

Universidad Nacional de Itapúa

Facultad de Ingeniería

Auditoria Informática

DOCUMENTACIÓN DE AUDITORIA

Lugar a Auditar: Sala de
Informática de la Facultad de
Ciencias y Tecnologías de la
Universidad Nacional de Itapúa.

Profesores:

- Dr. Horacio Kuna
- Ing. Andrea Romero

Integrantes:

- Diego Rodríguez
- Rodrigo Fernández
- Pedro Giménez

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.

La 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.

Objetivos

- ✓ Analizar el cableado de la red LAN de computadoras del laboratorio para determinar si se cumple con el estándar ANSI/TIA/EIA-568-A y B.
- ✓ 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.
- ✓ Examinar las disposiciones y reglamentos que colaboren para el buen mantenimiento del laboratorio de informática.
- ✓ Determinar las políticas de red implementadas y si estas responden al estándar ISO/IEC 27002.

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.

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.

Estimación de la probabilidad

La probabilidad del riesgo es una medida que calcula la posibilidad de que la situación descrita 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

En la siguiente tabla se expresan los riesgos identificados en la auditoria con las probabilidades estimadas subjetivamente para cada uno de ellos.

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

4.2.2 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

En la siguiente tabla se definen el impacto que producirían la ocurrencia de los riesgos citados anteriormente:

Riesgo	Impacto	Riesgo	Impacto
RI- 01	Insignificante	RI- 09	Medio
RI- 02	Insignificante	RI- 10	Insignificante
RI- 03	Crítico	RI- 11	Medio
RI- 04	Insignificante	RI- 12	Medio
RI- 05	Medio	RI- 13	Marginal
RI- 06	Insignificante		
RI- 07	Insignificante		
RI- 08	Crítico		

4.2.3 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