Universidad de Costa Rica
Sistema de Estudios de Postgrado

Auditoría de la gestión de la seguridad de redes de telecomunicación en la Universidad de Costa Rica.

Proyecto de trabajo final de Graduación
para optar al grado de Maestría
Posgrado en Auditoría de Tecnologías de Información

Ing. Francisco Lee Herrera

Ciudad Universitaria “Rodrigo Facio”,
Costa Rica, setiembre de 2007.

A mis padres y a mi hermana.

Agradezco:

A Dios por todas las personas que ha puesto en mi camino, a mis padres y a mi hermana por apoyarme durante estos años de estudio.

A mi compañera Gisela por todas las horas de trabajo y compañía; a Marycruz, Luis y Walter por la dedicación y el empeño dedicado a nuestros trabajos de grupo; a Carlos por ser excelente compañero de trabajo y de estudio.

A mis profesores, por compartir sus conocimientos, anécdotas y experiencia durante este proceso; al Máster Xiomar Delgado como tutor y al Lic. Manolo Córdoba por su amistad.

Al Máster Juan Diego Rojas Jiménez por brindarme su tiempo como lector académico de este trabajo y a los funcionarios y funcionarias del Centro de Informática de la Universidad de Costa Rica por la colaboración y confianza depositadas en mí, sin las cuales, la realización de mi proyecto no hubiera sido posible.

A Mariela y colaboradoras(es) por todo el esfuerzo y tiempo que han invertido en la Maestría y toda la ayuda que nos han dado.

A mis compañeros de trabajo César y Silvia por sus voces de aliento.

A Jorge por su apoyo, comentarios y ayuda como estudiante, ahora egresado de mi Maestría.

Tabla de contenidos

Marco teórico

Definiciones

¿Qué es la auditoría? Muchas definiciones se han escrito al respecto, sin embargo, la Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés) dice:

> *"La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes."*[1]

Enfocándose en el tema de redes concerniente a la investigación, éstas se han dividido en tres clases:

- **"Intranet":** Red interna de la empresa.
- **"Extranet":** Red externa pero directamente relacionada a la empresa.
- **"Internet":** La red de redes.

Uno de los problemas en estas implementaciones, entre varios, se relaciona con los puertos de estandarización pública de TCP/IP (protocolo de comunicaciones), por medio de los cuales puede entrar cualquier tercero para afectar la red o su flujo de información y; surgen así, una serie de riesgos que podrían impedir el cumplimiento de los objetivos de la organización y comprometer la información que administrada:

- Manejo inadecuado de la seguridad.

1 Normas Generales para la Auditoría de los Sistemas de Información.

- Insuficiencia de los programas para garantizar la seguridad.
- Protección inadecuada de la información.
- Fallas en la encriptación de los datos que viajan por la red.
- Carencias de implementación de seguridad que pueden degenerar en problemas de confidencialidad, integridad, no repudio y disponibilidad.

La auditoría de gestión de la seguridad de redes es entonces un estudio o una evaluación que permitirá a la administración conocer los riesgos presentes en la seguridad de las estructuras de telecomunicaciones y; brindará las recomendaciones para que se implementen los posibles controles para mitigar, o administrar los riesgos identificados y; así como verificar el funcionamiento de los controles existentes.

Justificación

Los cambios tecnológicos y el consecuente crecimiento en la instalación de la infraestructura de telecomunicaciones en la Universidad de Costa Rica; hace necesaria una gestión eficaz y eficiente en la seguridad, debido al volumen y al tipo de información que se administra en aplicaciones servidor – servidor y cliente - servidor.

Es en este punto que se plantea a la administración de tecnologías de información la necesidad de realizar una auditoría de la seguridad de redes, debido a la importancia de mantener la integridad, la disponibilidad, la confiabilidad de los datos y la información. Es importante hacer notar la actual carencia de

infraestructura para la realización de estudios de seguridad de redes en la Universidad de Costa Rica, por lo que este proyecto entregará valiosa información para su gestión.

Planificación de la auditoría

Objetivo general de auditoría

- Realizar una evaluación de la gestión de la seguridad de redes de la Universidad de Costa Rica para brindar a la administración el conocimiento de su estado actual, así como las recomendaciones que permitan su mejora.

Objetivos específicos de auditoría

1. Identificar los riesgos presentes en la gestión de la seguridad de redes para logar un mejor enfoque de la auditoría por realizar.
2. Verificar la existencia y la aplicación de políticas institucionales para el manejo de la seguridad de las redes.
3. Verificar la existencia y la aplicación de procedimientos para la gestión de la seguridad de redes en la Universidad.
4. Comprobar los niveles de acceso a diferentes funciones dentro de la red para verificar la correcta asignación de perfiles de los usuarios.
5. Evaluar el monitoreo que se realiza en las redes para establecer la suficiencia y pertinencia del mismo.
6. Verificar que están definidas las necesidades de sistemas de seguridad para “hardware” y “software”, flujo de energía, cableados locales y externos.
7. Verificar la aplicación de los sistemas de seguridad empleados en las redes lógicas y físicas.

8. Verificar la existencia y la aplicación de planes de pruebas de equipos como “routers”, “switches”, “firewalls” con el fin de evaluar la seguridad.
9. Evaluar al personal encargado de la seguridad de redes, esto con el propósito de verificar que recibe capacitaciones pertinentes con el objetivo de mejorar el desempeño en sus labores.

Alcance

La auditoría se desarrollará específicamente sobre la gestión de seguridad en la red roja en el campus universitario Rodrigo Facio (ver mapa en anexos).

Limitaciones

Para realizar la auditoría pueden existir limitaciones debido a la confidencialidad de cierta información, y disponibilidad del personal especializado en redes del Centro de Informática.

Metodología

Para realizar la auditoría se utilizarán:

- Entrevistas.
- Inspecciones oculares.
- Inspecciones lógicas mediante la utilización de aplicaciones especializadas.
- Revisión de documentos existentes.
- Revisión de estándares internacionales.
- Aplicación de cuestionarios (ver anexos).
- Análisis de la información recopilada.

Conocimiento preliminar de la organización

Visión

"La Visión del Centro de Informática es:

Ser el órgano rector universitario en el campo de las Tecnologías de Información y Comunicaciones, los servicios y aplicaciones institucionales que potencien a la institución hacia una posición de vanguardia y excelencia a nivel nacional e internacional en los campos de la docencia, investigación y acción social."

Misión

"La Misión del Centro de Informática es: Liderar los procesos técnicos y estratégicos de las Tecnologías de la Información y Comunicaciones en la Universidad de Costa Rica mediante las acciones rectoras necesarias que coadyuven al desarrollo e implementación de soluciones innovadoras y servicios apropiados de calidad y oportunos, que contribuyan a la eficiencia y eficacia del quehacer universitario con un personal comprometido, capacitado y experto, que selecciona y propicia la adopción y utilización de la mejor tecnología, de alianzas estratégicas y mejores prácticas de investigación permanente."

Valores Organizacionales

Los valores organizacionales del Centro de Informática son: compromiso, colaboración, dedicación, innovación, integridad, lealtad, liderazgo y respeto, los cuales proporcionan un sentido de dirección común para todo el personal y son los cimientos de la cultura organizacional que reflejan las metas, creencias, conceptos básicos de la organización y servicio al usuario. Los valores organizacionales se entenderán como:

- El compromiso, la obligación contraída de cumplir con los objetivos de una organización.
- La colaboración, la cooperación, contribución y participación con otras personas para lograr un objetivo.
- La dedicación, la actitud de brindarse a sus actividades con eficiencia y eficacia.
- La innovación, es esfuerzo por alterar el estado de las cosas, al introducir novedades y actuar proactivamente.
- La integridad, ser consistente, integrar los ideales, convicciones, normas, creencias con la conducta de sus acciones.
- La lealtad, demostrar fidelidad en las acciones y en el cumplimiento de las funciones.
- El liderazgo, conjunto de cualidades de personalidad y capacidad, que favorecen la guía y el control de otros.
- El respeto, la esencia y garantía de transparencia de las relaciones

humanas, del trabajo en equipo y decualquier relación interpersonal, que significa valorar a los demás y acatar la autoridad.

Modelo Organizacional por procesos del C.I.

El Centro de Informática es un promotor y facilitador de los servicios de tecnología en la Información y comunicaciones (TIC) en el ámbito institucional, a todas las unidades y entidades los cuales requieran de un servicio en las áreas que le competen. En consecuencia, la arquitectura de procesos y la estructura organizacional para un proveedor de servicios en TIC es altamente específica; representa un aspecto crítico para su eficiencia.

Se utilizará para el modelo organizacional del CI, uno que sustente una estructura que agrupe las áreas de proceso y procesos funcionales basados en el eTOM, y acorde con las características de un proveedor de servicios de esta índole.

Objetivos de la Red Telemática de la Universidad de Costa Rica (RedUCR)

El principal objetivo de la Red UCR es proveer un enlace de calidad, velocidad, confiabilidad, disponibilidad y seguridad aceptables, como medio para la transmisión de datos e información entre todas las unidades de la Universidad de Costa Rica, que incluye la Sede Central Rodrigo Facio, Ciudad de la Investigación (Finca 2), Sedes Regionales, Centros de Investigación Desconcentrados, etc.

Se utiliza la última tecnología en medios de transmisión, fibra óptica y cable UTP nivel 5, para lograr la calidad y velocidad. Se usan equipos cuya tecnología es también de avanzada en todos los puntos de interconexión, principalmente en aquellos considerados críticos (puntos de presencia -PdP-), que son soportados por equipo eléctrico de emergencia (UPS), para lograr la confiabilidad y disponibilidad.

Se han implementado dos redes lógicas sobre la red física. Una de ellas permite la interconexión y el acceso a los servicios de “Internet”, orientada a docentes, investigadores y estudiantes, su seguridad es mínima (Red Azul). La otra incluye una serie de modificaciones que minimicen los accesos no autorizados (Red Roja) para brindar seguridad aceptable en la transmisión de datos confidenciales, principalmente de carácter administrativo; es importante señalar que debido a esta condición, tal red será el objeto del presente estudio como se verá en los alcances posteriormente.

Una vez establecido el enlace citado, se pretende lograr otros dos objetivos:

- Poner a disposición de los universitarios, el acceso a los servicios de “Internet” de correo electrónico, acceso a bases y bancos de datos y, por otra parte, permitir que la Universidad ponga a disposición del resto del mundo, el resultado de sus investigaciones, estudios, y otros aspectos académicos.
- Permitir a la administración de la Universidad llevar a cabo sus planes de desconcentración de trámites sin poner en peligro la confidencialidad de los datos y la información, mediante un enlace

razonablemente seguro y confiable.

Identificación de riesgos para realizar la planificación

Se realizó la identificación de amenazas a la gestión de redes con el objetivo de determinar el mejor enfoque para la auditoría, los resultados se presentan a continuación:

Análisis de amenazas

	Recursos							
Amenazas	Equipos de red	Medios de comunicación	Servidores en red roja	Estaciones de trabajo en red roja	Mayor amenaza		Prob. ocurrencia	Amenaza + probable
Sabotaje	5	7	6	4	22		3	66
Acceso no autorizado.	4	6	6	8	24		4	96
Configuración deficiente de seguridad.	0	0	7	4	11		3	33
Deterioro.	7	7	8	4	26		7	182
Pérdida y/o alteración de la información.	7	0	9	6	22		4	88
Carencia de recursos financieros.	5	5	7	5	22		3	66
Carencia de procesos y políticas documentadas	8	7	5	5	25		9	225
Recurso más amenazado (suma columnas)	36	32	48	36				
Importancia relativa del recurso	6	6	8	4				
Recurso más vulnerable	216	192	384	144				

El valor en cada intersección se refiere a la evaluación del impacto de la amenaza sobre o debido al recurso

Recurso más amenazado: Servidores en red roja.

Mayores amenazas: Pérdida o alteración de la información y carencia de documentación

Recurso más vulnerable: Servidores en la red roja.

Programa de Auditoría Aplicado

Antecedentes

En la Universidad de Costa Rica se utiliza la última tecnología en medios de transmisión, fibra óptica y cable UTP nivel 5, para lograr calidad y velocidad del servicio.

Se usan equipos cuya tecnología es también de avanzada en todos los puntos de interconexión, principalmente en aquellos críticos (puntos de presencia -PdP-), que son soportados por equipo eléctrico de emergencia (UPS), para lograr confiabilidad y disponibilidad en los dispositivos de red.

Se han implementado dos redes lógicas sobre la red física. Una de ellas permite la interconexión y el acceso a los servicios de “Internet”, orientada a docentes, investigadores y estudiantes; su seguridad es mínima (Red Azul), la otra incluye una serie de modificaciones que minimizen los accesos no autorizados (Red Roja), con el fin de brindar seguridad aceptable en la transmisión de datos confidenciales, principalmente de carácter administrativo.

Objetivo general de auditoría

- Realizar una evaluación de la gestión de la seguridad de redes de la Universidad de Costa Rica con el propósito de brindar a la administración el conocimiento de su estado actual, así como las recomendaciones que permitan su mejora.

Objetivos específicos por cumplir.

1. Identificar los riesgos presentes en la gestión de la seguridad de redes para logar un mejor enfoque en la auditoría por realizar. Ver el análisis de amenazas en páginas anteriores.
2. Verificar la existencia y la aplicación de las políticas institucionales para el manejo de la seguridad de las redes.
3. Verificar la existencia y la aplicación de los procedimientos para la gestión de la seguridad de redes en la Universidad de Costa Rica.
4. Comprobar los niveles de acceso a las diferentes funciones dentro de la red para verificar la correcta asignación de perfiles de los usuarios.
5. Evaluar el monitoreo que se realiza en las redes para establecer la suficiencia y pertinencia del mismo.
6. Verificar que están definidas las necesidades de sistemas de seguridad

para “hardware” y “software”, flujo de energía, cableados locales y externos.

7. Verificar la aplicación de los sistemas de seguridad empleados en las redes lógicas y físicas.
8. Verificar la existencia y la aplicación de planes de pruebas de equipos como “routers”, “switches”, “firewalls” con el fin de evaluar la seguridad.
9. Evaluar al personal encargado de la seguridad de redes, esto con el propósito de verificar que recibe capacitaciones pertinentes para desempeñar sus labores.

Para cumplir cada uno de los objetivos de la auditoría propuestos, se debe realizar una serie de tareas expuestas en las páginas a continuación.

Objetivo 1

Identificar los riesgos presentes en la gestión de la seguridad de redes para logar un mejor enfoque en la auditoría por realizar. Ver el análisis de amenazas en páginas anteriores.

Este objetivo se desarrolló en la sección anterior, previo a la identificación de los objetivos siguientes.

Objetivo 2:

Verificar la existencia y la aplicación de las políticas institucionales para el manejo de la seguridad de las redes.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**18**	**07**	**07**	**18**	**07**	**07**	**2**	**3**	**+1**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
2.1		Documentación de políticas de seguridad	Verificar la existencia de políticas institucionales para la seguridad de las redes con el objetivo de garantizar la salvaguarda de la información de las aplicaciones institucionales, estas políticas deben estar: ● documentadas. ● aprobadas. ● publicadas. ● comunicadas. Solicitar una copia de dichas políticas	E1	
2.2		Revisión de las políticas de seguridad	Verificar si las políticas de seguridad son revisadas periódicamente y si se realizan cambios para asegurar: ● conveniencia. ● suficiencia. ● eficacia y ● continuación.		
2.3		Revisión de las políticas de seguridad	Verificar si las políticas de seguridad tienen asignado un encargado autorizado por la administración y además que sus funciones de revisión han sido claramente especificadas y documentadas.		
2.4		Revisión de las políticas de seguridad	Verificar si existen procedimientos documentados y autorizados para la revisión periódica de las políticas de seguridad.	E1	
2.5		Revisión de las políticas de seguridad	Verificar si la gerencia valida y autoriza las actualizaciones a las políticas.		

Objetivo 3:

Verificar la existencia y la aplicación de los procedimientos para la gestión de la seguridad de redes en la Universidad de Costa Rica.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**18**	**07**	**07**	**03**	**07**	**07**	**2**	**3**	**+1**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
3.1		Documentación de procedimientos operativos	Verificar si los procedimiento para la administración de la seguridad de redes están: ● documentados. ● autorizados. ● pertinentes. ● disponibles para los interesados.	E1	
3.2		Documentación de procedimientos operativos	Verificar si los procedimientos para la administración de redes son revisados y actualizados periódicamente. Verificar que toda actualización sea debidamente aprobada por la persona pertinente.		

Objetivo 4:

Comprobar los niveles de acceso a las diferentes funciones dentro de la red para verificar la correcta asignación de perfiles de los usuarios.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**18**	**07**	**07**	**03**	**07**	**07**	**2**	**3**	**+1**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
4.1		Política de control de acceso	Verificar la existencia de políticas documentadas para el control de acceso a los equipos de la red, estas políticas deben estar: ● documentadas. ● autorizadas. ● comunicadas. ● ser pertinentes. ● revisadas periódicamente.	E1	
4.2		Política de control de acceso	Verificar que tanto el acceso físico a los equipos como el acceso lógico están contemplados en dichas políticas.		
4.3		Registro de usuarios	Verificar si hay procedimientos formales para el registro y de-registro de usuarios con acceso a todos los equipos y servicios de redes.	E1	
4.4		Administración de privilegios	Verificar si la asignación y el uso de cualesquiera privilegios en el ambiente de redes es restringido y controlado es decir, los privilegios se asignan de acuerdo con la estricta necesidad del usuario base; los privilegios se asignan solamente después del proceso formal de la autorización.	E1	
4.5					

Objetivo 5:

Evaluar el monitoreo que se realiza en las redes para establecer la suficiencia y pertinencia del mismo.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
23	**07**	**07**	**25**	**07**	**07**	**03**	**07**	**07**	**1**	**1**	**0**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
5.1			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De un procedimiento para la revisión continua de los puertos de los equipos de red. ¿Quién es el encargado de revisar los puertos? ¿Que aplicaciones utilizan?	E1 PT1	
5.2			Verificar: ● Existencia documentada. ● Pertinencia. De bitácoras que contengan el resultado de las revisiones sobre los puertos de los equipos de red.	E1	
5.2			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De un procedimiento para la revisión continua del tráfico en la	E1	

			red. El procedimiento debe indicar los programas ejecutados, los intervalos de tiempo entre cada ejecución, cuáles reglas de trabajo se han implementado, quién se encarga de procesar los datos generados por ellos y cómo se actúa en consecuencia.		
5,3			Verificar la existencia documentada de bitácoras que contengan la información de incidentes referentes a sobrecargas de la red, puertos abiertos, transferencia de información en horarios no acostumbrados y otros.. Esta bitácora debería incluir la atención de dichos incidentes.	E1	

Objetivo 6

Verificar que están definidas las necesidades de sistemas de seguridad para “hardware” y “software”, flujo de energía, cableados locales y externos.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**18**	**07**	**07**	**03**	**07**	**07**	**2**	**3**	**+1**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
6,1			Verificar ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De estudios de necesidades de equipos, aplicaciones para seguridad de redes.		
6.2			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De estudios de factibilidad de equipos, aplicaciones para seguridad de redes.		
6.3			Verificar la existencia de un plan de revisión periódico de la infraestructura de redes, este debe estar documentado, ser pertinente, estar autorizado y comunicado a todos los involucrados.	PT2	

Objetivo 7:

Verificar la aplicación de los sistemas de seguridad empleados en las redes lógicas y físicas.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**27**	**07**	**07**	**03**	**07**	**07**	**4**	**6**	**+2**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
7,1			Además de las revisiones, verificar la existencia de controles establecidos para garantizar la seguridad de las redes. Preguntar acerca de los controles físicos y lógicos de las redes.	PT1 PT2 PT3	
			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De un procedimiento para la configuración de los equipos nuevos de red. ¿Quiénes son los encargados de llevar a cabo las instalaciones?	E1	

Objetivo 8:

Verificar la existencia y la aplicación de los planes de pruebas de equipos como “routers”, “switches”, “firewalls” para evaluar la seguridad.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
16	**07**	**07**	**27**	**07**	**07**	**03**	**07**	**07**	**2**	**3**	**+1**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
8,1			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De un plan de pruebas “in situ” de los equipos de red, el plan debe incluir cronogramas, encargados, pruebas que se realizan.		
8,2			Verificar: ● Existencia documentada. ● Pertinencia. De bitácoras resultantes de las pruebas realizadas.		

Objetivo 9:

Evaluar al personal encargado de la seguridad de redes para verificar que es capacitado para desempeñar sus labores.

Fecha de Inicio			Fecha de Terminación						Días Laborables		
			Estimado			Real			Estimado/hrs	Real/ hrs	Dif.
30	**07**	**07**	**3**	**08**	**07**	**3**	**08**	**07**	**2**	**2**	**0**

No.			PROCEDIMIENTO	Ref. P/T	FECHA
9,1			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De un plan para la capacitación de los funcionarios encargados de las redes. El plan debe indicar cronogramas, cursos, encargados de impartirlos.		
9,2			Verificar: ● Existencia documentada. ● Pertinencia. ● Autorización. ● Comunicación. De cursos de inducción para nuevos funcionarios.		
9,3			Averiguar sobre las últimas capacitaciones que se han impartido a los funcionarios de redes.		

Informe final y hallazgos

Auditoría de la gestión de la seguridad de redes de telecomunicación en la Universidad de Costa Rica

Informe a la Dirección

Señor.
Ing. Abel Brenes.
Director.
Centro de Informática.
Universidad de Costa Rica.

He auditado la gestión de las redes de la Universidad enfocando el estudio principalmente en la seguridad aplicada a la "red roja" de la Institución y, es mi responsabilidad, expresar una opinión sobre las situaciones encontradas que podrían afectar el cumplimiento de los objetivos y los servicios dentro de la organización.

La evaluación se basó principalmente en los criterios de COBIT 4.0 y la norma BSI 17799:2005. Los hallazgos presentes en este informe se sustentan con los resultados obtenidos de las pruebas selectivas, la obtención de evidencia tanto física como lógica y la evaluación dirigida a la gestión de las redes.

Considerando el importante proceso de reestructuración que atraviesa actualmente el Centro de Informática, es de suma importancia que la Dirección enfoque sus esfuerzos en la mejora de los aspectos expresados en los hallazgos adjuntos con este documento, de manera que, los cambios en la gestión de redes se realicen de forma efectiva.

Los factores que se debe mejorar son:

- La documentación de políticas y procedimientos para la administración de la seguridad de las redes de la Universidad de Costa Rica.
- El aseguramiento de los dispositivos de la red inalámbrica.
- Lo referente a la infraestructura física de la "red roja" principalmente en los edificios administrativos.

En mi opinión, la gestión de redes en la Universidad de Costa Rica se realiza eficaz y eficientemente, siendo muy importante para la institución la mejora de los aspectos antes mencionados.

Firma responsable:

_____
Ing. Francisco Lee Herrera.
Auditor.

TÍTULO	Hallazgo 1
Carencia de políticas documentadas y autorizadas para la administración de la RedUCR.	
CONDICIÓN	
Luego de entrevistas e investigar en el Consejo Universitario de la Universidad de Costa Rica, se determinó la carencia de políticas que establezcan los lineamientos para administrar la seguridad de la RedUCR.	
CRITERIO	COBIT 4.0, PO6.3 Administración de políticas para TI.
Según este criterio COBIT se debe: *"Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI"...*	
CAUSA	
La dirección tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. Anteriores administraciones han comunicado la necesidad de políticas, procedimientos y estándares de control, sin embargo, no se ha impulsado la aprobación de políticas para administrar la RedUCR.	
EFECTO	
Debido a la carencia de políticas autorizadas para la gestión de la RedUCR, la administración se ha hecho mediante prácticas informales por lo que, a este momento: • Las funciones y responsabilidades no están definidas formalmente. • Los aspectos que garanticen la calidad de la gestión no están claramente definidos. • Los controles establecidos para la seguridad de la información y la infraestructura de RedUCR no se encuentran formalmente respaldados. • Los encargados de la administración de RedUCR no pueden ejercer sus funciones dentro de un marco regulatorio institucional.	

RECOMENDACIÓN

Redactar y someter a la aprobación las políticas que respalden las estrategias de Tecnologías de Información.

"Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular."[2]

2 COBIT 4.0, PO6.3

TÍTULO	Hallazgo 2
Carencia de manuales y procedimientos documentados para la configuración de los equipos de red.	
CONDICIÓN	
Actualmente, no existen manuales de procedimientos para configurar la seguridad en los equipos de red. Los encargados del tema adquieren este conocimiento únicamente a través de capacitaciones y el trabajo cotidiano.	
CRITERIO	COBIT 4.0, AI4.4
Transferencia de conocimiento al personal de operaciones y soporte *"...La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario..."*	
CAUSA	
• Administraciones anteriores no han dado la importancia que se merece la documentación de procesos y manuales. • Carencia de tiempo. • Tradicionalmente, el conocimiento se ha transmitido a los nuevos funcionarios mediante capacitaciones o durante el quehacer diario.	
EFECTO	
El no poseer procedimientos documentados que estandaricen la correcta configuración de los equipos, podría tener, como consecuencia, la programación ineficaz de "routers", "switches" y otros; permitiéndose la entrada de virus, robo y modificación de información crítica de la Institución, así como grandes pérdidas económicas.	
RECOMENDACIÓN	
• Realizar un estudio de necesidades de documentación y generación de manuales para los equipos de red. • Crear y aprobar la documentación para la eficaz y la eficiente	

configuración de los dispositivos mencionados de acuerdo con las necesidades de la “red roja” institucional.

- Establecer un plan de revisión y actualización periódica de la documentación.

TÍTULO	
Posibilidad de atacar la red roja a través de la red inalámbrica institucional.	
CONDICIÓN	Hallazgo 3
Luego de realizar exitosamente pruebas de acceso a otros equipos en la red inalámbrica, se detectó carencia de seguridad en la misma. Durante las pruebas se comprobó la posibilidad de listar todos los ordenadores conectados, al ser de mayor gravedad poder insertar y extraer archivos hacia y desde varios de estos equipos.	
CRITERIO	COBIT 4.0, DS5.10
Seguridad de la red: *"Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, "firewalls", dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes."*	
CAUSA	
• Las técnicas implementadas para controlar los flujos de información así como los privilegios de acceso son deficientes. • Falta de procedimientos documentados para la configuración de equipos de red.	
EFECTO	
Un equipo no asegurado, con acceso inalámbrico (basta que posea una dirección "ip") y conectado a la "red roja" (mayoría de ordenadores portátiles en edificios administrativos) es un medio para insertar virus y otros programas maliciosos que podrían paralizar la operación de todos los equipos, así como el daño y el robo de información crítica de la Institución.	
RECOMENDACIÓN	
• Realizar un estudio de las necesidades de documentación y generación de manuales para los equipos de red inalámbrica. • Crear y aprobar la documentación para la eficaz y eficiente configuración	

de los dispositivos mencionados de acuerdo con las necesidades de la red inalámbrica institucional.

- Establecer un plan de revisión y actualización periódica de la documentación.
- Revisar y corregir la configuración de seguridad de los equipos de la red inalámbrica institucional para impedir el acceso y la visualización entre los ordenadores conectados a la misma.

TÍTULO	Hallazgo 4
Carencia de revisiones periódicas para detectar equipos inalámbricos conectados sin autorización a la red roja.	
CONDICIÓN	
Se carece de un procedimiento para la revisión periódica en los edificios administrativos y otros con el objetivo de detectar dispositivos inalámbricos conectados a la red roja de la Universidad.	
CRITERIO	
Características Técnicas recomendadas de los equipos para redes inalámbricas. La nota a continuación se obtuvo de http://ci.ucr.ac.cr/index.php?id=61: *"Nota: Por razones de Seguridad Informática, **no se autoriza** la instalación de equipos inalámbricos en la Intranet (Red Roja)."*	
CAUSA	
La cantidad de trabajo cotidiano en la atención de otras tareas propias de la gestión de redes ha hecho difícil la documentación y ejecución de un procedimiento para detectar dispositivos no autorizados conectados a la red roja.	
EFECTO	
Equipos inalámbricos no asegurados, conectados a la "red roja" pueden ocasionar introducción de virus, acceso a la información confidencial, así como la pérdida y manipulación de datos críticos de la Universidad.	
RECOMENDACIÓN	
• Establecer y ejecutar un plan para la revisión periódica de edificios administrativos y puntos de acceso a la "red roja" con el objetivo de detectar redes inalámbricas no autorizadas.	

Título	Hallazgo 5
Visible deterioro de la infraestructura que protege el cableado de red.	
Condición	
En edificios administrativos, específicamente en los niveles de alto tránsito de estudiantes y personas ajenas a la Universidad, existe cableado para el transporte de datos sobre y, por debajo del cielo raso, expuesto y sin protección contra posibles daños físicos.	
CRITERIO	
Tomado del documento CI-ADR-R-073, *"Especificaciones Técnicas para Instalación de Cableado Estructurado."* *"Cuando se indiquen canalizaciones superficiales en paredes, cielo rasos (de no ser posible el uso de canasta metálica) serán de tipo ducto plástico..."* *"...No se permitirá bajo ninguna circunstancia el utilizar las paredes de concreto, fibrolit, madera o metal como parte de la canalización."*	
Causa	
• Cuando se ensambló el tendido del cableado para la transferencia de datos, no se aplicaron las normas para el cableado estructurado. • Deterioro de la infraestructura que "protege" el cableado.	
Efecto	
La reposición del cableado, debido a un eventual daño, implicaría un alto costo en tiempo y dinero debido a que se debe reemplazar todo el cable dañado.	
Recomendación	
• Realizar una estudio para identificar las mejores soluciones de acuerdo con las Especificaciones Técnicas para Instalación de Cableado Estructurado publicado por el Centro de Informática que permitan proteger el tendido en los puntos vulnerables detectados. • Una vez realizado y aprobado el estudio, ejecutar las acciones recomendadas en el mismo a la brevedad posible.	

Bibliografía

Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información. *Normas Generales para la Auditoría de los Sistemas de Información.* [en línea]. Publicado en línea por el Information Systems Audit and Control Association ISACA. [Estados Unidos de Norteamérica]: Disponible en: http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/ContentManagement/ContentDisplay.cfm&ContentID=19227

International Organization for Standardization (ISO); *International Electrotechnical. Commission (IEC). Information technology — Security techniques — Code of practice for information security management.* Estados Unidos de Norteamérica, 2005.

IT Governance Institute. *Control Objectives for Information and Related Technology (CobiT).* [en línea]. Versión 4.0. [Estados Unidos de Norteamérica]: IT Governance Institute, 2006 [citado en agosto de 2007]. ISBN: 1-933284-37-4. Disponible en formato PDF en:

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf

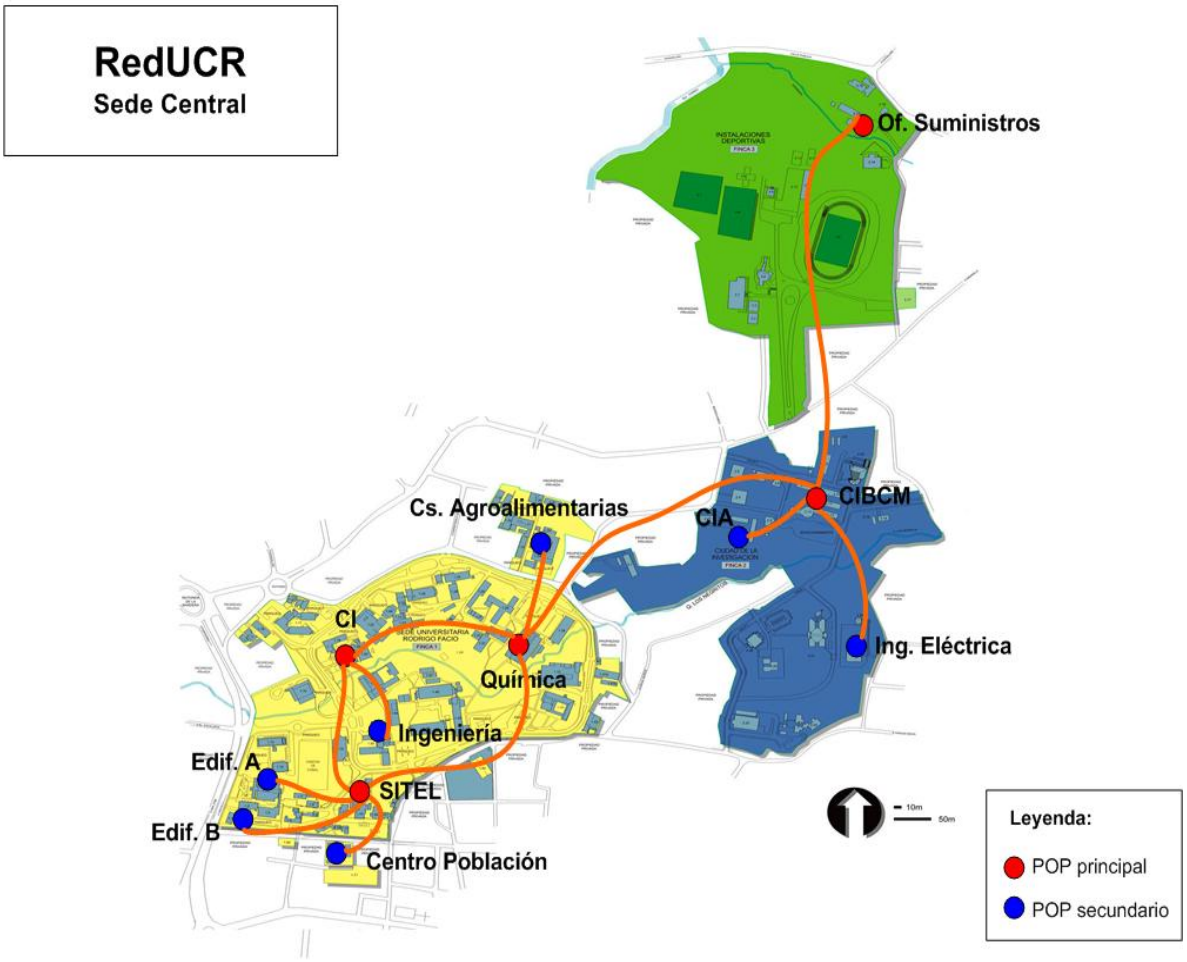
IT Governance Institute; Office of Government Commerce;The IT Service Management Forum. *Aligning COBIT, ITIL and ISO 17799 for Business Benefit.* [en línea]. Publicado en línea por las tres organizaciones. [Estados Unidos de Norteamérica]: Disponible en formato PDF en http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=32757

Espinoza, Jeans y otros. *Especificaciones Técnicas para Instalación de Cableado Estructurado.* [en línea]. Versión 1.0. [San José, Costa Rica]: Centro de Informática, Universidad de Costa Rica, marzo 2007 [citado en agosto de 2007]. Disponible en formato DOC en http://ci.ucr.ac.cr/fileadmin/templates/CI/documentos/estandares/RedUCR/3.Procedimientos/CI-ADR-R-073_Instalacion_de_Cableado_Estructurado.doc

Piattini, Mario; Del Peso, Mario. *Auditoría Informática. Un enfoque práctico. 2da Edición ampliada y revisada.* México D.F.: Alfaomega Ra-Ma, 2001. ISBN: 970-15-0731-2.

Anexos

Distribución geográfica del “backbone” principal de la Sede Central de la Universidad de Costa Rica.



Auditoría de la gestión de la seguridad de redes de telecomunicación en la Universidad de Costa Rica. *Auditor: Ing. Francisco Lee Herrera* *Cuestionario para conocimiento preliminar de la gestión de redes en la Universidad*	**C1**

Este cuestionario tiene como objetivo dar una idea muy general de la gestión de las redes en la UCR para luego enfocar la planificación de la auditoría sobre la base de objetivos, metas, políticas, estándares tanto de la Universidad como internacionales que se utilicen para tal efecto.

Entrevistad@:	Lugar de la entrevista:	Fecha:	Hora:

- ¿Cuenta la unidad con una misión, visión, objetivos establecidos? (solicitar una copia de los mismos).
- ¿Existen políticas para la administración de las redes de telecomunicación tanto general como de seguridad? (de existir, solicitar un a copia).
- ¿Utilizan estándares internacionales para la gestión de redes en general y en lo referente a seguridad? (Listar cuáles)
- Planes operativos (solicitar una copia)
- Existe análisis de riesgos para la gestión de redes?
- ¿Cuántos funcionarios están dedicados a la administración de redes?
- ¿Cuál es el área geográfica de actuación de la unidad?
- ¿Existen planes de capacitación para el personal de redes?
- ¿Cuál es la cobertura geográfica de la red roja?
- ¿Qué instancias utilizan la red roja?
- ¿Qué aplicaciones se utilizan sobre la red roja?
- ¿Se encuentra registrados los puntos de acceso a la red roja? (solicitar una copia de dichos puntos)
- ¿Cuáles son los criterios técnicos y administrativos utilizados para formar parte de la red roja?