**Universidad Nacional de Itapúa**

**Facultad de Ingeniería.**

**Informe**

**Auditoria Informática.**

**Fecha del Informe:** 14/04/2015.

## Nombre de la Entidad:   Universidad Nacional de Itapúa-Facultad de Ciencias y Tecnología.

**Lugar de la Auditoría**: Laboratorio de Informática.

**Fecha de Inicio de la Auditoría**:  08/04/2015

**Fecha de Finalización de la Auditoría**:  10/04/2015

AUDITORIA  DE  REDES DE COMPUTADORAS

1. **Marco Referencial**

**1.1 Introducción**

La auditoría informática a realizar en la Facultad de Ciencias y Tecnologías de la Universidad Nacional de Itapúa sede en Encarnación en el lugar del Laboratorio de informática que será en base a Cobit 5 donde ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

El marco de trabajo de Cobit se basa en el siguiente principio: Proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

Los principios y habilitadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

**1.2 La Información según COBIT 5**

* La Información constituye un Recurso Clave para todas las organizaciones.
* La Información se crea, usa, retiene, divulga y destruye.
* La Tecnología juega un Papel Clave en esas actividades.
* La Tecnología se está convirtiendo en parte integral de todos los aspectos de la vida personal y comercial.
  1. **Beneficios que arroja la información y la tecnología para las organizaciones**
* Mantener información de calidad para apoyar las decisiones del negocio.
* Generar un valor comercial de las inversiones habilitadas por la Tecnología de la Información (TI), o sea: lograr metas estratégicas y mejoras al negocio mediante el uso eficaz e innovador de la TI.
* Lograr una excelencia operativa mediante la aplicación eficiente y fiable de la tecnología.
* Mantener el riesgo relacionado con TI a niveles aceptables.
* Optimizar el costo de la tecnología y los servicios de TI.

**1.4 Los 5 Principios de COBIT 5:**

* Satisfacer las necesidades de las Partes Interesadas
* Cubrir la Compañía de Forma Integral
* Aplicar un solo Marco Integrado
* Habilitar un Enfoque Holístico
* Separar el Gobierno de la Administración

**1.5 Los Procesos Habilitadores de COBIT 5:**

Contiene una guía detallada de referencias a los procesos definidos en el Modelo de Referencia de Procesos de COBIT 5 que son las siguientes:

* Evaluar, Dirigir y Monitorear.
* Alinear, Planear y Organizar.
* Construir, Adquirir e Implementar.
* Entregar, Servir y dar soporte.
* Monitorear, Evaluar y Valorar.

1. **Plan de Auditoria**

**2.1 Alcance**

La auditoría se realizará en la Universidad Nacional de Itapúa, en la Facultad de Ciencias y Tecnologías del campus universitario con sede en Encarnación, específicamente en el Laboratorio de Informática donde se abarcará el análisis físico y lógico de la red LAN de computadoras interna del mencionado laboratorio. Así tambíén se auditará el convenio entre el departamento de Informática del Rectorado de la Universidad Nacional de Itapua para la virtualización de los servidores del Laboratorio.

El rango de tiempo en el que se realizará la auditoría es desde el 07 de abril hasta el 02 de junio del año 2015.

Todo esto se llevará a cabo con el fin de proporcionar un informe general y detallado donde se refleje los hallazgos descubiertos y las recomendaciones necesarias acerca de los resultados obtenidos.

**2.2 Objetivos**

* Analizar el cableado de la red LAN de computadoras del laboratorio para determinar si se cumple con el estándar ANSI/TIA/EIA-568.
* Verificar si el lugar donde se ubica la red de computadoras es apto y si cuenta con los requisitos mínimos de seguridad según las normas de control del estandar ISO/IEC 17799 ahora denominada ISO/IEC 27002.
* Determinar las políticas de red implementadas y si estas responden al estándar ISO/IEC 27002.
* Examinar las disposiciones y reglamentos que colaboren para el buen mantenimiento del laboratorio de informática**.**
* Recabar información sobre el convenio Cyt UNI para la virtualizacion de los servidores de CyT.

**2.3 Descripción de los Recursos**

**2.3.1 Donde se identifica los recursos cuya integridad puede estar amenazada**

* Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores, personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers.
* Software: Códigos fuente y objeto de aplicaciones, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, aplicaciones cliente-servidor.
* Información: En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos.
* Personas: Usuarios, operadores, administradores.
* Accesorios: Papel, cintas, tóners, CD´s.

**2.3.2 Se presenta a continuación los recursos que se van a utilizar para la presente auditoria.**

* Recursos Humanos:
  + Grupo de Auditoria:
    - Diego Rodríguez.
    - Rodrigo Fernández.
    - Pedro Giménez.
  + Encargados del lugar a Auditar:
    - Mary Carolina Cabral Franco (Encargada de la Sala de Informática).
    - Jesús Wilson Barrios Fretes (Auxiliar turno mañana).
    - Oscar Duarte (Auxiliar turno tarde).
* Hardware: Una Notebook, Smartphone.
* Accesorios: Cuaderno de Anotaciones, Bolígrafo.
* Software:
  + Microsoft Office Word
  + Gantt Project (Planificación del Proyecto)
  + Znmap (Para exploración de la red: servicios, escaneo de puertos abiertos, filtros de paquetes, etc).
  + TCPDump (Análisis de tráfico de la red).
* Estándares:
  + - Estándar COBIT 5.1.
    - EIA/TIA 568, ISO 27002.

**2.4 Análisis y Gestión de Riesgos**

Un riesgo es la probabilidad de que ocurra una contingencia o un daño en un proyecto que podría causar algún tipo de fracaso o impedir el éxito del mismo. Hablar de riesgos es hablar de futuro, de incertidumbre, de decisiones.

La identificación de riesgos en el plan del proyecto consiste en la determinación de las amenazas potenciales mediante la utilización de algún método consistente y estructurado; sin la correcta determinación de los mismos, no es posible desarrollar e implementar anticipadamente respuestas apropiadas a los problemas que puedan surgir en el proyecto.

**2.4.1 Análisis y prioridad de los riesgos**

El objetivo principal del análisis de riesgos es establecer las prioridades de la lista de los posibles riesgos que pondrían poner en juego el correcto funcionamiento del sistema y determinar cuál de ellos justifica la reserva de recursos para el planeamiento. Lo que nos permitirá visualizar el impacto que estos provocarían, si es no necesario mitigarlos, así como investigar las futuras mitigaciones y por sobre todo asignar prioridades a los riesgos permitiendo tratar en primer lugar los riesgos más importante del proyecto.

**2.4.2 Estimación de la probabilidad**

La probabilidad del riesgo es una medida que calcula la posibilidad de que la situación descripta en el apartado de consecuencias de los riesgos de la declaración de riesgos llegue a producirse de verdad.

Para cuantificar las posibles pérdidas y la incertidumbre acerca de la ocurrencia de los riesgos se emplearán las categorizaciones expresadas en lenguaje natural, en base a un rango de probabilidades establecido, como se muestra en la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| **Rango de probabilidad** | **Promedio para el calculo** | **Expresión de lenguaje natural** | **Valor numérico** |
| de 1% a 10% | 5 % | Baja | 1 |
| de 11 % a 25% | 18 % | Poco probable | 2 |
| de 26% a 55% | 40 % | Media | 3 |
| de 56% a 80% | 68 % | Altamente probable | 4 |
| de 81% a 99% | 90 % | Casi seguro | 5 |

**2.4.3 Estimación del impacto**

El impacto del riesgo calcula la gravedad de los efectos adversos, la magnitud de una pérdida o el costo potencial de la oportunidad si el riesgo llega a producirse dentro del proyecto.

Para el presente análisis se empleará la escala de medición subjetiva expresada en la siguiente tabla

|  |  |  |
| --- | --- | --- |
| **Criterio** | **Retraso en la planificación** | **Valor numérico** |
| Insignificante | 1 semana | 1 |
| Marginal | 2 semanas | 2 |
| Medio | 1 mes | 3 |
| Crítico | 2 meses | 4 |
| Catastrófico | Más de 2 meses | 5 |

**2.4.4 Exposición al riesgo.**

La exposición al riesgo calcula la amenaza general que supone el riesgo combinando la información que expresa la probabilidad de una pérdida real con información que indica la magnitud de la pérdida potencial en un único valor numérico.

Para el presente estudio la exposición al riesgo se calcula multiplicando la probabilidad de riesgo (en %) por el impacto (en valor numérico). Luego se utilizará la magnitud de la exposición al riesgo para clasificar los riesgos.

*Magnitud de exposición al riesgo:*

Aprox. 1 = bajo riesgo.

Aprox. 2 = riesgo medio.

Aprox. 3 = alto riesgo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Riesgo** | **Probabilidad** | **Impacto** | **Exposición** |
| RI- 01 | Catástrofes Naturales comunes en la zona (fuertes vientos, tormentas eléctricas, etc.) | 40% | 1 | 0.4 |
| RI- 02 | Información incorrecta de parte del encargado por desconocimiento de algunos temas | 40% | 1 | 0.4 |
| RI- 03 | Poca seguridad física en el laboratorio. | 68% | 4 | **2.72** |
| RI- 04 | No hay conexión de red LAN. | 18% | 1 | 0.18 |
| RI- 05 | Falla de uno o más equipos informáticos que sostienen la red (hub, switch, servidores, etc). | 18% | 3 | **0.54** |
| RI- 06 | Corte de energía eléctrica. | 18% | 1 | 0.18 |
| RI- 07 | Catástrofes Naturales poco comunes en la zona (deslizamiento de suelo, terremoto, etc.) | 5% | 1 | 0.05 |
| RI- 08 | El laboratorio no cuenta con servidor de respaldo | 90% | 4 | **3.6** |
| RI- 09 | Los backups no se realizan con regularidad | 40% | 3 | **1.2** |
| RI- 10 | La ISP deja de proporcionar los servicios. | 18% | 1 | 0.18 |
| RI- 11 | No cuentan con una planificación para gestionar riesgos | 90% | 3 | **2.7** |
| RI- 12 | No cuentan con una UPS de respaldo | 90% | 3 | **2.7** |
| RI- 13 | El bebedero se encuentra próximo al rack de servidores | 90% | 2 | **1.8** |

**2.5 Planificación**

**2.5.1 Cronograma de Actividades:**

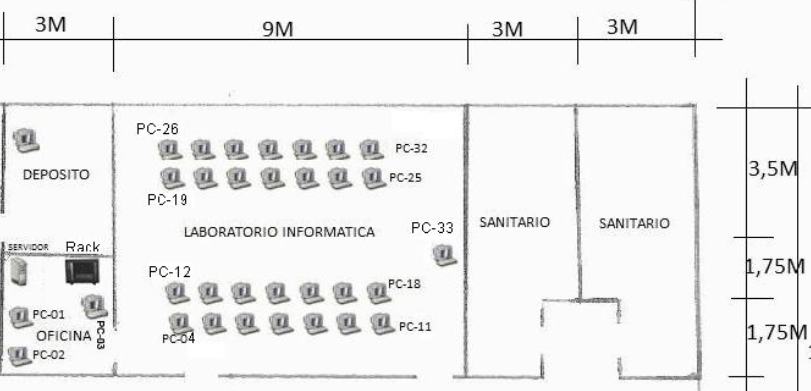
* Estudio Inicial del Entorno Auditable|
  + Visita a la entidad para obtener informaciones iniciales y presentación de los auditores.
  + Elaboración de la Solicitud de Auditoria.
  + Elaboración del cuestionario para la primera entrevista.
* Entrevista al encargado del Laboratorio de Informática (Jesús Wilson Barrios Fretes
* Elaboración del Proyecto
  + Definición del alcance y de los objetivos.
  + Redacción del Marco Referencial.
  + Determinación de los Recursos necesarios para realizar la auditoria.
  + Redacción del Análisis de Riesgos.
  + Elaboración del Plan de Auditoria.
* Desarrollo de la Auditoria.
  + Análisis Físico de la Red.
  + Revisión del Cuestionario para ANSI/TIA/EIA 568.
  + Verificar el cumplimiento de ANSI/TIA/EIA en la Seguridad física de la Red (Instalaciones de entrada, distribución de repartidor principal y secundario, distribución central de cableado, áreas de trabajo, etc.)
  + Redactar el Pre Informe de Auditoria.
  + Revisión de Cuestionario para ISO/IEC 27002.
  + Verificar el Cumplimiento de ISO/IEC 27002 de la Seguridad Física del Laboratorio (áreas seguras, controles de ingreso físico, protección contra amenazas internas y externas, ubicación y protección del equipo, etc. )
  + Redactar el Pre Informe de Auditoria.
* Análisis Lógico de la Red
  + Especificación de la actividad de prueba sustantiva.
  + Revisión del cuestionario de la prueba sustantiva de la red.
  + Verificar el cumplimiento de ISO/IEC 27002 Seguridad Lógica (Control de conexión a la red, transferencia de archivo, acceso a una aplicación, etc. ).
  + Redactar el Pre Informe de Auditoria.
  + Instalación y Comprobación del software necesario para pruebas sustantivas (Znmap, TCPdump, etc.)
  + Redactar el Pre Informe de Auditoria.
  + Redacción de cuestionario de cumplimiento del reglamento del laboratorio
  + Verificar el cumplimiento de los reglamentos del laboratorio
  + Redactar el Pre Informe de Auditoria.
* Convenio UNI CyT.
  + Redacción del Cuestionario de Convenio UNI CyT.
  + Revisión del Cuestionario de Convenio UNI CyT.
  + Redactar el Pre Informe de Auditoria.
* Revisión e informe
* Determinación del diagnóstico e implicancias.
* Elaboración de la carta de gerencia.
* Elaboración del borrador del informe.
* Elaboración final del informe.
* Presentación del informe final.

1. **Análisis y Obtención de Resultados**

# **3.1 Cuestionario de Auditoria según ANSI TIA EIA 568**

**3.1.1** ¿Se cuenta con una instalación de entrada? Se define como el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o dónde llegan las canalizaciones de interconexión con otros edificios de la misma corporación?.

(X) Si ( ) No

****

La instalación de entrada es la sala en la esquina inferior izquierda del plano. Sus dimensiones son 3 x 3.4 metros.

**3.1.2** ¿En la instalación de entrada se cuenta con dispositivos de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, y también equipos de telecomunicaciones?. Estas interfaces pueden incluir borneras (por ejemplo telefónicas) y equipos activos (por ejemplo modems).

(X) Si ( ) No

****

En la instalación de entrada ingresa un cable subterráneo de fibra óptica que provee de los servicios de internet a laboratorio y toda la facultad.

Hay un registro fuera del edificio para acceder al cable subterráneo (Imagen izquierda).

En la imagen derecha, debajo de las 2 cpu se nota un dispositivo por donde se conecta el servicio de internet por fibra óptica. En la base del rack de servidores hay un agujero en el piso, por donde entra el cable de fibra óptica y también por donde se distribuye la red a las máquinas del laboratorio.

**3.1.3** ¿Se cuenta con una sala de equipos?

(X) Si ( ) No

****

La instalación de entrada cumple el papel de sala de equipos. En esta sala también trabajan los 3 funcionarios del laboratorio de informática, por lo que también podría considerarse un área de trabajo.

**3.1.4** Los servicios prestados especificados en el punto 2. ¿Se encuentran en la sala de equipos?

(X) Si ( ) No

En una misma sala se cumple las funciones de área de trabajo, sala de equipos e instalación de entrada.

**3.1.5** ¿Se cuenta con un distribuidor o repartidor principal y secundario?

(X) Si ( ) No

# 

Esta es la vista cercana de los dispositivos que reparten la red, el dispositivo de arriba reparte la red por toda la facultad (repartidor principal) y el de abajo reparte la red al laboratorio (repartidor horizontal).

**3.1.6** El Distribuidor o repartidor principal y secundarios? Está ubicado en:

(X) La instalación de entrada (X) La sala de equipos

Una misma sala cumple las funciones de área de trabajo, sala de equipos e instalación de entrada.

**3.1.7** Se cuenta con distribuidores o repartidores horizontales?.

(X) Si ( ) No

Corresponde al dispositivo inferior de la imagen del punto 5.

**3.1.8** A los repartidores horizontales llegan los cables provenientes de las “áreas de trabajo”, el que también debe ser terminado en elementos de interconexión. adecuado. ¿Se cuentan con elementos de interconexión adecuados al fin mencionado?.

(X) Si ( ) No

Verificable en la imagen del punto 5. Son fichas RJ-45 para cables UTP5.

**3.1.9** ¿Se cuenta con una distribución horizontal de cableado? La distribución horizontal es la parte del cableado de telecomunicaciones que conecta las áreas de trabajo con los distribuidores o repartidores horizontales, ubicados en la sala de equipos o sala de telecomunicaciones.

(X) Si ( ) No

****

En la imagen se observa que el cableado horizontal que viene del repartidor desde la sala de equipos por debajo del piso y conecta a las máquinas del área de trabajo.

**3.1.10** El cableado horizontal ¿Cuenta con conectores de telecomunicaciones en las áreas de trabajo (dónde son terminados los cables de distribución horizontal)?.

( ) Si (X) No

**3.1.11** El cableado horizontal ¿Cuenta con terminaciones mecánicas?.

(X) Si ( ) No

Sus terminaciones son fichas RJ-45 que se conectan a las máquinas.

**3.1.12**. El cableado horizontal ¿Cuenta con cordones de en el área de trabajo o sala de telecomunicaciones?.

( ) Si (X) No

El cableado horizontal se conecta directamente al dispositivo repartidor. Imagen del punto 5.

**3.1.13** El cableado horizontal ¿Cuenta con puntos de consolidación?.

( ) Si (X) No

**3.1.14** El cableado de distribución horizontal debe seguir una topología del tipo “estrella”, con el centro en el área de trabajo o sala de telecomunicaciones, y los extremos en cada una de las áreas de trabajo ¿Se cumple el requerimiento?.

(X) Si ( ) No

Imagen del punto 5.

**3.1.15** Los conectores de telecomunicaciones en las áreas de trabajo deben ser conectados mediante un cable directamente al panel de interconexión ubicado en el armario de telecomunicaciones. No se admiten empalmes ni uniones, salvo en caso de existir un “punto de consolidación” ¿Se cumple el requerimiento?.

(X) Si ( ) No

No observamos ningún empalme. Imágen del punto 5.

**3.1.16** La distancia máxima para el cable de distribución horizontal es de 90 m, medida en el recorrido del cable, desde el conector de telecomunicaciones en el área de trabajo hasta el panel de interconexión en el armario de telecomunicaciones. ¿Se cumple el requerimiento?.

(X) Si ( ) No

**3.1.17** El cableado horizontal tiene una distancia inferior a los 40 metros

Los cordones de interconexión utilizados en las áreas de trabajo y en la sala de telecomunicaciones no deben ser más largos que 10 m en conjunto (completando una distancia de 100 m de “punta a punta”. Se recomienda que los cordones de interconexión en cada extremo no superen los 5 m ¿Se cumple el requerimiento?.

( ) Si (X) No

No se cuentan con cordones de interconexión.

**3.1.18** Cada área de trabajo debe estar equipada con un mínimo de 2 conectores de telecomunicaciones. Uno de ellos típicamente es asociado con servicios de “voz” y el otro con servicios de “datos”, aunque esta distinción puede de hecho no existir. ¿Se cumple el requerimiento?.

( ) Si (X) No

No se cuentan con conectores de telecomunicaciones.

**3.1.19** ¿Se cuenta con “Dispositivos de múltiples conectores de telecomunicaciones”?.

( ) Si (X) No

**3.1.20** ¿Se cumple con las medidas especificadas en la tabla anterior para los “Dispositivos de múltiples conectores de telecomunicaciones”?.

( ) Si ( ) No

No se cuenta con los dispositivos mencionados, por lo tanto no hay medidas a tener en cuenta.

**3.1.21** ¿Se cuenta con Áreas de Trabajo ?

(X) Si ( ) No



Se tiene el área de trabajo de los encargados del laboratorio (Imagen del punto 1) y el área de trabajo para los estudiantes de la facultad.

# **Hallazgos y Recomendaciones**

**4.1 Distribuidor o repartidor principal y secundario**

**4.1.1 Hallazgo**

El repartidor principal y secundario se encuentra en la misma sala que sería en la sala de equipos.

**4.1.2 Recomendación**

Según TIA EIA 568 se debería tener el repartidor principal en la sala de equipos y el repartidor secundario en la sala de telecomunicaciones.

**4.2 El cableado horizontal ¿Cuenta con cordones de interconexión en la sala de equipos.**

**4.2.1 Hallazgo**

El cable horizontal se conecta directamente al dispositivo repartidor y no cuentan con cordones de interconexión.

**4.2.2 Recomendación**

Según TIA EIA 568B se recomienda tener conectado al cableado horizontal un cordón de interconexión que facilidad de realizar cambios en la red al momento que se necesite, donde se puede conectar y desconectar los cables sin problemas.4.3 **El cableado horizontal ¿Cuenta con puntos de consolidación?.**

**4.3.1 Hallazgo**

No existe punto de consolidación dentro del cable horizontal.

**4.3.2 Recomendación**

Según TIA EIA 568B se recomienda tener punto de consolidación que permita, en caso de reubicaciones de oficinas (y por lo tanto de áreas de trabajo), re cablear únicamente parte del cableado horizontal (el que va desde el punto de consolidación hasta las nuevas áreas de trabajo).

**4.4 Cada área de trabajo debe estar equipada con un mínimo de 2 conectores de telecomunicaciones. Uno de ellos típicamente es asociado con servicios de “voz” y el otro con servicios de “datos”, aunque esta distinción puede de hecho no existir. ¿Se cumple el requerimiento?**

**4.4.1 Hallazgo**

No se cuentan con conectores de telecomunicaciones.

**4.4.2 Recomendación**

Según TIA EIA 568B se recomienda tener un dispositivo de conectores de

4.5 ¿**Se cuenta con “Dispositivos de múltiples conectores de telecomunicaciones” ?.**

**4.5.1 Hallazgo**

No se cuenta con dispositivos de múltiples conectores de telecomunicaciones

**4.5.2** **Recomendación**

Según TIA EIA 568 se recomienda tener un dispositivo de múltiples conectores de telecomunicaciones puesto que en él se podría conectar cables de tipo coaxial, par trenzado, fibra óptica dependiendo las necesidades en si del entorno.

**Conclusión**