material para realizar la evaluación. Se debe tomar en cuenta además el uso del lenguaje ya que los resultados del trabajo realizado pueden ser requeridos tanto a nivel gerencial como a nivel técnico por lo que la presentación de los informes debe ser clara y concisa; si los informes contienen gráficos, estos deben ser nítidos y la presentación de las conclusiones y recomendaciones debe ser objetiva.

4.2.3. Pasos para realizar la evaluación de Seguridades

4.2.3.1. Paso 1 Establecer los objetivos de la evaluación de la seguridad del servidor

[60] Fuente: Metodología para la Evaluación del Desempeño de una Unidad Informática; Naranjo Anda, Jaime Fabián, año 2000

Los objetivos deben expresar con claridad que es lo que es lo que se pretende alcanzar con la evaluación, lo que ayudará a esclarecer los requerimientos de seguridad del servidor.

4.2.3.2. Paso 2 Identificar las políticas de seguridad aplicadas al servidor a ser evaluado

En el capítulo anterior se definió la importancia del establecimiento de políticas de seguridad y de como estas permiten cumplir con una gestión efectiva de los mecanismos de protección existentes. Entre otras cosas se puede identificar si se aplica algún control de acceso, si existe alguna herramienta hardware o software para proteger al servidor, si se realizan evaluaciones periódicas y todos los demás aspectos que son sugeridos en los marcos de trabajo estudiados en el presente proyecto de titulación.

La identificación de las políticas de seguridad aplicadas al servidor permitirá determinar los posibles puntos débiles de seguridad que rodean al servidor.

4.2.3.3. Paso 3 Identificar y comprender las vulnerabilidades, las amenazas y los incidentes de seguridad

La identificación de las vulnerabilidades y amenazas está relacionada con el proceso de Análisis y Evaluación de Riesgos lo cual sugiere realizar un estudio de la forma como la organización gestionan los riesgos, con la finalidad de determinar si los resultados obtenidos benefician o no a la organización. En caso de no existir un proceso para gestionar los riesgos o si este no es el más adecuado, se podrá concluir que la organización está expuesta a posibles daños potenciales que pueden surgir por un proceso presente o un suceso futuro; afectando directamente al desempeño de la organización.

Para identificar las vulnerabilidades que afectan al servidor se puede realizar un escaneo de vulnerabilidades mediante el uso de herramientas software existentes y bajo la autorización del profesional de TI encargado de la administración del Servidor; este proceso permitirá intuir si el sistema puede resistir con un determinado nivel de confianza a las acciones malintencionadas e ilícitas que pudieran comprometer la disponibilidad, autenticidad, integridad y confidencialidad de los datos que gestiona o procesa el servidor evaluado.

4.2.3.4. Paso 4 Elaborar los informes

De igual forma la elaboración de informes debe cumplir con los aspectos descritos en el punto 4.2.2.6.

4.3. VALIDACIÓN DEL PROCEDIMIENTO

Para validar el procedimiento realizado en el presente proyecto de tesis se analizará el Servidor RADIUS ubicado en el Centro de Gestión de los Laboratorios DICC de la Facultad de Ingeniería de Sistemas.

La información y el apoyo para llevar a cabo la validación del procedimiento fueron suministrados por el Ingeniero Patricio Proaño (Jefe de Laboratorio) e Iván Proaño (ayudante de laboratorio) encargado de administrar el servidor RADIUS.

4.3.1. Evaluación del rendimiento

4.3.1.1. Paso 1 Plantear los objetivos de la evaluación del servidor

- El objetivo principal es el de conocer si el rendimiento del Servidor ayuda a alcanzar los objetivos de desempeño del Departamento de Informática y Ciencias de la Computación (DICC).

- Evaluar el rendimiento del Servidor, dando una visión real de cómo están trabajando sus componentes tanto individualmente como en conjunto; en base a la medición de los índices de desempeño.

- Identificar posibles cuellos de botella presentes en el servidor.

- Elaborar informes acorde a los destinatarios interesados.

4.3.1.2. Paso 2 Determinar las funciones que cumple el servidor a ser evaluado

Como se ha venido mencionando a lo largo del presente proyecto de tesis el rendimiento de un sistema se ve afectado no solo por su funcionamiento interno sino también por la interacción con los demás factores que lo rodean; lo que hace vital realizar una descripción de la organización, a continuación los aspectos relevantes de la misma:

Los Laboratorios DICC forman parte de los Laboratorios y Centros gestionados por el Departamento de Informática y Ciencias de la Computación (DICC); y están organizados en cinco salas: LAN, WIFI, BDD, DES, Internet y el Centro de Gestión; a continuación se describe las funciones específicas de cada sala:

Sala	Funciones
LAN	* Prácticas de Redes alámbricas * Prácticas de Software
WIFI	* Prácticas de Redes inalámbricas * Prácticas de Software
BDD	* Prácticas de Bases de Datos * Prácticas de Software
DES	* Prácticas de Software
Internet	Servicio de Internet para los estudiantes de la FIS[61]
Centro-Gestión	Administración técnica de la Red de datos instalada en el edificio de la FIS

Tabla 4:21 Salas y Funciones de los Laboratorios DICC [62]

De lo que se puede ver en la tabla anterior, entre las actividades principales que se realizan en los Laboratorios DICC están: brindar soporte académico a la docencia,

[61] FIS [Facultad de Ingeniería de Sistemas]

[62] Fuente: http://www.epn.edu.ec/index.php?option=com_content&task=view&id=206&Itemid=455

proveer del servicio de Internet a los estudiantes de la Facultad y administrar la Red de datos. Los recursos hardware y software con los que se cumplen dichas actividades están registrados en el sitio Web de la EPN.[63]

Para realizar la descripción del Servidor es necesario establecer primero la definición del protocolo RADIUS ya que basa su funcionamiento en este y además da origen a su nombre.

"RADIUS (Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) sobre el protocolo PPP (Point to Point Protocol), quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como EAP (Extensible Authentication Protocol). Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le

[63] Fuente 1:
http://www.epn.edu.ec/index.php?option=com_content&task=view&id=764&Itemid=1036#gestion

Fuente 2:
http://www.epn.edu.ec/index.php?option=com_content&task=view&id=765&Itemid=1037#software

asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio." [64]

El Servidor RADIUS que se encuentra en los Laboratorios DICC, recibe los pedidos de conexión de los usuarios, los autentica y autoriza su acceso a la red, permitiendo así conectarse al servicio de Internet Inalámbrico. La autenticación la realiza mediante el protocolo EAP y PEAP. Este servidor es catalogado como AAA, ya que a más de autenticar y autorizar a los usuarios, incluye la función para generar informes (Accounting) como por ejemplo: generar el listado de usuarios conectados en cada momento.

Cabe mencionar que en este servidor se encuentran configurados además los servicios de DHCP, DNS y Directorio Activo; dichos servicios son independientes a la labor que cumple el Servidor de Autenticación y Autorización RADIUS, pero se encuentran en este debido a las condiciones de infraestructura existentes. De este modo, se puede señalar que las cuentas de usuario, grupos, permisos y privilegios son gestionados desde este servidor.

Entre las características de hardware y software el Servidor RADIUS posee:

---

[64] Fuente: http://es.wikipedia.org/wiki/RADIUS

- 2 Discos Duros de 63 GB cada uno aunque solo se utiliza uno
- Memoria RAM de 1 GB
- Procesador Intel XEON 5110 de 1,6 GHz de velocidad
- 2 Interfaces de red Broadcom BCM5708C NetXtreme
- Sistema Operativo Windows 2003 Server R2 Service Pack 1

Para proveer el servicio de Internet el Servidor RADIUS toma parte del ancho de banda provisto por la Unidad de Gestión de la Información (UGI) para toda la facultad de Ingeniería de Sistemas que es de aproximadamente 10 Mbps, es decir, el ancho de banda se distribuye para el personal docente, estudiantes usuarios del Internet de los laboratorios DICC y estudiantes usuarios del servicio Inalámbrico.

Para acceder al servicio de Internet el usuario se registra en el Active Directory en donde se le asigna una cuenta de usuario y su respectiva contraseña, luego se registra la dirección MAC de su computador portátil en los Access Point ya que el filtrado se lo realiza mediante este parámetro. Finalmente se configura el cliente con los parámetros de la red.

Durante las horas pico el servidor presenta dos eventos frecuentes: el primero es que disminuye la velocidad del servicio de Internet que por lo general se debe a que los usuarios realizan gran cantidad de descargas. Para solventar este problema el auxiliar limita el ancho de banda al usuario y va dando prioridades a las descargas.

El otro incidente frecuente que se produce es el bloqueo de los access point cuando los usuarios fallan al intentan iniciar su sesión; y para esto se reinician los access point para que se vuelva a funcionar y continuar con el servicio de Internet.

4.3.1.3. Paso 3 Determinar los recursos del servidor que necesitan ser evaluados

El servidor RADIUS es catalogado básicamente como Servidor de Autenticación aunque además funciona como DNS y Active Directory; por lo que los parámetros a ser medidos son:

Área		**Parámetros de Evaluación**
Memoria	Física	▪ Bytes confirmados (asignados) en uso ▪ Mb disponibles
	Lógica	▪ Páginas por segundo
Red		▪ Total de bytes por segundo ▪ Longitud de la cola de salida ▪ Ancho de banda
Disco Lógico		▪ Espacio libre
Servidor		▪ Errores de permiso de acceso ▪ Errores del sistema ▪ Sesiones cerradas debido a un error

Tabla 4:22 Parámetros de Evaluación [65]

[65] Elaborado por La Autora

4.3.1.4. Paso 4 Seleccionar la herramienta de evaluación

El servidor RADIUS trabaja bajo la plataforma Windows Server 2003 por lo que se utilizó la herramienta propia de los sistemas operativos de la familia Windows que es Performance Monitor (Monitor de Rendimiento), esta herramienta permite incluir todos los contadores establecidos en la tabla 4:22; además, su funcionamiento no interfiere en el desempeño del servidor. Esto último no ocurre con otras herramientas sugeridas en el capítulo 1 y 2 que por ser un software que necesita ser instalado consume recursos del servidor.

4.3.1.5. Paso 5 Medir el recurso en conflicto y analizar los resultados obtenidos

Para poder medir los recursos del servidor RADIUS se establecieron los días y horas de mayor carga de trabajo (horas pico) que son los días lunes, martes y miércoles en los horarios de 9 a 12 de la mañana y de 3 a 6 de la tarde de dichos días.

A continuación se presentan los valores obtenidos en promedio y los valores con los que deberían cumplir:

Parámetros de Evaluación	**Valores Umbrales**	**Servidor RADIUS**	
		9 – 12 h	**15 – 18 h**
Bytes asignados en uso	Menor al 80%	22,64%	22,37 %

Páginas por segundo	Menor a 5 – deseado Mayor a 10 – cuello de botella Mayor o igual a 20 – sistema degradado	3	2
Total de bytes por segundo	70% de la interfaz	Client: 3504,50 Client_2: 0	Client: 2771,31 Client_2: 0
Longitud de la cola de salida	Menor a 2	Client: 0 Client_2: 0	Client: 0 Client_2: 0
Ancho de banda actual	Conexión de banda ancha	10 Mbps	10 Mbps
Espacio libre	Mayor al 15 %	90,05%	90,04%
Errores de permiso de acceso	0	153,78	162
Errores del sistema	0	0	0
Inicios de sesión/s	Menor al 1% de los reingresos	0	0
Sesiones cerradas debido a un error	Menor al 1% de las sesiones activas	190,67	199

Tabla 4:23 Comparación de los valores umbrales medidos [66]

Interpretación de datos

Al analizar los valores obtenidos en promedio de cada parámetro en general se deduce que el Servidor RADIUS tiene un rendimiento aceptable para el tipo de función que desempeña.

- Los valores de Bytes asignados en uso están dentro del umbral permitido lo que indica que no existe problemas con el recurso, que en este caso es la memoria; por lo que el Servidor puede realizar las tareas que le han sido asignadas sin problemas de memoria.

- Con respecto al número de páginas por segundo se leen en promedio 3 Pág./seg en la mañana y 2 pag/seg en la tarde, valores que están por debajo del umbral deseado que es de 5 pag/seg. Esto refuerza la conclusión emitida en el punto anterior, que el recurso memoria trabaja sin problemas.

- Los valores obtenidos en promedio para el Total de bytes por segundo que en la mañana es de 3504,5 B/seg y en la tarde es de 2771,3; no superan al valor umbral del 70% de la interfaz ya que cada interfaz de red permite transmitir un promedio de 11,92 MBps. Lo cual permite concluir que no existen problemas con este recurso; además se puede observar que solamente se usa una de ellas.

[66] Elaborado por: La Autora

- El valor promedio de la longitud de la cola de salida es 0 el mismo que no supera al valor umbral lo que indica que no existen cuellos de botella presentes en el recurso red.

- La conexión de Internet es de banda ancha y es provisto por la UGI con un valor aproximado de 10 Mbps el mismo que es detectado por la interfaz de red como se puede ver en la Tabla 4:23.

- El porcentaje de espacio libre promedio es del 90% el mismo que está en el umbral permitido; lo cual indica que el recurso disco trabaja sin problemas.

- El promedio de los Errores de permiso de acceso tanto en la mañana como en la tarde superan al valor umbral establecido, lo que puede indicar que algún usuario no autorizado está intentando tener acceso a los archivos de información que no estén debidamente protegidos.

- El umbral del parámetro Errores del sistema es 0 lo que indica que el servidor no presenta problemas internos.

- Los valores promedio obtenidos para el parámetro Sesiones cerradas debido a un error superan el valor umbral tanto en la mañana como en la tarde, lo que indica puede existir un cuello de botella en el recurso servidor.

4.3.1.6. Paso 6 Elaborar los Informes

Una vez realizada la evaluación del rendimiento del Servidor RADIUS se elaboró el informe técnico que recopila los datos obtenidos con la aplicación del procedimiento. Del informe presentado al Ingeniero Patricio Proaño existen algunos puntos que fueron aclarados con respecto a los datos presentados en dicho informe entre los que se puede mencionar:

- Dado que el inventario de los equipos que se encuentra publicado en el sitio Web de la EPN registra como última fecha de actualización mayo de 2009 el Ingeniero Proaño supo manifestar que ya se realizó una actualización reciente en octubre por lo que la información encontrada en el sitio Web no está actualizada.

- Con respecto a la velocidad de conexión del servicio de Internet a criterio del Ingeniero tanto la distribución del ancho de banda como la misma estructura de red hacen que la velocidad se vea afectada. Los 10 Mbps asignados por la UGI no abastecen para el número de usuarios que desean acceder al servicio (considerando que: el personal docente tiene siempre activo este servicio, además hay estudiantes que utilizan el Internet desde los laboratorios y hay estudiantes que acceden al Internet Inalámbrico).

Los demás datos obtenidos de la evaluación del rendimiento del Servidor RADIUS se encuentran en el Informe Técnico especificado en el Anexo 2; el mismo que ha sido revisado por el Ingeniero Patricio Proaño, quien aportó con las respectivas correcciones al informe.

4.3.2. Evaluación de las Seguridades

4.3.2.1. Paso 1 Establecer los objetivos de la evaluación de la seguridad del servidor

- Determinar si la administración de la seguridad del servidor RADIUS se gestiona de forma adecuada y si esta responde a los requerimientos del Centro de Gestión de los Laboratorios DICC.

- Determinar si existen los controles necesarios sugeridos en las mejores prácticas para mantener la seguridad del sistema.

- Fomentar una cultura sobre la importancia de precautelar la seguridad del servidor y en general de los sistemas de información.

4.3.2.2. Paso 2 Identificar las políticas de seguridad aplicadas al servidor a ser evaluado

Actualmente no existe un documento formal que exponga las políticas de seguridad para la administración del servidor RADIUS. Aunque si existen algunos criterios para protegerlo como: Antivirus (provisto por el servidor de Antivirus), firewall y cierto nivel de control de acceso.

4.3.2.3. Paso 3 Identificar y comprender las vulnerabilidades, las amenazas y los incidentes de seguridad

Según los criterios de las mejores prácticas en cuanto a la seguridad de los sistemas se refiere la organización debe mantener ciertos controles que garanticen la seguridad de los mismos, y cuando esto no se da se crea el ambiente preciso para la presencia de vulnerabilidades y amenazas que conllevan a la aparición de riesgos que deben ser tratados adecuadamente.

Para este paso se tomó como referencia Los Objetivos de Control y Controles sugeridos tanto en la Norma ISO 27001[67] y en COBIT[68]. A continuación se establecen los puntos débiles existentes:

---

[67] Fuente: Anexo A, Estándar Internacional ISO/IEC 27001-2005, primera edición, 2005

- La organización actualmente no cuenta con planes, políticas y procedimientos de seguridad formalmente documentados aunque las personas que administran los Servidores tienen conocimiento de cómo llevar a cabo su trabajo.

- No se cuenta con la estructura organizacional para mantener la seguridad de la información.

- El auxiliar de laboratorio conoce y entiende bien su responsabilidad en el uso y gestión del servidor pero no cuenta con los mecanismos necesarios para apoyar el aseguramiento de la información que gestiona el servidor.

- El acceso físico al servidor RADIUS no tiene un control de acceso muy riguroso que permita precautelar su seguridad.

- El ambiente en el que se encuentra el Servidor varía entre los 26 y 30 grados Centígrados, temperatura no muy apta para el desenvolvimiento de este.

- No existe un procedimiento formal que describa al responsable del servidor como crear cuentas de usuario y de cómo otorgar los privilegios de acceso.

- No se realizan pruebas de seguridad ni monitoreos que permitan detectar posibles vulnerabilidades existentes en el sistema.

---

[68] Fuente: COBIT 4.0, CobiT4_Espanol.pdf; IT Governance Institute; Pág. 119

- No se realiza una gestión de incidentes de seguridad.

- No se lleva a cabo un proceso de análisis de riesgos lo que puede causar una interrupción del servicio a mediano o largo plazo.

- Los usuarios del servicio de Internet no se encuentran satisfechos con la velocidad de conexión que se les asigna.

4.3.2.4. Paso 4 Elaborar los informes

Al evaluar las seguridades del servidor RADIUS se hallaron algunos puntos débiles los mismos que fueron recopilados en el Informe Técnico presentado en el Anexo 2. Con respecto a los resultados obtenidos, el Ingeniero Proaño corroboró en algunos aspectos y aclaró otros, entre ellos se tiene:

- La organización cuenta con políticas y procedimientos de seguridad sencillos que han permitido su buen desempeño hasta el momento. Con respecto a los planes y estructura organizacional de seguridad no se los ha desarrollado primero porque en los Laboratorios DICC no se gestiona información de mayor relevancia y por otro lado la unidad está atravesando por un proceso de modernización al igual que los demás centros de TI de la EPN.

- El acceso físico al Servidor RADIUS no tiene un control muy riguroso tomando en cuenta que si se cierran las puertas de acceso, se concentrará mucho más el calor.

- La unidad no cuenta con un sistema de ventilación y de aire acondicionado que permitan controlar la temperatura del lugar. Los dos ventiladores existentes ayudan a mitigar en parte el problema.

- Los monitores CRT han sido cambiados por LCD lo que mejora el aspecto visual evitando el cansancio visual de las personas que utilizan los equipos.

- No se realizan análisis muy frecuentes del rendimiento del servidor debido a que la información que se almacena en este no es relevante para la unidad ya que tienen los respaldos necesarios para mantener el servicio en funcionamiento.

- Dado que hasta el momento no se han producido problemas que causen interrupciones en el servicio, no se cree conveniente la implementación de un proceso para la gestión de incidentes de seguridad ni para la realización de un análisis de riesgos.
- No se puede llevar a cabo un continuo proceso de capacitación al personal dado que no tienen un contrato fijo de tiempo.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez realizada la aplicación del procedimiento para evaluar el rendimiento y las seguridades de los servidores Windows se llega a las siguientes conclusiones:

- La aplicación de normas y estándares internacionales garantiza que la TI de las organizaciones sostengan y extiendan las estrategias y objetivos organizacionales.

- El procedimiento desarrollado en el presente proyecto de tesis es aplicable en pequeñas y medianas organizaciones, ya que permite obtener resultados expeditos de la situación actual de los servidores.

- El actual proceso de modernización de las unidades de TI de la EPN no ha permitido establecer un plan de seguridad en los Laboratorios DICC, por cuanto se sometería a continuos cambios, lo que incurre en pérdida de tiempo hasta encontrar un nivel estable de funcionamiento de las unidades.

- De acuerdo a los resultados obtenidos en la evaluación del rendimiento se concluye que el servidor se encuentra en buenas condiciones ya que no presentó cuellos de botella relevantes, en decir, presenta un buen desempeño.

- Los sistemas operativos Windows ofrecen continuos mejoramientos en cuanto a aspectos de seguridad y rendimiento se refiere lo que ayuda a mejorar y mantener buenos niveles de disponibilidad de los sistemas.

- De acuerdo al proyecto programado para dotar de Internet Inalámbrico en todo el Campus Politécnico por parte de la UGI, el Laboratorio DICC tendrá que prescindir de los servicios del Servidor RADIUS, por lo que, por el momento no se puede solicitar un aumento del ancho de banda a la Unidad de Gestión de Información.

- Durante la aplicación del procedimiento se pudo identificar que la información que se almacena en el servidor RADIUS cuenta con los respaldos para asegurar la disponibilidad del servicio, uno de dichos respaldos se encuentra en la UGI.

- Las pruebas de seguridad y monitoreos del rendimiento del Servidor RADIUS no se realizan muy frecuentemente, ya que la información almacenada en este no es susceptible de ataques.

5.2. RECOMENDACIONES

Para lograr un mejor rendimiento de los Servidores Windows y asegurar su protección se realizan las siguientes recomendaciones:

- Tomar como base las mejores prácticas utilizadas actualmente para mejorar el rendimiento de la organización en el corto y largo plazo.

- Dado que los sistemas están en permanente cambio y expansión, sus componentes cambian y adicionalmente el personal y las políticas de

seguridad también cambian lo que implica que se produzcan nuevos riesgos de seguridad por lo que se recomienda llevar a cabo un proceso de Gestión del Riesgo que esté en permanente evolución.

- Se recomienda utilizar el procedimiento de evaluación y las herramientas estudiadas en el presente Proyecto de Titulación, ya que permiten realizar un estudio óptimo del rendimiento y de las seguridades de los servidores Windows.

- El presente Proyecto de Titulación incluye tablas descriptivas de algunos tipos de servidores las mismas que pueden servir para identificar funciones que no deben estar en un mismo servidor ya que el fallo de un servicio puede afectar a los demás.

- El procedimiento de evaluación desarrollado en el presente Proyecto de Titulación recomienda gestionar la adquisición un sistema de ventilación y un sistema de aire acondicionado para que la temperatura de la unidad no afecte al rendimiento tanto de los servidores como del personal que labora en el Centro de Gestión de los Laboratorios DICC.

- Se recomienda que se tome la información de esta tesis como pauta para implementar un proceso de Gestión de Incidentes de Seguridad que permitan mejorar la productividad de los usuarios del servicio de Internet.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

1. H. M. Deitel, Introducción a los Sistemas Operativos, Addison-Wesley, México, 1987.
2. Estándar Internacional ISO/IEC 2700, Primera Edición, año 2005.
3. OCTAVE Method Implementation Guide, Version 2.0, Volume 1.

PÁGINAS WEB

1. Cómo tomarle el pulso a un servidor; Internet.

http://technet.microsoft.com/es-es/magazine/2008.08.pulse.aspx

Acceso último: 2/12/2009

2. Herramientas de Evaluación; Internet.

http://www.paessler.com

http://www.ks-soft. net

http://www.serverassist.com

http://www.speedtestpro.net

http://www.gfi.com

http://www.futuremark.com/products/pcmark05

http://www.tango04.es/productos/vcw/index.php

http://www.manageengine.com

Acceso último: 2/12/2009

3. Círculo de Deaming; Internet.

http://es.wikipedia.org/wiki/PDCA

Acceso último: 2/12/2009

4. Planes de Seguridad; Internet.

http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad

Acceso último: 2/12/2009

5. Gestión de Incidentes; Internet.

http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

Acceso último: 6/02/2010

6. Recursos de Hardware del Centro de Gestión; Internet.

http://www.epn.edu.ec/index.php?option=com_content&task=view&id=764&Itemid=1036#gestion

Acceso último: 2/12/2009

7. Recursos de Software del Laboratorio L-DICC; Internet.

http://www.epn.edu.ec/index.php?option=com_content&task=view&id=765&Itemid=1037#software

Acceso último: 2/12/2009

8. Protocolo RADIUS; Internet.

http://es.wikipedia.org/wiki/RADIUS

Acceso último: 6/02/2010

ANEXOS

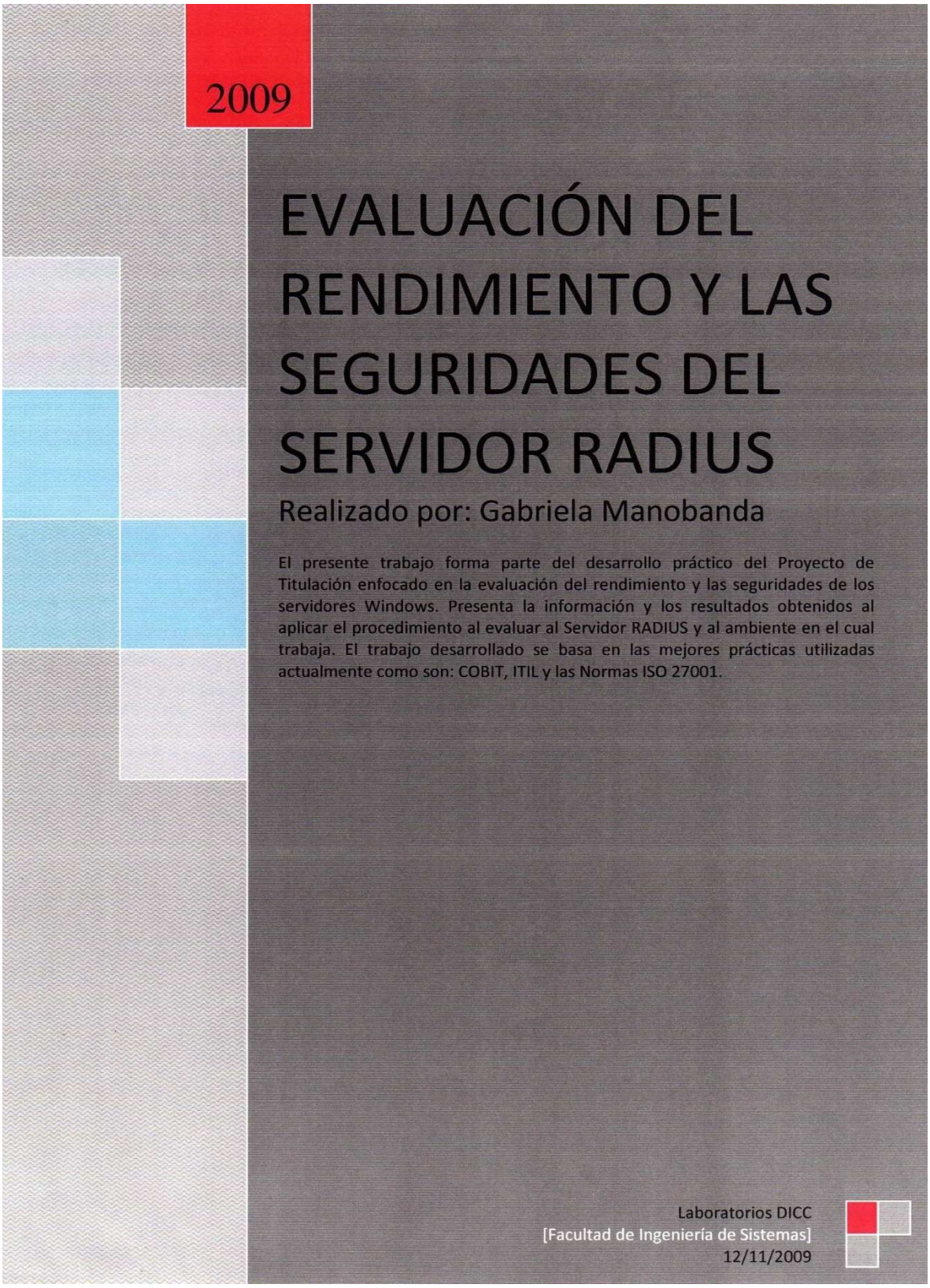
ANEXO 1: GLOSARIO

TÉRMINO	SIGNIFICADO
Activo	Cualquier cosa que tenga valor para la organización
Análisis de riesgo	Uso sistemático de la información para identificar fuentes y para estimar el riesgo
COBIT	Objetivos de Control para la Información y Tecnologías Relacionadas
Confidencialidad	Propiedad de que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados
Disponibilidad	Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada
Evaluación del riesgo	Proceso de comparar los tipos de riesgo para determinar la importancia del riesgo.
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización con relación al riesgo

IEC	Comisión Electrotécnica Internacional
Incidente de seguridad	Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
Integridad	Propiedad de salvaguardar la exactitud e integridad de los activos.
ISO	Organización Internacional para la Estandarización
ITIL	Biblioteca de la Infraestructura de las Tecnologías de la Información
NORMA ISO/IEC 27001	Estándar para la seguridad de la Información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.
RADIUS	Remote Authentication Dial-In User Server. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la Información; además pueden estar

	involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.
TI	Tecnología de la Información
Windows 2003 Server	Sistema operativo de la familia Windows de la marca Microsoft para servidores que centra el uso de procesador en las características de servidor lo que permite obtener un mejor rendimiento.
Windows 2008 Server	Sistema operativo de la familia Windows de la marca Microsoft para servidores, gestiona el sistema de forma más efectiva.
Windows Server	Es una plataforma que permite la creación de una infraestructura de aplicaciones, redes y servicios Web conectados, del grupo de trabajo al centro de datos.

ANEXO 2: INFORME TÉCNICO



EVALUACIÓN DEL RENDIMIENTO Y LAS SEGURIDADES DEL SERVIDOR RADIUS

1. OBJETIVOS DE LA EVALUACIÓN DEL RENDIMIENTO Y LAS SEGURIDADES DEL SERVIDOR RADIUS

Rendimiento

- El objetivo principal es el de conocer si el rendimiento del Servidor ayuda a alcanzar los objetivos de desempeño del Departamento de Informática y Ciencias de la Computación (DICC).
- Evaluar el rendimiento del Servidor dando una visión real de cómo están trabajando sus componentes tanto individualmente como en conjunto; en base a la medición de los índices de desempeño.
- Identificar posibles cuellos de botella presentes en el servidor.

Seguridad

- Determinar si la administración de la seguridad del servidor RADIUS se gestiona de forma adecuada y si esta responde a los requerimientos del Centro de Gestión de los Laboratorios DICC.
- Determinar si existen los controles necesarios sugeridos en las mejores prácticas para mantener la seguridad del sistema.
- Fomentar una cultura sobre la importancia de precautelar la seguridad del Servidor y en general de los sistemas de información.

2. DESCRIPCIÓN DE LA ORGANIZACIÓN

Los Laboratorios DICC forman parte de los Laboratorios y Centros gestionados por el Departamento de Informática y Ciencias de la Computación (DICC); y están

organizados en cinco salas: LAN, WIFI, BDD, DES, Internet y el Centro de Gestión; a continuación se describe las funciones específicas de cada sala:

SALA	**FUNCIONES**
LAN	* Prácticas de Redes alámbricas * Prácticas de Software
WIFI	* Prácticas de Redes inalámbricas * Prácticas de Software
BDD	* Prácticas de Bases de Datos * Prácticas de Software
DES	* Prácticas de Software
Internet	Servicio de Internet para los estudiantes de la FIS
Centro-Gestión	Administración técnica de la Red de datos instalada en el edificio de la FIS

Tabla 24 Salas y Laboratorios de los Laboratorios DICC [69]

De lo que se puede ver en la tabla anterior, entre las actividades principales que se realizan en los Laboratorios DICC están: brindar soporte académico a la docencia, proveer del servicio de Internet a los estudiantes de la Facultad y administrar la Red de datos.

[69] Fuente: http://www.epn.edu.ec/index.php?option=com_content&task=view&id=206&Itemid=455

3. AMBIENTE TECNOLÓGICO

RECURSOS HUMANOS

La organización cuenta con personas que trabajan directamente en ella entre las que se puede citar:

- Ing. Patricio Proaño: Quien tiene a su mando la gestión de la unidad.
- Auxiliares y Ayudantes de Laboratorio: Quienes se encargan de gestionar los servidores existentes en la unidad, brindan soporte al personal docente y estudiantes de la Facultad.

INFRAESTRUCTURA TECNOLÓGICA

Los recursos hardware y software con los que se cumplen dichas actividades constan en el sitio Web de Universidad. Cabe mencionar que la información fue actualizada por última vez en octubre del presente año. Los enlaces son:

- http://www.epn.edu.ec/index.php?option=com_content&task=view&id=764&Itemid=1036#gestion
- http://www.epn.edu.ec/index.php?option=com_content&task=view&id=765&Itemid=1037#software

4. ASPECTOS DE GESTIÓN DE LA SEGURIDAD DEL CENTRO DE GESTIÓN

Seguridad física

El ingreso a Los Laboratorios DICC se lo hace mediante la debida autenticación con la persona encargada de gestionar el ingreso en la puerta principal. Además, para ingresar al Centro de Gestión no existen controles rigurosos, únicamente se pide el ingreso a un ayudante o auxiliar presente en ese momento.

Con respecto a los servidores, cada uno de ellos es protegido por su respectivo Auxiliar o Ayudante de Laboratorio.

Seguridad para los recursos humanos

En cuanto a la seguridad para recursos humanos el principal inconveniente que se encontró es que no existe un adecuado sistema de ventilación ni de aire acondicionado que permitan controlar el exceso de calor que se produce tanto por los servidores como por el medio ambiente en especial al medio día y al transcurrir la tarde; lo que conlleva a que el personal no se sienta cómodo en el área en dichos instantes. Los dos ventiladores existentes ayudan a mitigar en parte el calor.

Por otro lado, se pudo ver que los monitores son LCD lo que evitan el cansancio visual de los usuarios de los equipos.

Cabe mencionar que en caso de que los usuarios necesiten ayuda médica cuentan con el dispensario médico de la Universidad.

Seguridad lógica

Existe el uso obligado de cuentas y claves de usuario que responden a los requerimientos de perfiles de usuario es decir existen cuentas limitadas y de administrador. En el Servidor RADIUS solamente existe la cuenta de administrador para ingresar al sistema, la misma que por definición tiene todos los privilegios.

Existen políticas para la gestión de contraseñas las mismas que especifican que las cuentas y contraseñas serán cambiadas cada inicio de semestre.

Seguridad de Datos

Los datos que se manejan en el servidor son protegidos básicamente mediante la utilización del firewall y de antivirus. El servidor RADIUS almacena la información de los usuarios para que estos puedan acceder al servicio de Internet Inalámbrico está propenso a intrusiones por parte de los usuarios que se conectan al servicio de Internet, lo que afectaría directamente en rendimiento del Servidor por lo que un continuo análisis de este garantizaría la eficiencia del servicio. Esta actividad no se la lleva a cabo muy frecuentemente ya que según el criterio del Jefe de Laboratorio la información almacenada en este Servidor no es relevante para quienes deseen atentar contra el sistema y además que cuentan con los respaldos correspondientes.

Seguridad Legal

Los productos software utilizados son adquiridos con licencia como se puede ver en el documento provisto en sitio Web de Universidad cuyo enlace es:

- http://www.epn.edu.ec/index.php?option=com_content&task=view&id=765&Itemid=1037#software

5. PLANES DE LA UNIDAD

Si bien es cierto los auxiliares y ayudantes de laboratorio conocen y entienden bien sus responsabilidades las cuales han sido comunicadas de forma verbal; no existen documentos formales en que ellos puedan apoyarse para llevar a cabo su trabajo ya que la unidad se encuentra en un proceso de transición con respecto a la anterior administración por lo que los planes, políticas y procedimientos están en una etapa de actualización.

6. CARGA DEL SISTEMA

Los usuarios utilizan el servicio de Internet en mayor cantidad en los horarios de 9h00 a 12h00 en la mañana y de 15h00 a 18h00 por la tarde de los días lunes, martes y miércoles. En dichos horarios los problemas más frecuentes son: la disminución de la velocidad del servicio que por lo general se debe a que los usuarios realizan gran cantidad de descargas; para solventar este problema el auxiliar limita el ancho de banda al usuario y va dando prioridades a las descargas. Otro incidente frecuente que se produce es el bloqueo de los access point cuando los usuarios fallan al intentan iniciar su sesión; y para esto se reinician los access point para que retomen su funcionamiento continuando así con el servicio de Internet.

7. PROBLEMAS E HIPÓTESIS

Posibles problemas

- La organización actualmente no cuenta con planes, políticas y procedimientos de seguridad documentados, formalizados ni comunicados a las personas que administran el Servidor.
- No se cuenta con la estructura organizacional para mantener la seguridad de la información.
- El auxiliar de laboratorio conoce y entiende bien su responsabilidad en el uso y gestión del servidor pero no cuenta con los mecanismos necesarios para apoyar el aseguramiento de la información que gestiona el servidor.
- El acceso físico al servidor RADIUS no tiene un control de acceso muy riguroso que permita precautelar su seguridad.
- El ambiente en el que se encuentra el Servidor varía entre los 26 y 30 grados Centígrados, temperatura no muy apta para el desenvolvimiento de este.

- No existe un procedimiento formal que describa al responsable del servidor como crear cuentas de usuario y de cómo otorgar los privilegios de acceso.
- No se realizan pruebas de seguridad ni monitoreos que permitan detectar posibles vulnerabilidades existentes en el sistema.
- No se realiza una gestión de incidentes de seguridad.
- No se lleva a cabo un proceso de análisis de riesgos lo que puede causar una interrupción del servicio a mediano o largo plazo.
- Los usuarios del servicio de Internet no se encuentran satisfechos con la velocidad de conexión que se les asigna.

Hipótesis

- El problema de no contar con planes, políticas, procedimientos o una estructura organizacional de seguridad se debe a que la unidad se encuentra en una etapa de actualización en la que se ha empezado a manejar procedimientos y políticas sencillas.
- El problema del acceso físico al servidor se debe que no se utilizan los estándares internacionales en cuanto a la seguridad de los sistemas se refiere.
- El exceso de calor en el que se encuentra el servidor se debe a que el ventilador existente no abastece lo que puede afectar a su rendimiento.
- El no realizar monitoreos ni pruebas de seguridad frecuentes puede deberse a la falta de coordinación de los niveles de gestión de la organización.
- El problema de no llevar a cabo un proceso de análisis de riesgos y de gestión de los incidentes puede causar una interrupción del servicio a mediano o largo plazo.
- El problema de los usuarios insatisfechos puede deberse a la forma en que se ha desarrollado el esquema de red o puede deberse al elevado incremento en el número de usuarios que acceden al servicio en la actualidad.

8. SESIONES DE MEDIDA

Descripción del servidor

La función del Servidor RADIUS es básicamente proveer el servicio de Internet inalámbrico a los estudiantes de la Facultad de Ingeniería en Sistemas; además trabaja como servidor de dominio y Active Directory. De modo que, las cuentas de usuario, grupos, permisos y privilegios son gestionados desde este servidor.

Entre las características de hardware y software el Servidor RADIUS posee:

- 2 Discos Duros de 63 GB cada uno aunque solo se utiliza uno
- Memoria RAM de 1 GB
- Procesador Intel XEON 5110 de 1,6 GHz de velocidad
- 2 Interfaces de red Broadcom BCM5708C NetXtreme
- Sistema Operativo Windows 2003 Server R2 Service Pack 1

Para proveer el servicio de Internet el Servidor RADIUS toma parte del ancho de banda provisto por la Unidad de Gestión de la Información (UGI) para toda la facultad de Ingeniería de Sistemas que es de aproximadamente 10 Mbps, es decir, el ancho de banda se distribuye para el personal docente, estudiantes usuarios del Internet de los laboratorios DICC y estudiantes usuarios del servicio Inalámbrico.

Para acceder al servicio de Internet el usuario se registra en el Active Directory en donde se le asigna una cuenta de usuario y su respectiva contraseña, luego se registra la dirección MAC de su computador portátil en los Access Point ya que el

filtrado se lo realiza mediante este parámetro. Finalmente se configura el cliente con los parámetros de la red.

Durante las horas pico el servidor presenta dos eventos frecuentes: el primero es que disminuye la velocidad del servicio de Internet que por lo general se debe a que los usuarios realizan gran cantidad de descargas. Para solventar este problema el auxiliar limita el ancho de banda al usuario y va dando prioridades a las descargas. El otro incidente frecuente que se produce es el bloqueo de los access point cuando los usuarios fallan al intentar iniciar su sesión; y para esto se reinician los access point para que se vuelva a funcionar y continuar con el servicio de Internet.

Herramientas a utilizar

El servidor RADIUS trabaja bajo la plataforma Windows Server 2003 por lo que se utilizó la herramienta propia de los sistemas operativos de la familia Windows que es Performance Monitor (Monitor de Rendimiento), esta herramienta permite añadir todos los contadores necesarios; además, su funcionamiento no interfiere en el desempeño del servidor. Esto último no ocurre con otras herramientas de monitoreo que al ser un software que necesita ser instalado consumen recursos del servidor.

Recolección y Selección de datos

Para poder medir los recursos del servidor RADIUS se establecieron los días y horas de mayor carga de trabajo (horas pico) que son los días lunes, martes y miércoles en los horarios de 9 a 12 de la mañana y de 3 a 6 de la tarde de dichos días.

El servidor RADIUS es catalogado básicamente como Servidor de Autenticación aunque además funciona como DNS y Active Directory; por lo que los parámetros a ser medidos son:

ÁREA		PARÁMETROS DE EVALUACIÓN
Memoria	Física	▪ Bytes confirmados (asignados) en uso ▪ Mb disponibles
	Lógica	▪ Páginas por segundo
Red		▪ Total de bytes por segundo ▪ Longitud de la cola de salida ▪ Ancho de banda
Disco Lógico		▪ Espacio libre
Servidor		▪ Errores de permiso de acceso ▪ Errores del sistema ▪ Sesiones cerradas debido a un error

A continuación se presentan los valores obtenidos en promedio y los valores con los que deberían cumplir los parámetros medidos:

PARÁMETROS DE EVALUACIÓN	VALORES UMBRALES	SERVIDOR RADIUS	
		9 – 12 h	15 – 18 h
Bytes asignados en uso	Menor al 80%	22,64%	22,37 %
Páginas por segundo	Menor a 5 – deseado Mayor a 10 – cuello de botella Mayor o igual a 20 – sistema degradado	3	2

Total de bytes por segundo	70% de la interfaz	Client: 3504,50 Client_2: 0	Client: 2771,31 Client_2: 0
Longitud de la cola de salida	Menor a 2	Client: 0 Client_2: 0	Client: 0 Client_2: 0
Ancho de banda actual	Conexión de banda ancha	10 Mbps	10 Mbps
Espacio libre	Mayor al 15 %	90,05%	90,04%
Errores de permiso de acceso	0	153,78	162
Errores del sistema	0	0	0
Sesiones cerradas debido a un error	Menor al 1% de las sesiones activas	190,67	199

Interpretación de datos

Al analizar los valores obtenidos en promedio de cada parámetro en general se deduce que el Servidor RADIUS tiene un rendimiento aceptable para el tipo de función que desempeña.

- Los valores de Bytes asignados en uso están dentro del umbral permitido lo que indica que no existe problemas con el recurso, que en este caso es la memoria; por lo que el Servidor puede realizar las tareas que le han sido asignadas sin problemas de memoria.

- Con respecto al número de páginas por segundo se leen en promedio 3 pag/seg en la mañana y 2 pag/seg en la tarde, valores que están por debajo del umbral deseado que es de 5 pag/seg. Esto refuerza la conclusión emitida en el punto anterior, que el recurso memoria trabaja sin problemas.

- Los valores obtenidos en promedio para el Total de bytes por segundo que en la mañana es de 3504,5 B/seg y en la tarde es de 2771,3; no superan al valor umbral del 70% de la interfaz ya que cada interfaz de red permite transmitir un promedio de 11,92 MBps. Lo cual permite concluir que no existen problemas con este recurso; además se puede observar que solamente se usa una de ellas.

- El valor promedio de la longitud de la cola de salida es 0 el mismo que no supera al valor umbral lo que indica que no existen cuellos de botella presentes en el recurso red.

- La conexión de Internet es de banda ancha y es provisto por la UGI con un valor aproximado de 10 Mbps el mismo que es detectado por la interfaz de red que es de 10 Mbps.

- El porcentaje de espacio libre promedio es del 90% el mismo que está en el umbral permitido; lo cual indica que el recurso disco trabaja sin problemas.

- El promedio de los Errores de permiso de acceso tanto en la mañana como en la tarde superan al valor umbral establecido, lo que puede indicar que alguien está intentando tener acceso aleatoriamente a distintos archivos con el objeto de obtener acceso a información no debidamente protegida.

- El umbral del parámetro Errores del sistema es 0 lo que indica que el servidor no presenta problemas internos.

- Los valores promedio obtenidos para el parámetro Sesiones cerradas debido a un error superan el valor umbral tanto en la mañana como en la tarde, lo que indica puede existir un cuello de botella en el recurso servidor.

9. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Dado que la unidad se encuentra en un proceso de cambio los procedimientos y políticas de seguridad existentes se han categorizado como sencillos.

- No se puede llevar a cabo planes de seguridad debido a que tanto los auxiliares como los ayudantes de laboratorio son temporales, lo que no permite dar continuidad a los procesos de gestión de la organización.

- El actual proceso de modernización de los Centros de Gestión de TI de la universidad afecta a los planes establecidos para la unidad.

- Las seguridades físicas son una parte muy importante dentro de cada organización y deben ser gestionadas de forma adecuada a sus necesidades. En el Centro de Gestión de los Laboratorios DICC no se tienen un nivel aceptable en las seguridades de acceso.

- El área de los servidores no tiene la temperatura adecuada para su funcionamiento, debido a que no se cuenta con sistemas de ventilación ni de aire acondicionado.

- El nivel de acceso físico al servidor puede verse afectado y está relacionado con la temperatura en la que se encuentran los servidores ya que si se cierran todas las puertas, el calor sería mucho más elevado.

- El auxiliar de laboratorio encargado de administrar el Servidor RADIUS conoce y entiende bien su responsabilidad en el uso y gestión del servidor pero no cuenta con los mecanismos necesarios para apoyar el aseguramiento de la información que gestiona el servidor debido a que dicha información no es relevante.

- El servidor evaluado se encuentra en buenas condiciones, no presentó cuellos de botella graves en los días de medición que podrían afectar a su rendimiento. El servidor presenta un buen desempeño.

- Al realizar la evaluación de las seguridades se pudo observar que no se realizan pruebas de seguridad ni monitoreos frecuentes que permitan conocer el estado del Servidor.

- El actual incremento de los usuarios que acceden al servicio de Internet causan disminución de la velocidad de conexión ya que hasta el momento están registrados en el servidor RADIUS 300 usuarios.

- El aumento de ancho de banda que se ha pedido analizar a la UGI no se lo llevará acabo a corto plazo ya que se está implementando el servicio de Internet inalámbrico para todo el campus politécnico. Lo que conllevaría a la eliminación del Servidor RADIUS.

Recomendaciones

- Se deben establecer formalmente los planes y políticas de seguridad de manera que todos los integrantes del área conozcan y se apoyen en ellas para llevar a cabo una adecuada gestión de las Tecnologías de la Información.

- Las seguridades físicas deben ser reforzadas para que no haya el peligro de pérdida de los equipos, o de otra forma se deben establecer políticas de acceso que brinden mayor protección al área de los Laboratorios DICC.

- Se recomienda realizar pruebas y monitoreos de seguridad frecuentes para poder asegurar la continuidad del servicio de Internet. Por ejemplo, se puede realizar un escaneo de vulnerabilidades.

- Se recomienda además aprovechar de las ventajas que brinda el sistema operativo Windows Server 2003 como tal.

- Para evitar que el Centro de Gestión se caliente en demasía se recomienda gestionar la adquisición de un sistema de ventilación y de aire acondicionado.

- Se recomienda además la implementación de procesos para gestionar los incidentes de seguridad y la implantación de análisis de riesgos que permitan a futuro continuar y mejorar con el buen desempeño del servicio de Internet.

- Para evitar que haya más quejas sobre el servicio de Internet se sugiere dar a conocer a los usuarios las posibles causas de la baja capacidad de conexión.

- Se recomienda separar las funciones del Servidor RADIUS ya que no es conveniente que el servicio de DNS, DHCP y Active Directory estén en el mismo equipo que trabaja como servidor de Autenticación de Usuarios, de esta forma se protegería a la información que en ellos se registra.

10. REFERENCIAS

- Salas y Funciones de los Laboratorios DICC: http://www.epn.edu.ec/index.php?option=com_content&task=view&id=206&Itemid=455
- Recursos Hardware del Centro de Gestión: http://www.epn.edu.ec/index.php?option=com_content&task=view&id=764&Itemid=1036#gestion
- Recursos Software del Centro de Gestión: http://www.epn.edu.ec/index.php?option=com_content&task=view&id=765&Itemid=1037#software