



UNIVERSIDAD NACIONAL DE INGENIERÍA

Recinto Universitario “Simón Bolívar”

Facultad de Electrotecnia y Computación

**Auditoría de red en la Universidad Nacional Agraria sede Managua
aplicando el Marco de Gobierno de las Tecnologías de Información
“Cobit”**

TRABAJO MONOGRÁFICO

Para optar al Título de
Ingeniero en Computación

Presentado por:

Br. Engels Mijaíl Estrada López

Tutor:

MSc. María Lourdes Montes

Managua, Nicaragua

Enero del 2016

DEDICATORIA

Trabajo monográfico dedicado a Dios, el Eterno Padre, por darme la oportunidad de vida, las fuerzas y los medios necesarios para continuar mi formación como profesional, siendo un apoyo incondicional en cada etapa de mi existencia terrenal y una luz para iluminar mi entendimiento. Sin Él ningún esfuerzo hubiese valido la pena.

A mi madre: Jacqueline López Martínez, cuyo ejemplo, amor y motivación fueron el eslabón primordial para cumplir mis metas. Su creencia en mí ha sido el impulso para llegar a ser un Ingeniero y mejor persona.

Dedicado también al resto de mi familia, que en algún momento de mis estudios fueron pilares de apoyo para continuar con el objetivo de obtener el título de la carrera. No es posible mencionar a todos, pero queda grabado en mi memoria los actos de bondad incondicional hacia mí. Estaré eternamente agradecido por ello.

Finalmente, a todos mis docentes que influyeron con sus lecciones y experiencias en formarme y prepararme para los diferentes retos que nos pone la vida. Y a mis amigos que desde el inicio de mi etapa en la Universidad demostraron, con sinceridad, ser los mejores exponentes de la correcta definición de amistad.

A todos ustedes éste esfuerzo es dedicado.

AGRADECIMIENTO

Agradezco infinitamente al Gran Dios Eterno por la oportunidad de vida y ser el motor de fuerzas que me han impulsado a superarme académicamente y como persona; gracias doy por proveerme de todo lo esencial para cumplir logros y seguir adelante.

Con profundo sentimiento agradezco a mi Madre por el amor, ánimo y apoyo que me ha brindado desde el primer día de vida, cuyo esfuerzo ha valido tanto para que yo pueda salir adelante. Gracias por hacer posible este triunfo de llegar a ser un Ingeniero.

Al resto de mi familia y amigos que de alguna manera contribuyeron a que culminara con mi carrera y obtuviera el título de Ingeniero en Computación; gracias por el ánimo, apoyo y las más sinceras muestras de fraternidad incondicional.

A mi tutora y amiga MSc. María Lourdes Montes por toda su valiosa colaboración en la realización de esta tesis, gracias por guiarme en todo el proceso de elaboración de ésta monografía. Agradecimiento perpetuo por transmitir de su sabiduría en el desarrollo de mi formación académica.

A mis Docentes y Mentores que sin duda sus conocimientos y experiencias de vida me ayudaron a superarme en las diferentes fases de las carreras. Sus consejos quedarán atesorados en mi mente y corazón para siempre.

Gratitud especial a los Directivos de OTIC-UNA por permitirme llevar a efecto la realización de esta auditoría. Gracias por todo el tiempo que me dieron y la paciencia de brindarme la información necesaria para concluir con la auditoría informática. Sus ayudas fueron invaluable.

Tabla de contenido

Resumen	VI
I. Introducción.....	1
II. Objetivos	2
Objetivo General.....	2
Objetivo Específico	2
III. Justificación	3
IV. Marco Teórico	4
4.1. Generalidades Auditoría Informática	4
4.2. Objetivos de la Auditoría Informática.....	5
4.3. Control Interno Informática	5
a. Controles Preventivos	6
b. Controles de Detección	6
c. Controles Correctivos.....	7
4.4. Procedimientos Generales de Auditoría Informática	7
4.5. Recopilación de Información	8
a. Entrevistas.....	8
b. Encuestas.....	8
c. Revisión Documental.....	8
4.6. Análisis de Riesgos	8
4.7. Metodología de Auditoría Informática.....	9
4.8. Tipos de Auditoría Informática.....	9
4.9. Auditoría de Redes.....	10
a. Auditoría de la Red Física	10
b. Auditoría de la Red Lógica	11
4.10. Vulnerabilidad en Redes	11
4.11. Cobit.....	12
4.11.1. Procesos y Controles de Cobit.....	14
4.11.2. Objetivos de Control para Auditoría de Red.....	14
4.11.3. Modelos de Madurez de Cobit	15
4.11.4. Justificación del Modelo de Referencia Cobit 4.1	17
V. Análisis y Presentación de Resultados.....	18
5.1. Metodología.....	18

5.2.	Desarrollo del Tema	19
5.2.1	Generalidades de la Institución.....	19
5.2.1.1.	Misión	20
5.2.1.2.	Visión.....	20
5.2.2.	Riesgos de la Implementación de la Auditoría	21
5.2.2	Aplicación de Cobit	23
PO1	Definir un Plan Estratégico de TI	23
PO3	Determinar la Dirección Tecnológica	26
PO5	Administrar la Inversión de TI	29
PO8	Administrar la Calidad.....	32
PO9	Evaluar y Administrar los Riesgos de TI	35
PO10	Administrar Proyectos.....	39
AI3	Adquirir y Mantener Infraestructuras Tecnológicas	42
AI4	Facilitar la Operación y el Uso.....	45
AI5	Adquirir Recursos de TI.....	48
AI6	Administrar Cambios	51
DS1	Definir y Administrar los Niveles de Servicio.....	54
DS2	Administrar los Servicios de Terceros.....	57
DS3	Administrar el Desempeño y la Capacidad	60
DS4	Garantizar la Continuidad del Servicio	64
DS5	Garantizar la Seguridad de los Sistemas	67
DS9	Administrar la Configuración	70
DS12	Administración del Ambiente Físico	74
DS13	Administración de Operaciones	77
ME1	Monitorear y Evaluar el Desempeño de TI	80
VI.	Conclusiones	83
VII.	Recomendaciones.....	84
VIII.	Glosario de Términos.....	85
IX.	Bibliografía.....	89
X.	Anexos	90
Anexo 1.	Objetivos de Control de Cobit.....	i
Anexo 2.	Modelo Genérico de Madurez.....	vii

Anexo 3.	Niveles de Madurez de la UNA.....	viii
Anexo 4.	Encuesta a los usuarios.....	ix
Anexo 5.	Evidencias de Auditoría.....	x
Anexo 6.	Ejemplo de Cuestionarios Meycor Cobit.....	xv
Anexo 7.	Ejemplo de Formulario de Evaluación.....	xxi

Tabla 1: Riesgos de la Auditoría de redes - UNA	22
---	----

Resumen

El presente proyecto monográfico contempla la aplicación de una Auditoría de red en la Universidad Nacional Agraria, sede Managua, aplicando el marco de gobierno de las Tecnologías de la Información Cobit¹. A partir de un análisis en la situación actual de la infraestructura física y lógica de la red de Computadoras en la Universidad, se desarrolló un análisis de riesgos cuyo enfoque está orientado a la aplicación de los procesos de auditoría.

Metodológicamente, la auditoría de red fue realizada bajo un enfoque investigativo cualitativo, tomando como base los recursos de TI identificados, se procedió a determinar las directrices iniciales del proyecto y el alcance de la auditoría, se seleccionaron los procesos de COBIT relacionados con la Auditoría de Redes, los que posteriormente fueron analizados y evaluados en base al documento: Directrices de Auditoría COBIT. Se empleó la observación y se aplicó una serie de encuestas al personal y usuarios del servicio de Red, para llegar a los resultados mostrados en este documento.

Finalmente al concluir este trabajo monográfico, se obtuvo como resultado un informe final que muestra los resultados obtenidos mediante la ejecución del plan de auditoría, en el que se muestran los hallazgos y recomendaciones que servirán a la empresa para evaluar la eficiencia de dicha área, para beneficiar tanto a la universidad, como a los usuarios de la red.

¹ Objetivos de Control para Información y Tecnologías Relacionadas, en lo sucesivo referido simplemente Cobit



I. Introducción

El escrito que se presenta a continuación tiene un carácter monográfico donde plantea la ejecución de una auditoría a la red física y lógica de la Universidad Nacional Agraria, sede Managua, ubicada en el km 12 carretera Panamericana norte; institución que se dedica a la enseñanza educativa e investigación científica en el campo agropecuario. La Universidad como parte de su crecimiento hace uso de las Tecnologías de la Información y Comunicación (TIC) para sistematizar los procesos académicos y administrativos con el fin de brindar un servicio de calidad los usuarios de la red de datos.

Actualmente, es de su interés evaluar los controles establecidos en el área de las redes de computadoras, para corroborar si cumplen con los objetivos de control de las mejores prácticas de Cobit.

Por lo antes planteado, el presente trabajo monográfico tiene como finalidad realizar el proceso de auditoría de redes de computadoras (a la estructura física y lógica) en la UNA con el propósito de evaluar su funcionamiento, verificar el cumplimiento de las normas que rigen dicha área, e identificar en qué casos los controles son suficientes o qué procesos requieren ser mejorados, para posteriormente emitir las recomendaciones pertinentes a los hallazgos encontrados. Estas recomendaciones deberán ser tomadas en cuenta por la Universidad con el fin de mejorar las debilidades obtenidas, que de ser acatadas, garantizarán una utilización más eficiente y segura de la información, mejorando la toma de decisiones.

Para efectos del presente documento se ha realizado un acápite de definiciones y glosario de términos que ayudan en la aclaración de cualquier duda conceptual que pueda surgir en el momento de la lectura del documento.



II. Objetivos

Objetivo General

Realizar una Auditoria de Red de computadoras en la estructura física y lógica, en la Universidad Nacional Agraria - sede Managua - utilizando el estándar internacional COBIT a fin de identificar su estado actual y emitir recomendaciones necesarias que permitan a la institución mejorar su infraestructura.

Objetivos específicos

1. Analizar la gerencia de redes, a fin determinar que su función de gestión esté claramente definida.
2. Verificar que las actividades de control de la red de computadoras determinen el cumplimiento de normas internacionales de estandarización en los mecanismos de hardware e instalación de la misma.
3. Investigar las medidas de protección de la información y procesos de la red de computadoras.
4. Efectuar un informe final de auditoría informática que contenga la evaluación de los elementos auditados, así como las recomendaciones aplicables para la estandarización y mejora de la estructura y procesos de red.



III. Justificación

La auditoría de Red de la Universidad Nacional Agraria sede Managua aplicando el Marco de Gobierno de las Tecnologías de Información Cobit, se realizará para verificar si tienen establecidos los controles suficientes en su red y emitir recomendaciones que le permitan a la institución mejorar su infraestructura de Red, de manera que puedan posteriormente contar con una infraestructura de red, con bases sólidas, que garantice la seguridad, integridad, confidencialidad y confiabilidad de la información que comparten y mejore la toma de decisiones dentro de la universidad.

Por lo antes planteado, el proceso de auditoría de red, que suplirá a través de los hallazgos encontrados, las recomendaciones pertinentes con datos específicos de aspectos a mejorar y modelos a seguir, fundamentados en una norma internacional de buenas prácticas.

El proceso de auditoría que se llevará a cabo, estará basado en la revisión de los objetivos de control de los procesos de Cobit que tienen relación directa con las Redes Informáticas, tomando como referencia las Directrices de Auditoría de Cobit, que proporcionan asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los objetivos detallados de control.

El resultado de este trabajo monográfico se va a canalizar a las autoridades competentes, que son quienes van a garantizar el seguimiento de las recomendaciones.



IV. Marco Teórico

Dentro de esta sección se hará un análisis teórico sobre auditoría, su definición, sus objetivos, importancia, metodología, entre otros elementos necesarios para la comprensión de lo que se abordará durante el proceso de realización de la monografía.

4.1 Generalidades Auditoría Informática

Conceptualmente la auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas (Piattini & Del Peso, 2001, pág. 4).

En el caso de estudio que se despliega en éste documento nos limitaremos a desarrollar el tema entorno a la auditoría informática preparada para la ejecución dentro de la Universidad Nacional Agraria. La definición se describe de la siguiente forma: “proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos” (Piattini & Del Peso, 2001, págs. 28-29).

Por otro lado, Alonso Rivas, define en su libro la auditoría informática de la siguiente manera: “es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficiencia y la rentabilidad del servicio, o del sistema, que resultan auditados” (Alonso Rivas, 1988, págs. 39-40).

Se debe tener en cuenta que la auditoría no es una actividad meramente mecánica que conlleve a aplicar procedimientos para adquirir resultados; por el contrario, demanda un criterio profesional, sólido y sensato para dictaminar



los procedimientos que deben de seguirse con el fin de estimar los resultados logrados (Canales Mena, 2006).

4.2 Objetivos de la Auditoría Informática

El principal objetivo de la Auditoría Informática es recomendar a la Administración de una empresa en el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, comentarios y recomendaciones relacionados con las actividades del procesamiento de la información.

4.3 Control Interno Informático

“Actualmente el concepto de control interno es de vital importancia para las empresas, hacen fuertes exigencias para mejorar el control de las empresas que dirigen” (Mosquera Vizuete, 2006).

El control interno informático permite controlar las actividades de los sistemas de información cumpliendo procedimientos, estándares y normas fijadas por la administración de las empresas, así como los requerimientos legales.

Con el control interno informático las empresas se aseguran de que las medidas que se obtienen de los mecanismos implantados sean correctas y válidas.

Como principales objetivos podemos citar:

- ★ Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijadas, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- ★ Asesorar sobre el conocimiento de las normas.
- ★ Colaborar y apoyar el trabajo de la Auditoría Informática.
- ★ Definir, implantar y ejecutar mecanismos y controles para comprobar el logro del servicio informático.



Según Emilio del Peso señala “Los controles cuando se diseñen, desarrollen o implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto último habrá que analizar el coste-riesgo de su implementación” (Del Peso Navarro & Piattini, 2003, págs. 28-30).

Ante cualquier amenaza a la que está expuesta una organización existe un riesgo que puede impedir o va en contra de lograr los objetivos propuestos. Toda actividad genera riesgo, el no tener riesgos, implica no ejecutar la actividad, para cada actividad se generan prácticas de control que permitirán evitar los riesgos variando ampliamente en su efectividad y eficiencia.

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y qué eventos no deseables o riesgos serán prevenidos o detectados y corregidos mediante controles establecidos (Mosquera Vizuite, 2006).

Los controles informáticos pueden ser preventivos, de detección o correctivos.

a. Controles Preventivos

Estos controles operan en las primeras etapas del flujo del proceso a fin de prevenir la ocurrencia del error o riesgo. Con estos controles se atacan a las causas del riesgo.

b. Controles de Detección

Siguen los controles preventivos y están diseñados para captar errores que escapen a los controles preventivos. Estos controles apuntan a la forma de ocurrencia del riesgo.

En otras palabras, son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos, son los más importantes ya que sirven para evaluar la eficiencia de los controles preventivos.



c. Controles Correctivos

Aseguran que los efectos de errores o fraudes detectados se corrijan o disminuyan. Normalmente se piensa que los controles correctivos son parte inherente de los controles de detección, pero muy frecuentemente se encuentran controles de detección funcionando sin el correctivo complementario.

Los procesos de negocios que se llevan a cabo dentro las unidades de una empresa, se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. El control que provee la auditoría es parte de dichos procesos y está integrado el ellos, permitiendo su funcionamiento adecuado y supervisando su comportamiento y aplicabilidad en cada momento, con lo que, constituye una herramienta útil para la gestión, pero no sustituto de ésta (Espinola, 2007).

4.4 Procedimientos generales de Auditoría Informática

Para los autores de “Auditoría Informática: un enfoque práctico” (Piattini & Del Peso, 2001) se establecen normas y procedimientos dentro de la auditoría que se resumen de la siguiente forma:

- ★ El trabajo se planificará apropiadamente y se supervisará adecuadamente.
- ★ Se estudiará y evaluará el sistema de control interno.
- ★ Se obtendrá evidencias suficiente y adecuada.

Como toda auditoría, se lleva a cabo en 3 fases generales denominada planeación, ejecución (trabajo de campo) y comunicación de resultados (informes); en cada una de esas fases se ejecutan una serie de actividades, labores y tareas de acuerdo al área de auditoria y sus respectivos objetivos de control (Controlaría General de la República, 2009, pág. 5).



4.5 Recopilación de información

Para llevar a cabo la auditoria de red en la UNA, es imprescindible contar con herramientas para la recopilación de la información, motivo por el cual se ha decidido utilizar las siguientes:

a. Entrevistas

Se preparará un formato de entrevista para formular diversas preguntas al personal seleccionado de la UNA, que permita conocer su opinión sobre la funcionalidad y condición física de la red y sus componentes, así como, la infraestructura de ubicación de los equipos y las políticas bajo las que se rige.

b. Encuestas

Se utilizaran para conocer las posibles debilidades de la red de la UNA en cuanto a su funcionamiento.

c. Revisión documental

Se verificará la existencia de documentos, tales como, políticas de seguridad y plan de contingencias; así como, sus actualizaciones según los cambios que se realicen.

4.6 Análisis de Riesgos

Se debe determinar el impacto que para cada riesgo tienen los diferentes controles existentes en la aplicación. De esta manera puede concluir sobre áreas donde hay deficiencias de control o en otras palabras, áreas donde los riesgos reales son altos.

Los controles de riesgos se evalúan de acuerdo al tipo de impacto sea este bajo, medio y alto. Si el control es preventivo apuntará hacia una de las causas, se examina si la causa es la que más probabilidad tiene de generar el riesgo o si tiene una probabilidad media o baja.



4.7 Metodología de Auditoría Informática

Se pueden encontrar en la Auditoría Informática las Auditorías de Controles Generales como estándar de auditores profesionales y las Metodológicas de los auditores internos. Las metodologías de auditoría informática son del tipo cualitativo/subjetivo, están basadas en profesionales con gran nivel de experiencia y formación, capaces de recomendar con gran profesionalismo dentro de las áreas técnicas, operativas y jurídicas.

En otras palabras, la metodología es el fruto de un nivel profesional dado por la formación continua, y de la visión de cómo conseguir un mejor resultado. La auditoría informática debe respaldarse en un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa.

4.8 Tipos de auditoría informática

En la disciplina informática se destaca en la auditoría diferentes clases que son subcategorías o áreas del mismo orden. Entre las principales se mencionan (Piattini & Del Peso, 2001):

- ★ La auditoría física
- ★ Auditoría de la ofimática
- ★ Auditoría de la dirección
- ★ Auditoría de la explotación
- ★ Auditoría del desarrollo
- ★ Auditoría del mantenimiento
- ★ Auditoría de Bases de datos
- ★ Auditoría de técnicas de sistemas
- ★ Auditoría de la calidad
- ★ Auditoría de la seguridad
- ★ Auditoría de redes
- ★ Auditoría de aplicaciones



4.9 Auditoría de redes

Antes de continuar, debemos de saber que es una red de computadoras: conjunto de computadoras autónomas interconectadas. Se dice que dos computadoras están interconectadas si pueden intercambiar información (Tanenbaum, 2003, pág. 2).

Comprender el concepto anterior nos da un preámbulo al término detallado a continuación respecto a la auditoría de redes, cito textualmente: "Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitecturas, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red" (Muñoz Razo, 2002, págs. 621-622).

a. Auditoría de la red física

Casi el 50% del campo auditable en el área de red (puesto que el otro 50% representa a la parte lógica de la red), está orientado a la infraestructura física de la red (LAN², MAN³, WAN⁴) es allí donde se dictamina hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes. Se considerara que desde el interior del edificio no se intercepta físicamente el cableado (Piattini & Del Peso, 2001).

En caso de desastres, bien sea total o parcial, ha de poder comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y

² LAN: Local Area Network – Red de área Local

³ MAN: Metropolitan Area Network – Red de área Metropolitana

⁴ WAN: Wide Area Network – Red de área Extendida



que operatividad puede soportar. Ya que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencias deben tener prevista la recuperación en comunicaciones (Piattini & Del Peso, 2001).

b. Auditoría de la red lógica

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas.

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la organización para perder información, o bien para que ésta sea utilizada de forma inadecuada (Echenique García, 2002).

Es necesario monitorizar la red, revisar los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala. En general, si se quiere que la información que viaja por la red no pueda ser espiada, la única solución totalmente efectiva es la encriptación (la encriptación es el mecanismo principal para la seguridad de las comunicaciones. Se encarga de convertir un texto normal en un texto codificado de forma que las personas que no conozcan el código sean incapaces de leerlo (Maiwald, 2005, pág. 15)).

4.10 Vulnerabilidad en redes

Si bien es conocido la clara confusión de pensar en redes de computadoras y el internet como un mismo término, desde luego esto no es verídico la internet como tal es la unión de múltiples redes alrededor del mundo donde los servidores de páginas web ofrecen al público productos, información y entretenimiento. Gran parte de los ataques a los ordenadores personales o



institucionales provienen del acceso al internet. A pesar de los beneficios tangibles que la internet a demostrado desde sus orígenes a quienes “piensan en América Latina que ante tantas necesidades insatisfechas, internet es un lujo de países ricos y que primero debemos lograr llevar electricidad y agua potable a millones de familias antes de pensar en internet” (Arebalos, 2010).

En el párrafo anterior se hacía mención que la mayoría de ataques y fuentes de vulnerabilidad provenían del internet, puesto que la información transita por lugares físicamente alejados de las personas responsables. Esto presupone un compromiso en la seguridad, ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información (Piattini & Del Peso, 2001).

En las redes de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente 3 tipos de incidencias:

1. Alteración de bits.
2. Ausencia de tramas.
3. Alteración de secuencia.

Por causas dolosas, y teniendo en cuenta que es físicamente posible interceptar la información, los 3 mayores riesgos a atajar son:

1. Indagación.
2. Suplantación.
3. Modificación.

4.11 CobiT

CobiT (Control Objectives for Information and Related Technology) Objetivos de Control para la Información y Tecnología Relacionada.

Según el IT Governance Institute, “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”.

COBIT se divide en tres niveles:

- ★ Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- ★ Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- ★ Actividades: Acciones requeridas para lograr un resultado medible.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. (Véase *Anexo 1: Objetivos de Control de Cobit*)

Según el IT Governance Institute “COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de CobitT, estos dominios se llaman:

- Planear y Organizar (PO) – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- Adquirir e Implementar (AI) – Proporciona las soluciones y las pasa para convertirlas en servicios.
- Entregar y Dar Soporte (DS) – Recibe las soluciones y las hace utilizables por los usuarios finales.
- Monitorear y Evaluar (ME) -Monitorear todos los procesos para asegurar que se sigue la dirección provista.



4.11.1 Procesos y Controles de CobiT

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

4.11.2 Objetivos de control para Auditoría de red⁵ (IT Governance Institute, 2007)

- P01 Definir el plan estratégico de TI
- P03 Determinar la dirección tecnológica
- P05 Administrar la inversión en TI
- P08 Administrar la calidad
- P09 Evaluar y administrar riesgo de TI
- P010 Administrar proyectos
- AI3 Adquirir y mantener la infraestructura tecnológica.
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios

⁵ Para tener un detalle completo de los Objetivos de Control véase el Anexo 1

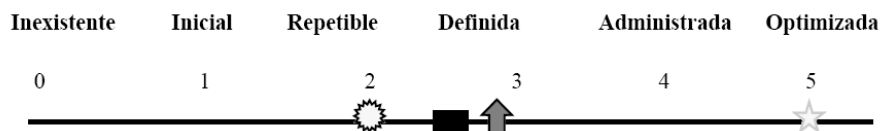


- DS1 Definir y Administrar niveles de servicio
- DS2 Administrar servicios de terceros
- DS3 Administrar el desempeño y la capacidad
- DS4 Aseguramiento de la continuidad del servicio
- DS5 Aseguramiento de la seguridad de los sistemas
- DS9 Gestión de la configuración
- DS12 Gestión del entorno físico
- DS13 Gestión de operaciones
- ME1 Detalle de recomendaciones

4.11.3 Modelos de madurez de COBIT

Los Modelos de Madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5). Este método ha sido derivado del Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Contra estos niveles, desarrollados para cada uno de los 34 procesos de TI de COBIT, la administración puede mapear o cruzar:

- ★ El estado actual de la organización - dónde está la organización actualmente
- ★ El estado actual de la industria (la mejor de su clase en) - la comparación
- ★ El estado actual de los estándares internacionales - comparación adicional
- ★ La estrategia de la organización para mejoramiento - dónde quiere estar la organización



LEYENDA PARA LOS SÍMBOLOS USADOS	LEYENDA PARA LAS CLASIFICACIONES USADAS
Situación actual de la empresa	0 Inexistente - los procesos de administración no se aplican en absoluto
Lineamientos Estándar Internacionales	1 Inicial - Los procesos son ad hoc y desorganizados
Mejor Práctica de la Industria	2 Repetible - Los procesos siguen un patrón regular
Estrategia de la Empresa	3 Definida - Los procesos son documentados y comunicados
	4 Administrada - Los procesos son monitoreados y medidos
	5 Optimizada - Las mejores prácticas son seguidas y automatizadas

Las clasificaciones anteriores indican lo siguiente:

0 Inexistente	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definida	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrada	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizada	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Las escalas del Modelo de Madurez ayudarán a la gerencia de usuarios a explicar a los administradores dónde existen deficiencias en la administración de TI y a fijarse objetivos donde necesitan estar comparando las prácticas de control de su



organización con los ejemplos de la mejor práctica. El nivel correcto de madurez estará influenciado por los objetivos de negocio y el entorno operativo de la empresa. Específicamente, el nivel de madurez de control dependerá de la dependencia de TI que tenga la empresa, de la sofisticación de la tecnología y, lo que es más importante, del valor de su información.

4.11.4 Justificación del Uso del Modelo de Referencia COBIT 4.1

Para la ejecución de la auditoría se ha tomado como marco de referencia COBIT 4.1, el cual es un marco de gobernabilidad de TI y un conjunto de herramientas de ayuda que permite asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos institucionales. Este conjunto de las mejores prácticas permiten evaluar la seguridad, eficacia, calidad y eficiencia de las TI., mediante lo cual se determinan los riesgos, se obtiene una gestión efectiva de los recursos, se mide el desempeño y cumplimiento de metas, y de manera principal el nivel de madurez de los procesos de la organización. Se ha elegido COBIT debido a que satisface las necesidades que tiene la organización en lo referente a las TI, tomando en cuenta los requerimientos de la institución, organizando las actividades mediante el modelo de procesos, identificando los recursos de TI prioritarios a ser utilizados y definiendo los controles de TI.

Como ventajas de implementar COBIT podemos citar:

1. Compatibilidad entre los parámetros de evaluación de Auditoría y los objetivos de control de COBIT
2. Flexibilidad en la parametrización de COBIT con respecto a los dominios y objetivos de control a evaluar en cada cliente.
3. Herramienta de documentación de hallazgos y recomendaciones.
4. Provee un marco único reconocido a nivel mundial de las "mejores prácticas" de control y seguridad de TI
5. Consolida y armoniza estándares originados en diferentes países desarrollados.
6. Concientiza a la comunidad sobre importancia del control y la auditoría de TI.



V. Análisis y Presentación de resultados

5.1 Metodología

El enfoque metodológico propuesto para la realización de la auditoría fue de carácter cualitativo ya que los pasos a seguir y los resultados de la ejecución de la misma se hicieron mediante un plan de trabajo flexible y con criterio humano. Como parte del proceso que se llevó a cabo se utilizó el lineamiento del estándar Cobit 4.1 para reforzar el procesamiento que se llevó a cabo al momento de la ejecución.

Para lograr lo propuesto en los objetivos de esta auditoría, se emplearon instrumentos y técnicas orientadas a obtener información relevante, estos fueron recolectados a través de las siguientes técnicas:

- **Cuestionarios:** El cuestionario es el método que utiliza un instrumento o formulario impreso, destinado a obtener respuestas sobre el problema de estudio y que el investigado o consultado llena por sí mismo (Piura López, 2006).
- **Entrevista:** Es la comunicación interpersonal establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto (Piura López, 2006).
- **Observación:** Método de recopilación de información primaria acerca del objeto estudiado mediante la directa percepción y registro de todos los factores concernientes al objeto estudiado, significativo desde el punto de vista de los objetivos de la investigación (Piura López, 2006).
- **Inspección:** La inspección consiste en examinar registros, documentos, o activos tangibles. La inspección de registros y documentos proporciona evidencia de auditoría de grados variables de confiabilidad dependiendo de su naturaleza y fuente y de la efectividad de los controles internos sobre su procesamiento (Instituto Mexicano de Contadores Públicos, A.C., 2004).



5.2 Desarrollo del Tema

En la siguiente sección expondremos las generalidades de la institución para la comprensión de los resultados y los hallazgos como parte del estudio realizado a la infraestructura física y lógica de la red de computadoras, basada en el Marco de referencia Cobit 4.1.

Para efectos de comprensión el acápite contendrá en su totalidad el informe ejecutivo de Auditoría que se despliega a continuación.

5.2.1 Generalidades de la Institución

La Universidad Nacional Agraria, una institución pública y autónoma orientada a la educación superior, creada bajo decreto ejecutivo el 25 de mayo de 1917, bajo el nombre de Escuela Nacional de Agricultura en el Departamento de Chinandega hasta que el 20 de abril de 1990 en la edición número 77 de la Gaceta (Diario oficial) se constituye como Universidad.

El Recinto universitario “Juan Francisco Paguaga” (conocido también como la sede Central), está ubicado en el km 12 carretera Panamericana norte, municipio de Managua. Cuenta actualmente con 11 carreras de Pregrado, 9 Postgrados, 1 Doctorado y 1 Especialidad. A dicho recinto se le añaden otras sedes regionales en Camoapa, Juigalpa y el Departamento de Carazo.

Con una población estudiantil y laboral que superan los 2 mil integrantes, la Universidad ha ido diversificando sus enfoques tecnológicos para el aprovechamiento en la innovación de las TIC's. Eventualmente la transmisión de datos ha alcanzado nuevos niveles de demanda en la comunicación de datos, que solventan con la incorporación de una red de computadoras en todas las áreas de la Universidad.



5.2.1.1 Misión

La Universidad Nacional Agraria es una institución de educación superior pública, autónoma, sin fines de lucro, que contribuye, desde la perspectiva del Compromiso Social Universitario, al desarrollo agrario integral y sostenible, y a la conservación del ambiente, mediante la formación de profesionales competentes, con valores éticos, morales y cultura ambientalista; la construcción de conocimiento científico y tecnológico; y la producción, gestión y difusión de información.

5.2.1.2 Visión

Es una institución líder en Educación Superior Agraria, caracterizada por su calidad, eficiencia y transparencia, con impacto nacional y proyección regional e internacional en la formación de profesionales, en tanto contribuye con la generación de conocimientos científico-técnicos e innovación para el desarrollo agrario, integral y sostenible.

Es reconocida por su vinculación e integración al desarrollo regional y nacional a través de programas académicos pertinentes, flexibles e innovadores que abarcan diferentes áreas del conocimiento agrario y son desarrollados en ambientes que fomentan el aprendizaje significativo, con escenarios variados y utilización de tecnologías de comunicación apropiadas para la construcción del conocimiento y el desarrollo de competencias técnicas y valores (Universidad Nacional Agraria, 2015).

Es una institución consolidada orgánicamente, con una estructura flexible, dinámica y adaptada al cambio. Los miembros de la comunidad están comprometidos con la calidad en el desarrollo de todos los procesos y procedimientos académicos y administrativos.

5.2.2 Riesgos en la implementación de la Auditoría

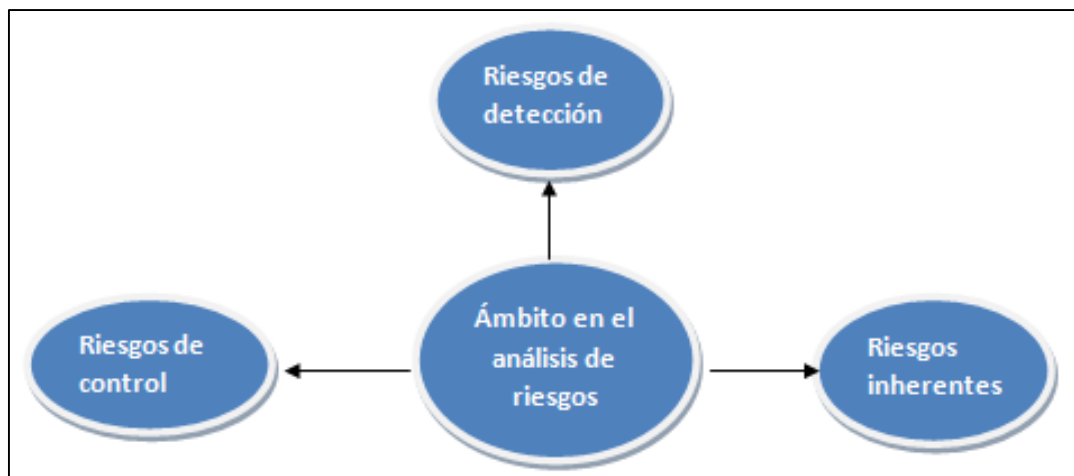


Figura 1. Clasificación de riesgos

El riesgo es la probabilidad de que una o varias amenazas se conviertan en un desastre. La vulnerabilidad o las amenazas, por separado, pueden no representar un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. El riesgo se refiere a la "posibilidad de daño o fracaso" bajo determinadas circunstancias.

El riesgo en Auditoría Informática está categorizado en 3 tipos de componentes descritos a continuación:

Riesgos de detección: Es el riesgo de que un auditor no detecte una representación errónea que exista en una aseveración y que pudiera ser de importancia relativa, ya sea en lo individual o cuando se acumula con otras representaciones erróneas (Federación Internacional de Contabilidad, 2007).

Riesgos de Control: El riesgo de que una representación errónea que pudiera ocurrir en una aseveración y que pudiera ser de importancia relativa, ya sea en lo individual o cuando se acumula con representaciones erróneas en otros saldos o clases, no se prevenga o detecte y corrija oportunamente por el control interno de la entidad (Federación Internacional de Contabilidad, 2007).

Riesgos inherentes: El riesgo que se somete una organización en ausencia de acciones de la administración para alterar o reducir su probabilidad de ocurrencia e impacto (Cartaya, 2009).

Auditoría de red en la Universidad Nacional Agraria sede Managua aplicando

N° de Ref.	Riesgo	Categoría de riesgo	Impacto			Probabilidad	Plan de reducción del riesgo
			Alta	Media	Baja		
1	Calidad de la auditoría sería nula.	Detección		X		10%	Seguimiento y verificación de los procesos de ejecución de la auditoría.
2	Información desorganizada o no disponible.	Control	X			40%	Garantizar un plan de comunicación para la entrega formal de documentación crítica.
3	Administradores y personal a cargo del control de redes no esté disponible.	Detección		X		60%	Consulta anticipada de horarios disponibles para la realización de entrevista al personal.
4	Cierre temporal de las oficinas por disturbios, cambios ambientales, emergencias o huelgas.	Inherente	X			35%	Fuera del alcance del auditor.
5	Falta de entrenamiento en las herramientas de auditoría.	Detección			X	80%	Realizar un estudio previo que permita el aprendizaje adecuado del manejo de las herramientas necesarias.
6	Finalización inesperada de los permisos para la ejecución de la auditoría.	Control		X		15%	Presentar recursos escritos que expliquen la necesidad en la continuidad del proyecto.
7	Desfase del cronograma estipulado en la ejecución de la auditoría	Detección			X	40%	Reajustar el calendario para dar cumplimiento a los objetivos. Expresar por escrito la situación.

Tabla 1. Riesgos de la auditoría de redes - UNA




5.2.3 Aplicación de Cobit

Como se ha planteado desde el inicio de la monografía, las áreas a evaluar fueron analizadas mediante el procedimiento del estándar Cobit 4.1 el cual establece cuatro dominios, donde se hará uso cada uno de ellos, sin embargo no se utilizarán todos los subprocesos. Los dominios son los siguientes: **Planeación y organización (PO)**, **Adquisición e implementación (AI)**, **Entrega de servicios y soporte (DS)**, **Monitoreo y evaluación (ME)**.

Guías de auditoría

Planear y Organizar
Definir un Plan Estratégico de TI

PO1

Dominio:	Planeación y organización
Proceso:	PO1: Definir un plan estratégico de TI
Objetivo de control:	Asegurar un plan estratégico que mejore la comprensión de los interesados en cuanto a las oportunidades y limitaciones de TI, evaluando el desempeño actual, identificando la capacidad y los requerimientos de recursos humanos.
Enfoque:	Incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para entregar estos servicios de una forma transparente y rentable.
Herramienta de recopilación de la información	<div>  <p>P1 - Definición de un plan estratégico de TI (PO1).rtf</p> </div> <p>Entrevista</p>
Hallazgos	
<ul style="list-style-type: none"> • No se cuenta con un plan estratégico de TI. • No se realizan estudios para la generación de la estrategia. 	



- Se realiza un POA⁶ pero no se profundiza en él.
- El portafolio de proyectos y servicios es muy limitado y desactualizado.
- No hay control de incidentes, ni bitácoras de proyectos.
- No se identifican políticas de medición de desempeño de los planes actuales.
- Los planes tácticos de TI son inexistentes.
- No hay seguimiento a la documentación que contiene las políticas y metas del área de TI.
- La visión de las estrategias futurísticas del área de TI son casi nulas.
- Las necesidades del hardware y todo equipo de red depende de las fallas del mismo.
- La comunicación e integración de estrategias de TI no son claras.
- No es claro el plan informático que contempla el crecimiento de usuarios, necesidades de hardware, evolución temporal y seguridad.
- No hay un lineamiento establecido que se debe seguir para gestionar la inversión de los programas de TI.

Conclusiones:

La planificación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y las prioridades de la institución.

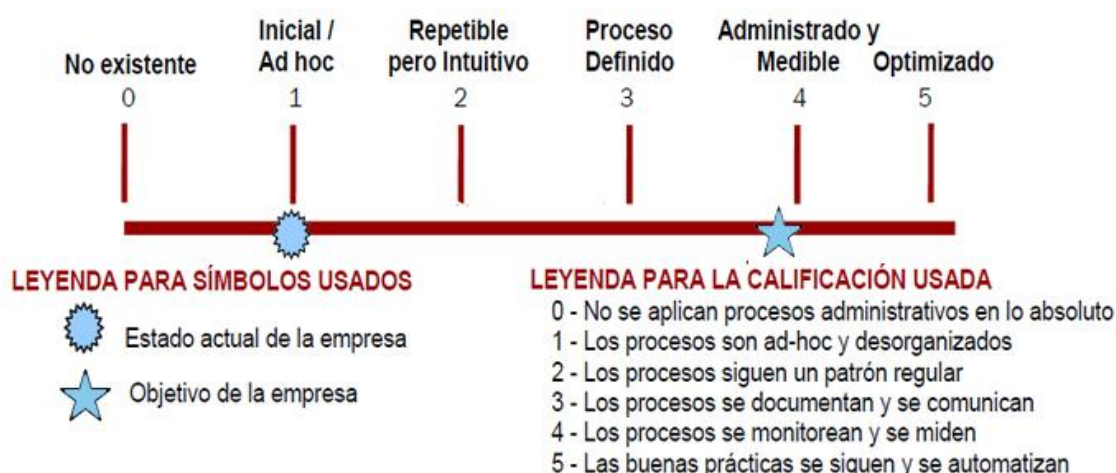
La función de TI y las partes interesadas del negocio son responsables de asegurar que se obtenga el valor óptimo a partir de un portafolio de servicios y proyectos. Un plan estratégico mejora la comprensión de las partes interesadas clave sobre las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica los requisitos de capacidad y de recursos humanos, aclarando el nivel de inversión requerido.

⁶ Véase definición en el glosario de términos como POA (Plan Operativo Anual)



En el caso particular la UNA no define un plan estratégico de TI, la estrategia de la institución y sus prioridades no se reflejarán en portafolios lo que conlleva a que la gestión y dirección de todos los recursos de TI no estén en línea con los objetivos y metas de la Universidad.

Modelo de madurez⁷:



Estado Actual: **Inicial/Ad Hoc.**

La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requerimiento de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.

Recomendaciones:

- Establecer y mantener un modelo de información institucional que facilite el desarrollo de aplicaciones y las actividades de soporte, a la toma de decisiones, consistente con los planes de TI. Este modelo debe facilitar la creación, uso y el compartimiento en forma óptima de la información por

⁷ Véase también el Modelo genérico de Madurez en el Anexo 2



parte de la Universidad de manera tal que se mantenga su integridad, sea flexible funcional, rentable, oportuna, segura y tolerante a fallos.


- Documentar los cambios efectuados que se presenten en las políticas, normas, prácticas y elementos físicos o virtuales que atañen a la red de computadoras.
- Desarrollar un plan de adquisiciones óptimas basadas en estudios previos de factibilidad para la gestión de la inversión en los programas de TI, esto incluye la compra de nuevos equipos de cómputos.
- Establecer un esquema de clasificación de datos que sea aplicado a toda la UNA donde se defina claramente quién puede tener acceso, el responsable de los accesos apropiados, la aprobación y requerimientos específicos necesarios para el acceso.
- Desarrollar un diccionario institucional de datos que contenga las reglas de sintaxis de los datos de la Universidad y los niveles de seguridad.
- Implementar un plan de comunicación en el área de TI, que permita la elaboración de un portafolio de proyecto debidamente documentado.

Planear y Organizar
Determinar la Dirección Tecnológica

PO3

Dominio:	Planeación y organización
Proceso:	PO3: Determinar la dirección tecnológica
Objetivo de control:	Determinar la dirección tecnológica para dar soporte al negocio, mediante la creación de un plan de infraestructura tecnológica que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.



Enfoque:	Definir e implementar un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.
Herramienta de recopilación de la información	<div>Entrevista</div> <div>  <p>P3 - Determinación de la dirección tecnológica (P...</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No existe planes de contingencia, en caso que los servicios de red fallen por daños, es posible que la Universidad suspenda sus servicios a los usuarios y algunas labores se vean perjudicadas por tiempo indefinido. • Los planes de mantenimiento de la infraestructura de la red física y lógica son muy débiles, puesto que no hay un seguimiento o verificación. • El acoplamiento de la infraestructura de red con respecto a las buenas prácticas o normas internacionales es mínima. • La administración de la función de servicios de información no tiene un proceso definido en cuanto al monitoreo y evaluación de nuevas tecnologías, que incorpora tecnologías apropiadas a la infraestructura de servicios de información actual. • No existe un patrón a seguir, en caso de adquirir nuevos equipos de hardware, que se debe adoptar para la incorporación del mismo. • El plan de infraestructura tecnológica o planes de adquisición de hardware y software de tecnología de información que no sean consistentes con los estándares de tecnología. • No hay estrategias de migración de datos, de un servidor a otro, completamente definidos. 	



- La estructura organizacional no contempla un área de seguridad de la información.

Conclusiones:

La función de servicios de información determina la dirección tecnológica para apoyar al negocio. Este proceso permite una respuesta oportuna a los cambios en el entorno competitivo, las economías de escala sobre el personal y las inversiones en sistemas de información, así como una mejor interoperabilidad de plataformas y aplicaciones.

En el caso de la UNA no existe un comité de arquitectura que desarrolle y gestione un plan de infraestructura tecnológica en donde se identifiquen los beneficios de las tecnologías en términos de productos y servicios. Esto impide a la organización contar con respuestas oportunas a cambios en el ambiente competitivo.

No hay conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento en cuanto a que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.

Modelo de madurez:





Estado Actual: **Inicial/Ad Hoc**

La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica esté impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.

Recomendaciones:


- Analizar las tecnologías existentes y las emergentes para la definición y el planeamiento de la dirección tecnológica adecuada para la UNA.
- Elaborar y mantener un plan de infraestructura tecnológica alineado con los planes estratégicos y tácticos de TI, que esté basado en la dirección tecnológica de la UNA, que incluya alineamientos para contingencia y orientación para la adquisición de recursos tecnológicos.
- Organizar un comité de arquitectura de información que establezca y dirija expectativas de lo que la tecnología puede ofrecer.
- Redactar un plan para la adquisición de Hardware y Software.

Planear y Organizar
Administrar la Inversión en TI

P05

Dominio:	Planeación y organización
Proceso:	PO5: Administrar la inversión de TI
Objetivo de control:	Identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, tomando medidas correctivas según sea necesario, para la fomentación de la asociación entre TI



	y la parte interesada, que facilite el uso efectivo y eficiente de recursos de TI y brinde transparencia.
Enfoque:	Tomar decisiones de portafolio e inversiones de TI efectivas y eficientes, para el establecimiento y seguimiento de presupuesto de TI de acuerdo a la estrategia de TI y a las decisiones de inversión.
Herramienta de recopilación de la información	<div style="text-align: center;">  <p>Entrevista</p> <p>P5 - Gestión de la inversión en TI (PO5).rtf</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • El portafolio de inversiones de TI no existe. • No hay documentación con los detalles de negociaciones para las nuevas inversiones de TI. • No hay un presupuesto detallado, en un rango de fecha específico, que permita la administración autónoma de los gastos para inversión de nuevas tecnologías. • No existe un proceso que permite una continua revisión, ajuste y aprobación del presupuesto global y de los presupuestos detallados de programas individuales de TI dentro de la Universidad. • No se realizan estudios de factibilidad para las nuevas inversiones. • No tienen definido ni implementado criterios de evaluación ni procesos para monitorear los beneficios de las inversiones de TI. 	

Conclusiones:

En la UNA no se establece ni mantiene un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto. La dirección es consultada para identificar y controlar los costos y beneficios totales dentro del contexto de los planes



estratégicos y tácticos de la red, y a la vez es la encargada de aprobar estos costos y tomar medidas correctivas según sean necesarias, sin embargo el tiempo de respuesta es muy prolongado, retrasando consigo las tareas aunque sean de carácter crítico.

La organización reconoce la necesidad de administrar la inversión en aunque esta necesidad se comunica de manera inconsistente. La asignación responsabilidades de selección de inversiones en TI y de desarrollo presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas selección y presupuesto de inversiones en la infraestructura de red, con documentación informal.

Modelo de madurez:



Estado Actual: Inicial/Ad Hoc

La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de una forma ad hoc. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.



Recomendaciones:


- Establecer un marco de trabajo financiero para redes de computadoras que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.
- Redactar Políticas, métodos y procedimientos organizacionales relacionados con la elaboración de presupuestos y las actividades de costeo.
- Para cada categoría de inversión, establecer criterios de evaluación para asegurar una evaluación justa, transparente, repetible y comparable. Los criterios de evaluación deben incluir, como mínimo:
 - La alineación con los objetivos estratégicos de la Universidad.
 - Los beneficios tanto financieros, como no financieros.
 - El riesgo, tanto el riesgo de entrega así como el riesgo de beneficio.
- Cuando existan desviaciones identificadas de forma oportuna, evaluar el impacto de esas desviaciones sobre los programas e incluir las medidas correctivas apropiadas. En caso de ser necesario, actualizar el caso institucional del programa de inversión.
- Detallar los informes de donaciones de equipos o dispositivos, que formen parte de la infraestructura de red, como beneficio de los programas del compromiso social corporativo de la empresa privada hacia la UNA con el fin de desligar de los presupuestos internos.

Planear y Organizar
Administrar la Calidad

PO8

Dominio:	Planeación y organización
Proceso:	PO8: Administrar la Calidad
Objetivo de control:	Elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición, por medio de la



	planeación, implantación y mantenimiento del sistema de administración de calidad, que a la vez proporcione requerimientos, procedimientos y políticas claras de calidad.
Enfoque:	Definir en un sistema de administración de calidad, el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI.
Herramienta de recopilación de la información	<div style="text-align: center;">  <p>Entrevista</p> <p>P8 - Gestión de la calidad (PO8).rtf</p> </div>
Hallazgos	
<ul style="list-style-type: none"> Existen ciertas normas aplicadas en la infraestructura física de la red de computadoras que dan como resultado un cierto porcentaje de calidad, sin embargo los métodos utilizados son basados en la práctica y no en normas internacionales (ISO 9000) (<i>Para más detalle vea la figura 13 en los anexos</i>). No existen políticas para la detección, corrección y prevención de inconformidades. Los estándares que más se tratan de cumplir son los de protocolo de comunicación los cuales rigen y especifican qué tipo de cables se utilizan, qué topologías se utilizarán, que topología tendrá la red. La identificación de las normas y buenas prácticas presenta escasos en su uso dentro de la red física y lógica. No existe un plan para la resolución de problemas presentados por los usuarios en cuanto al uso de la red. 	

Conclusiones:

El Administrador de la red dentro de la Universidad, hace un plus esfuerzo por mantener y ejecutar normas internacionales y buenas prácticas para la



creación, manipulación y mantenimiento de la infraestructura de red en su parte física y lógica, considerando que la capacitación en cuanto al tema es mínima y se limita únicamente a sus bases teóricas en pregrado.

La herencia en errores en cuanto a malos procedimientos en la implementación de la red es evidente, no teniendo un plan para la corrección paulatina de dichos errores.

Modelo de Madurez:



Estado Actual: **Repetible pero Intuitivo**

Se establece un programa para definir y monitorear las actividades de QMS⁸ dentro de TI. Las actividades de QMS que ocurren están enfocadas en iniciativas orientadas a procesos y proyectos, no a procesos de toda la organización.

Recomendaciones:

- Desarrollar documentación respecto a estándares, políticas y procedimientos de:
 - Seguridad y salud (incluye ergonomía).
 - Confidencialidad.
 - Seguridad.

⁸ Sistema de Administración de calidad (QMS, por sus siglas en Inglés)




- Se deben establecer lineamientos al comento de implementar una nueva red, esto siguiendo las recomendaciones de los organismos internacionales que rigen el funcionamiento debido de las estructuras de redes, por ejemplo:
 - La construcción de una red de área local especificada en el estándar de la IEEE⁹ número 8802, llamada comúnmente Ethernet (más precisamente la especificación 802.3) 10BaseT, que se refiere a una transmisión sobre UTP¹⁰ Categoría 5 a una velocidad de 10 MHz con topología estrella.
 - La instalación de los cables UTP siguiendo una norma jerárquica de conexión denominada “cableado estructurado” (*Mejorar lo existente, vea la figura 8 en la sección anexos*).
 - Las computadoras se conectarán con cualquier otro dispositivo a través de un switch, las conexiones se harán en puertos (RJ-45 End-Plug) o conectores hembras RJ-45 situados en la parte posterior de los switch convencionales (CISCO).
- Capacitar al personal a cargo de la red, en cuento al buen proceder y la debida aplicación de las normas internacionales de calidad, seguridad y buenas practicas al momento de implementar, dar mantenimiento o cambiar por completo la red de computadoras.

Dominio:	Planeación y organización
Proceso:	PO9: Evaluar y Administrar los Riesgos de TI
Objetivo de control:	Crear y dar mantenimiento a un marco de trabajo de administración de riesgo que documente un nivel común y acordado de los riesgos de TI, estrategias de mitigación

⁹ Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers)

¹⁰ Par trenzado sin blindaje (del inglés Unshielded twisted pair)



	y riesgos residuales, cuyo resultado de la evaluación debe ser entendible para los interesados y traducidos en términos financieros.
Enfoque:	La elaborar un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.
Herramienta de recopilación de la información	<div style="text-align: center;">  <p>Entrevista</p> <p>P9 - Evaluación y gestión de riesgos (P09).rtf</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No existen procedimientos de evaluación de riesgos. • No existe personal asignado para el monitoreo y el mejoramiento continuo de la evaluación de riesgos y controles de mitigación. • La determinación del impacto de los riesgos y ataques es nula. • Al no contar con estudios previos que reflejen o prevengan los riesgos, los servicios de red se encuentran vulnerables. • No hay un especialista encargado de la gestión de riesgos. • No existe un informe escrito con el detalle de los 3 últimos años que refleje la vulnerabilidad que presenta la red de computadoras de la Universidad. • No hay controles de seguridad apropiados, según ISO 27000. Hay fácil acceso al cuarto de servidores, dentro hay información visible que puede ser utilizada con fines de lucro por terceros. • No hay clasificación en los tipos de acceso en los nodos principales de la red. Hay un alto grado de vulnerabilidad. • No tienen planes detallados que deben seguir en el procedimiento de los riesgos, es decir, que una vez ejecutada una acción en contra que 	



perjudique la red, parcial o íntegramente, el personal desconoce el proceder adecuado basado en normas internacionales.

Conclusiones:

La evaluación y administración de riesgos es necesaria para identificar, analizar y evaluar cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado. Crear y dar mantenimiento a un marco de trabajo de administración de riesgos es importante para mitigar cualquier amenaza.

Particularmente en la UNA no existe tal marco de trabajo. No se adoptan estrategias de mitigación de riesgos residuales, a un nivel aceptable. No realizan evaluación de riesgos para los procesos y las decisiones de la institución con respecto a TI. La organización solo toma en cuenta los riesgos de operaciones académicas o financieras, no toma en cuenta los impactos institucionales asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos de TI. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.

Modelo de Madurez:



Estado Actual: **No Existe**



La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.

Recomendaciones:


- Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización. Este debe contemplar al menos:
 - Establecimiento del contexto.
 - Evaluación del riesgo.
 - Tratamiento del riesgo.
 - Aceptación del riesgo.
 - Comunicación del riesgo.
 - Monitorización y revisión del riesgo.
- Realizar un análisis detallado de amenazas o establecer planes de avance para mitigar riesgos.
- Determinar el impacto y la probabilidad de ocurrencia asociados al riesgo inherente en forma individual, por categoría y basado en el portafolio.
- Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua.
- Identificar estrategias para las respuestas a riesgos tales como: evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos, la documentación de evaluación de riesgos deberá incluir:
 - Una descripción de la metodología de evaluación de riesgos.
 - La identificación de exposiciones significativas y los riesgos correspondientes.



- Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución.
- Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.
- Considerar la contratación de un especialista en gestión de riesgo, de no ser posible capacitar al personal adecuado para que funjan con tal tarea.

Planear y Organizar PO10

Administrar Proyectos

Dominio:	Planeación y organización		
Proceso:	PO10: Administrar Proyectos		
Objetivo de control:	Establecer un marco de trabajo de administración de programas y proyectos para el control y manejo de todos los proyectos de TI establecidos, garantizando la correcta asignación de prioridades y la coordinación de todos los proyectos, mediante la elaboración de un plan maestro que asegure la calidad y todo lo necesario en torno a la administración adecuada de proyectos de TI.		
Enfoque:	Ejecutar un programa con enfoque en la administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos.		
Herramienta de recopilación de la información	Entrevista	 <p>P10 - Gestión de proyectos (PO10).rtf</p>	



Hallazgos

- No se define y ni se documenta la naturaleza y el alcance del proyecto para ratificar y desarrollar una comprensión común entre las partes interesadas acerca su alcance y cómo el mismo se relaciona con otros proyectos dentro del programa de inversión global posibilitado por la TI.
- No está establecido un plan de proyecto formal, aprobado e integrado (que abarque los recursos de la institución y de información de sistemas) a fin de guiar la ejecución y el control del proyecto a lo largo de todo su ciclo de vida.
- En caso que el proyecto se ejecute y los materiales escaseen para el cumplimiento en tiempo del proyecto, no existe un plan adecuado para solventar a lo inmediato el abastecimiento de los productos y servicios.
- No existe un sistema de medición de desempeño del proyecto en relación a los criterios clave del proyecto (por ej. alcance, calendarios, calidad, costos y riesgos).

Conclusiones:

Cada proyecto ejecutado dentro de la UNA es aprobado debidamente y analizado de forma adecuada por la parte interesada. Sin embargo gran parte de los proyectos no cuentan con una documentación que incluya los estudios de factibilidad previos al proyecto.

Los proyectos son ejecutados en gran parte bajo el presupuesto constitucional asignado a la Universidad, sin embargo hay proyectos mínimos bajo el financiamiento de entes no gubernamentales o de la empresa privada que requieren de retroalimentación, de lo cual no hay documentación existente.



Modelo de Madurez:



Estado Actual: **Definido**

El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TL se ha establecido una Oficina de administración de proyectos dentro de TI, con roles y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, cronogramas y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos de aseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia por parte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.

Recomendaciones:

- Para alcanzar un nivel óptimo, la Universidad debe de tener más énfasis en el establecimiento de un área específica para proyectos de TI.
- Se debe de tomar en cuenta la autoevaluación que se revisarán mediante métricas y lecciones aprendidas al final de cada proyecto.




- La documentación es indispensable para el futuro rumbo del área de redes, por lo que se debe de llevar un portafolio de proyectos con los detalles en el ciclo de vida de cada ejecución aprobada.
- Los riesgos deben ser correctamente administrados.
- Se debe de tener un plan de contingencia en caso que haya un mal cálculo en el presupuesto en los materiales de proyectos.

Adquirir e Implementar

Adquirir y Mantener Infraestructura Tecnológica

AI3

Dominio:	Adquisición e Implementación
Proceso:	AI3: Adquirir y Mantener Infraestructura Tecnológica
Objetivo de control:	Contar con proceso para adquirir, implementar y actualizar la infraestructura tecnológica, teniendo un enfoque planeado de acuerdo con las estrategias tecnológicas convenidas y con disposición de ambiente de desarrollo y pruebas.
Enfoque:	Proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.
Herramienta de recopilación de la información	<div>  <p>Entrevista</p> <p>P13 - Adquisición y mantenimiento de la infraestructura t...</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No existe un plan para la adquisición, implementación y mantenimiento de la infraestructura tecnológica. 	



- No se implementan medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y el software de infraestructura.
- No se definen las responsabilidades para el uso de componentes de infraestructuras sensitivas.
- No se monitorea y evalúa el uso de los componentes de infraestructura.
- No se toma en cuenta, en la selección del hardware, aspectos tales como: antecedentes del proveedor, nivel del servicio de mantenimiento técnico, capacidad de tolerancia a las fallas de la tecnología a adquirir contra el grado de criticidad de las aplicaciones a procesar y equipos similares existentes en la plaza.
- Los accesos a los puertos de diagnósticos no son controlados, puesto que no hay un mecanismo de seguridad.
- No se establecen entornos de prueba y desarrollo para apoyar la viabilidad eficaz y eficiente y la integración de las pruebas de las aplicaciones y la infraestructura en las primeras etapas del proceso de adquisición y desarrollo.

Conclusiones:

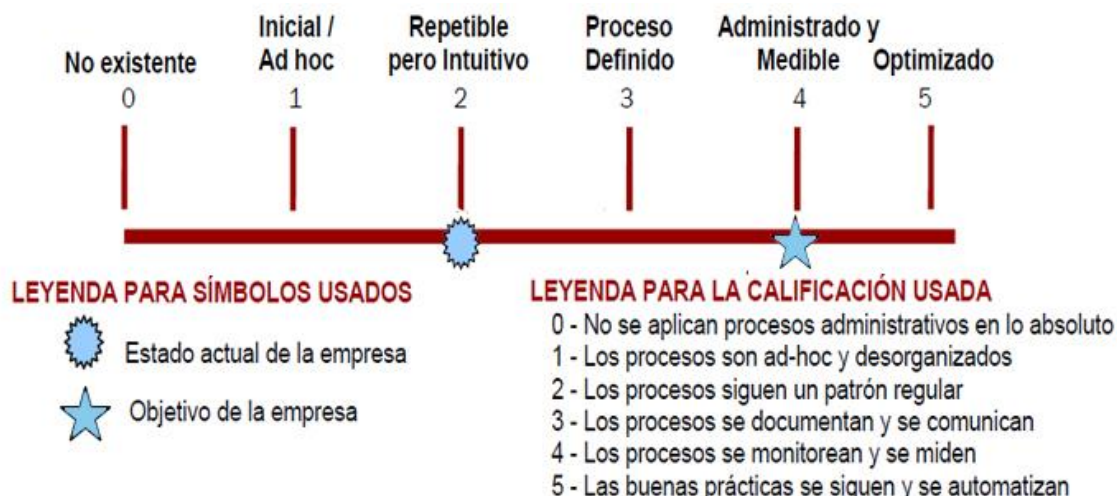
Este proceso asegura la disponibilidad continua de soporte tecnológico para las aplicaciones del negocio.

La UNA tiene procesos para la adquisición, implementación y actualización de su infraestructura tecnológica (pero no un plan concreto a seguir como un patrón recurrente), sin embargo estos procesos no son documentados ni se asignan responsabilidades.

La adquisición y mantenimiento de la infraestructura de TI se basa en una estrategia definida para todo el negocio. Se tiene la noción de que la infraestructura de TI es importante y que se apoya en algunas prácticas formales.



Modelo de Madurez:



Estado Actual: **Repetible pero Intuitivo**

No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.

Recomendaciones:

- Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar al menos:
 - Flexibilidad futura para agregar capacidad.
 - Costos de transición.
 - Los riesgos técnicos.
 - Vida útil de las inversiones para actualizar la tecnología.




- Implementar medidas de control interno, seguridad y auditoría durante la configuración, integración y mantenimiento del hardware y software de la infraestructura de red, para proteger los recursos y garantizar su disponibilidad e integridad.
- Realizar evaluaciones de costos de complejidad y viabilidad del producto cuando se hace una incorporación tecnológica.
- Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar al menos:
 - Funcionalidad.
 - Configuración del software y del hardware.
 - Pruebas de integración y desempeño.
 - Migración entre ambientes.
 - Control de versiones.
 - Herramientas y datos de prueba.
 - Seguridad.

Adquirir e Implementar
Facilitar la Operación y el Uso

AI4

Dominio:	Adquisición e Implementación
Proceso:	AI4: Facilitar la Operación y el Uso
Objetivo de control:	Generar documentación y manuales para el usuario y TI, con el fin de proporcionar entrenamiento que garantice el uso y operaciones correctas de las aplicaciones y la infraestructura.
Enfoque:	Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir



	el conocimiento necesario para la operación y el uso exitosos del sistema.
Herramienta de recopilación de la información	<div style="text-align: center;">  <p>Entrevista</p> <p>P14 - Habilitación de la operación y el uso (AI4).rtf</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No existe un plan para soluciones de operación. • No se transfiere el conocimiento de los sistemas de red a la Gerencia. • Se transfieren los conocimientos y habilidades a los administradores de la red mediante capacitaciones, pero el tiempo y los recursos brindados no son suficientes para que los involucrados puedan hacer un uso efectivo y eficiente de las configuraciones de red y el entorno de trabajo. 	

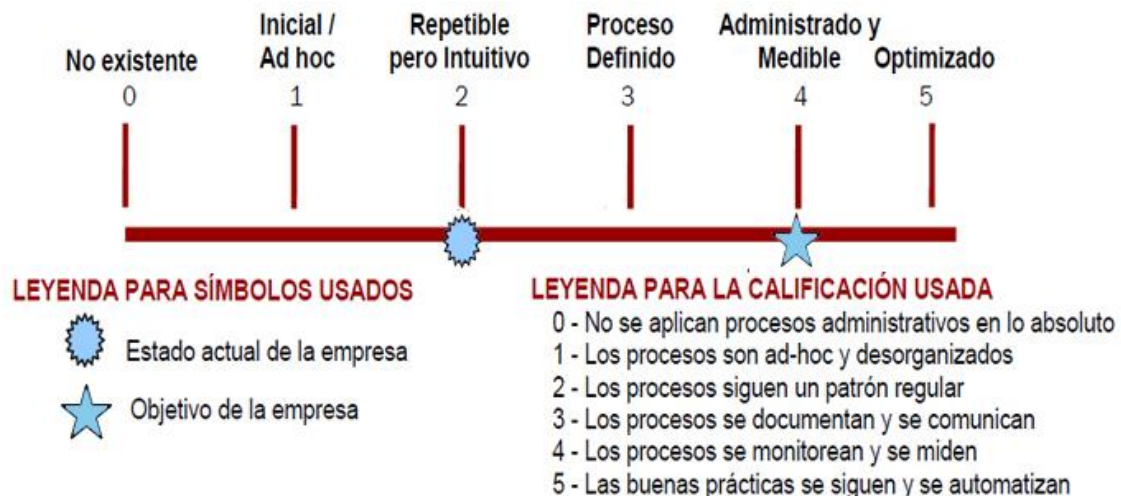
Conclusiones:

Transferir el conocimiento se hace necesario para la operación exitosa del sistema. La disponibilidad del conocimiento sobre los sistemas nuevos requiere la producción de documentación y manuales para usuarios y para TI, a la vez que proporciona entrenamiento para asegurar el uso y operación adecuados de las aplicaciones y la infraestructura.

En la *UNA* no se basan en un enfoque estructural o marco de trabajo para generar procedimientos y documentación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para la Universidad y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.



Modelo de Madurez:



Estado Actual: **Repetible pero Intuitivo**

Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.

Recomendaciones:


- Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operativos, como resultado de la introducción o actualización de la infraestructura de red.
- Mejorar los planes de capacitación incluyendo los siguientes recursos:



- Materiales de capacitación.
 - Manuales de usuario y de procedimientos.
 - Ayuda en línea.
 - Asistencia a usuarios.
 - Identificación de usuarios clave.
 - Evaluación.
- Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoyen y mantengan las aplicaciones, configuraciones y la infraestructura que atañe a la red de computadoras de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

Adquirir e Implementar
Adquirir Recursos de TI

AI5

Dominio:	Adquisición e Implementación
Proceso:	AI5: Adquirir Recursos de TI
Objetivo de control:	Suministrar recursos de TI de una manera oportuna y rentable, que incluya personas, hardware, software y servicios, a través de definiciones y ejecuciones de los procedimientos de adquisición, selección de proveedores y ajustes de arreglos contractuales.
Enfoque:	Adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI.
Herramienta de recopilación de la información	<div>Entrevista</div> <div>  <p>P15 - Abastecimiento de recursos de TI (AI5).rtf</p> </div>



Hallazgos

- No existe un conjunto de procedimientos y estándares de TI para la adquisición de infraestructura de TI.
- El procedimiento para establecer, modificar y finalizar los contratos con todos los proveedores y la selección de los mismos se realiza mediante licitaciones pero estas solamente se dan en proyectos grandes y no contemplan aspectos importantes al momento de la contratación.
- En dichas licitaciones se incluyen algunos ítems acerca de los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de TI, pero no incluyen los términos necesarios para cumplir y proteger los intereses de la organización.
- El contrato generado por ISP¹¹ contiene términos contractuales que no benefician en gran medida a la Universidad, técnicamente es un contrato unilateral que debe ser sometido a revisión.
- No hay asesoría legal en cuanto a temas de adquisición de servicios o bienes de TI que verifiquen los términos en el contrato.

Conclusiones:

Para la UNA muchas de las adquisiciones se dan mediante licitaciones, sin embargo éstas no contemplan aspectos importantes para la adquisición de recursos de TI.

Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de recursos de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización de la institución.

Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la

¹¹ Véase ISP (Internet Service Provider) en el Glosario de términos



experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.

Modelo de Madurez:



Estado Actual: **Repetible pero Intuitivo**

Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.

Recomendaciones:

- Desarrollar e implementar un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada



con TI, instalaciones, hardware, software y servicios necesarios por el negocio.


- Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones. Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.
- Las licitaciones deben contener ítems de los derechos y responsabilidades de las partes, que incluyan:
 - Propiedad y licenciamiento de la propiedad intelectual.
 - Mantenimiento.
 - Garantías.
 - Procedimientos de arbitraje.
 - Términos de actualización.
 - Seguridad, custodia y derechos de acceso.

Adquirir e Implementar
Administrar Cambios

AI6

Dominio:	Adquisición e Implementación
Proceso:	AI6: Administrar Cambios
Objetivo de control:	Administrar cada cambio efectuado, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, gestionándose formalmente y controladamente; esto se debe de registrar, evaluar y autorizar previo a la implantación.
Enfoque:	Controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de



	TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados.
Herramienta de recopilación de la información	Entrevista  P16 - Gestión de cambios (A16).rtf
Hallazgos	
<ul style="list-style-type: none"> • No existen procedimientos formales de administración de cambios. • No existe un procedimiento formal para la administración de cambios de emergencia. • No existe un sistema de seguimiento y reporte de los solicitantes de cambio. • No existe un proceso de revisión de cambios implantados (en la configuración después de la actualización del sistema de operativo). • No se han establecidos procesos de revisión para asegurar las implantaciones correctas de cambios. • No se lleva un registro de los nombres de las personas que efectúan cambios en los sistemas de red. 	

Conclusiones:

Dentro de la *UNA* los cambios, inclusive sobre procedimientos, procesos y parámetros de servicio y de red no son registrados, evaluados ni autorizados antes de su implementación.

No existiendo un plan de administración de cambios, se nota un ambiente de vulnerabilidad propicio para que terceros y con intenciones maliciosas ejecuten actos en contra de la universidad haciendo cambios en las configuraciones de



redes de las computadoras; existe acceso al CMD¹² en el 90% de las computadoras de la institución, pudiendo realizarse cambios virtualmente sin control alguno.

Modelo de Madurez:



Estado Actual: **No Existe**

No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.

Recomendaciones:

- Los procedimientos para la administración de cambios deben incluir al menos:
 - Valoración del impacto del cambio solicitado sobre el ambiente de producción.
 - Criterios para categorización del cambio solicitado.
 - Criterios para la priorización del cambio solicitado.

¹² Véase la definición CMD (Command Prompt) en el Glosario de términos




- Autorización para la puesta en producción del cambio solicitado por la persona adecuada.
- Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, después de la implantación del cambio de emergencia.
- Tener una biblioteca de documentación donde se incluya la bitácora de configuraciones de la red en caso de haber cambios, ésta información debe ser resguardada bajo llave y con las medidas de seguridad apropiadas, adicionalmente contener una copia digital en un medio de almacenamiento que está bajo las mismas normas de seguridad.

Entregar y Dar Soporte

Definir y Administrar los Niveles de Servicio

DS1

Dominio:	Entregar y Dar Soporte
Proceso:	DS1: Definir y Administrar los Niveles de Servicio
Objetivo de control:	Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, haciendo posible una comunicación efectiva entre la gerencia de TI y los clientes del negocio respecto de los servicios requeridos.
Enfoque:	Identificar los requerimientos de servicios, el acuerdo de niveles de servicios y el monitoreo del cumplimiento de los niveles de servicio.
Herramienta de recopilación de la información	<div>Entrevista</div>  <p>P18 - Definición de los niveles de servicio (DS1).rtf</p>
Hallazgos	
<ul style="list-style-type: none"> • No se realiza un proceso para la creación de requerimientos de servicio. 	



- No se define una estructura organizacional para la administración de los niveles de servicio.
- No se encuentra definido un criterio de desempeño especificado para el monitoreo de los niveles de servicio.
- No existe en la organización un verdadero compromiso con la calidad del servicio TI ofrecido.
- El servicio que se brinda a los usuarios están establecidos de acuerdo a los requerimientos de los mismos, pero no existe un documento en donde se establezcan los servicios; se hace de una manera mental e intuitiva.
- No se mantiene un inventario actualizado o un registro con los activos importantes asociados a la infraestructura de red.
- No hay un análisis de las estadísticas de monitoreo donde se actúe en consecuencia para identificar las tendencias positivas y negativas de los servicios en forma individual y global.

Conclusiones:

Hacer uso de un marco de referencia que provea un proceso formal para la administración de niveles de servicio entre los usuarios y los administradores de los servicios será de suma importancia para el alineamiento continuo con los requerimientos y prioridades del negocio.

La gestión de niveles de servicio es responsable de buscar un compromiso realista entre las necesidades y expectativas del usuario y los costes de los servicios asociados, de forma que estos sean asumibles por la organización TI.

Los criterios para la definición de los niveles de servicio están basados en la criticidad del negocio e incluyen consideraciones de disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad.



Modelo de Madurez:



Estado Actual: **Inicial/Ad Hoc**

Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y la administración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa. La notificación es informal, infrecuente e inconsistente.

Recomendaciones:

- Realizar una detallada identificación y análisis de las necesidades del usuario.
- Elaborar un documento de "Requisitos de Nivel de servicio (SLR)". El SLR debe incluir información sobre las necesidades del usuario y sus expectativas de rendimiento y nivel de servicios, respecto a:
 - La funcionalidad y características.
 - La disponibilidad.
 - La interacción con su infraestructura TI o de otro tipo.
 - Los niveles de calidad.
 - Tiempo y procedimientos de implantación.
 - La escalabilidad.




- Elaborar "Hojas de Especificación del Servicio", las cuales contengan, una descripción con todos los detalles técnicos necesarios, sobre cómo se prestará el servicio y cuáles serán los indicadores internos de rendimiento y calidad del servicio.
- Elaborar un "Plan de Calidad del Servicio (SQP)", el cual incorpore:
 - Objetivos de cada servicio.
 - Estimación de recursos.
 - Indicadores clave de rendimiento.
 - Procedimientos de monitorización de proveedores.
- Llevar a cabo y analizar estadísticas de monitoreo que permitan identificar las tendencias, tanto para los servicios individuales como para los servicios en conjunto.

Entregar y Dar Soporte
Administrar los Servicios de Terceros

DS2

Dominio:	Entregar y Dar Soporte
Proceso:	DS2: Administrar los Servicios de Terceros
Objetivo de control:	Asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros, mediante una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.
Enfoque:	Establecer relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.



Herramienta de recopilación de la información	<p data-bbox="727 304 868 331">Entrevista</p> <div data-bbox="922 199 1096 462">  <p data-bbox="933 357 1088 457">P19 - Gestión de los servicios prestados por terceros (DS2.rtf)</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No se mantiene una documentación formal de relaciones técnicas y organizacionales. • No se formaliza un proceso de gestión de relaciones para cada proveedor. • No se asegura la calidad de la relación cliente- proveedor, puesto que no se define un acuerdo de nivel de servicios, ni similares. Aun cuando los equipos fuesen donados a la Universidad. • No se identifican y mitigan los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. • No se monitorea la entrega del servicio del proveedor, mayoritariamente en el caso del ISP (<i>Véase figura 10 en la sección de anexos</i>). • No se identifican y categorizan los servicios de los proveedores. 	

Conclusiones:

Resulta de suma importancia asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, se requiere de un proceso efectivo de administración de terceros que se ocupe de gestionar la relación con los proveedores de servicios de los que depende la organización TI y de esta forma alcanzar la mayor calidad a un precio adecuado.

En vista de que existen varios servicios que se adquieren de organizaciones externas se debe procurar obtener un producto de calidad, precio adecuado, en el momento preciso, esto se logra mediante una clara definición de



roles, responsabilidades y expectativas en los acuerdos con terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos, de esta forma se asegura que el proveedor está cumpliendo con los requerimientos del negocio actuales y que el desempeño es competitivo con las condiciones del mercado.

La Dirección de OTIC-UNA está consciente de la importancia de tener políticas y procedimientos para la administración de los servicios de terceros, sin embargo no hay condiciones estandarizadas para los convenios (a pesar que hay convenios suscritos, en este caso las condiciones son particularmente diferentes a los expuesto) con los prestadores de servicios, la medición de los servicios prestados es informal y reactiva, las prácticas dependen de la experiencia de los individuos y del proveedor. .

Modelo de Madurez:



Estado Actual: Inicial/Ad Hoc

La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. NO hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).



Recomendaciones:


- Al momento de seleccionar un nuevo proveedor se debe considerar lo siguiente:
 - Su adecuación a los requisitos previamente definidos.
 - Referencias de otros competidores.
 - Disponibilidad y capacidad
 - Aspectos financieros.
 - Condiciones del servicio a prestar.
- Una vez elegido el proveedor, negociar los términos del servicio. El resultado debe quedar reflejado en un Contrato de Provisión del Servicio.
- Definir un proceso para monitorear la entrega del servicio de manera que se asegure que el proveedor:
 - Este cumpliendo con los requerimientos de la Institución.
 - Continúe adhiriéndose a los acuerdos contractuales.
 - Su desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

Entregar y Dar Soporte
Administrar el Desempeño y la Capacidad

DS3

Dominio:	Entregar y Dar Soporte
Proceso:	DS3: Administrar el Desempeño y la Capacidad
Objetivo de control:	Revisar periódicamente el desempeño actual y la capacidad de los recursos de TI, que incluya el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias.
Enfoque:	Cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de



	desempeño y capacidad de TI a través del monitoreo y la medición.
Herramienta de recopilación de la información	<p>Entrevista</p>  <p>P20 - Gestión de la capacidad y del desempeño del sistema (.rtf)</p>
Hallazgos	
<ul style="list-style-type: none"> • No se lleva un control con respecto a las cargas de trabajo. • No se implementan planes de contingencia apropiados para la capacidad y desempeño de los recursos individuales de TI. • No se realiza un análisis de rendimiento de la infraestructura de red, considerando que es diferente cuando se habla de tráfico de red. • No se gestiona la demanda de servicios de red, ancho de banda y capacidad de almacenamiento en los servidores. • No se monitorea continuamente el desempeño y la capacidad de los recursos de red. • No se toman las medidas que garanticen la mejora del servicio. • No existe un plan que prevea a mediano o largo plazo el crecimiento de la información que debe ser almacenada en los servidores locales. • No hacen uso de un Data Warehouse. • Los planes de contingencias, en caso que hipotéticamente se llegue al límite de la capacidad de la red, no existen. 	

Conclusiones:

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso de revisión periódica. Su primordial objetivo es poner a disposición de usuarios y de las propias áreas de OTIC-UNA, los recursos informáticos necesarios para desempeñar de una manera eficiente sus tareas, todo ello sin incurrir en costes desproporcionados.

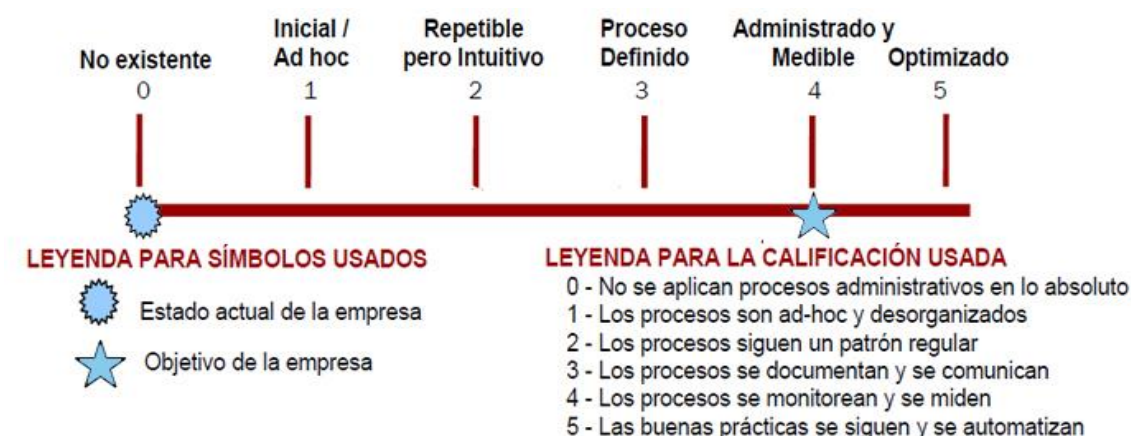


Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias; brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.

En conjunto con una correcta gestión de la demanda, se debe asegurar que los servicios críticos no se ven afectados o, cuando menos, lo sean en la menor medida posible. Para llevar a cabo esta tarea de forma eficiente es imprescindible que se conozcan las prioridades de la institución y del cliente y actuar en consecuencia.

Una correcta monitorización de la capacidad permite reconocer puntos débiles de la infraestructura de red o cuellos de botella y evaluar redistribución a largo plazo de la carga de trabajo que permita calidad sin aumento de la capacidad.

Modelo de Madurez:



Estado Actual: **No Existe**

La gerencia no reconoce que los procesos clave de la institución pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.



Recomendaciones:

- Elaborar un Plan de Capacidad y desempeño que recoja, como mínimo:
 - Toda la información relativa a la capacidad de la infraestructura TI.
 - Las previsiones sobre necesidades futuras basadas en tendencias y previsiones de negocio.
 - Los cambios necesarios para adaptar la capacidad de red a las novedades tecnológicas y las necesidades emergentes de los usuarios.
- Realizar modelos y simulaciones sobre diferentes escenarios para llevar a cabo previsiones de carga y respuesta de la infraestructura de TI.
- Elaborar planes de contingencia, donde se aborde lo siguiente:
 - Determinación de los objetivos.
 - Realizar un inventario completo.
 - Análisis y valoración de riesgos.
 - Ejecución
 - Pruebas
 - Documentación
 - Difusión y mantenimiento.
- Proporcionar reportes administrativos para ser revisados por la alta dirección, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados para redes de computadoras, niveles de servicio de programas individuales y la contribución de red a ese desempeño.
- Optimizar y racionalizar los recursos de red.
- Identificar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.
- Evaluar periódicamente, a través de encuestas o de otras herramientas de recopilación de información, el nivel de satisfacción del usuario producto de




la capacidad de la red en su totalidad, esto incluye almacenamiento, velocidad, etc...

Entregar y Dar Soporte

Garantizar la Continuidad del Servicio

DS4

Dominio:	Entregar y Dar Soporte
Proceso:	DS4: Garantizar la Continuidad del Servicio
Objetivo de control:	Brindar continuidad en los servicios de TI, para el almacenamiento de respaldos de información fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad.
Enfoque:	Desarrollar entornos de resistencia en las soluciones automatizadas y desarrollo, mantenimiento y probando los planes de continuidad de TI.
Herramienta de recopilación de la información	<div>Entrevista</div>  <div>P21 - Aseguramiento de la continuidad del servicio (DS...</div>
Hallazgos	
<ul style="list-style-type: none"> • No existe un marco que desenvuelva la continuidad de los servicios de red, donde se apoye la gestión de la continuidad de los servicios de red, de la universidad, con un proceso coherente. • No hay planes correctamente trazados que la institución debe seguir a fin de iniciar una recuperación de información en caso perdida o desastre, adicionalmente no existen planes de contingencia de TI. • No existen políticas de pruebas o de simulacros en caso que ocurran eventualidades que pongan en riesgo los datos críticos de la Universidad. 	



- El orden y las responsabilidades que cada individuo (trabajador/administrador) de la red debe seguir a fin de cumplir con un plan de emergencia en la recuperación de información.
- No existe un plan de verificación de recuperación paulatina posterior a los acontecimientos que dieron lugar a la pérdida de datos o daños a la infraestructura.
- No se desarrolló un plan estratégico basado en los resultados del análisis de riesgos para definir un enfoque general a la continuidad de los servicios de red en la Universidad.
- No hay un centro de telecomunicaciones de respaldo.
- El tiempo estipulado posterior a interrupciones o fallos en los servicios de red, es indefinido.
- La arquitectura de red utilizada en la Universidad no permite la diversificación de rutas alternas en las telecomunicaciones.
- La comunicación en los cambios dentro del plan de seguridad y respaldo es nula, puesto que no existe un tópico de esta índole en la institución.
- No existe un formato, ni un procedimiento a seguir para redactar y emitir informes de recuperación.
- No se garantiza la compatibilidad entre el hardware y el software de restauración y no hay métodos de prueba y actualización periódicamente los datos archivados.

Conclusiones:

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar mantener y probar planes de continuidad de TI. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.



La gestión de la continuidad del Servicio se preocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.

Modelo de Madurez:



Estado Actual: **No Existe**

No hay entendimiento de los riesgos, vulnerabilidad y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.

Recomendaciones:

- Implementar planes de continuidad de TI para todos los servicios críticos de TI.
- Considerar distintas posibilidades de migración de información y aplicaciones críticas en caso de interrupciones o fallos, esto puede ser de la siguiente forma:
 - Ejecutarlas manualmente
 - Migrar a un esquema de ejecución degradado donde solo se procesa lo imprescindible y con menor calidad (por ejemplo, solo los procesos en lotes y no los interactivos).
 - Migrar las configuraciones de red a distintos equipos de trabajo de forma "Fragmentada".



- Definir y ejecutar procedimientos dentro del proceso de control de cambios para asegurar que el plan de continuidad de TI se mantenga actualizado y refleje continuamente los requerimientos actuales de la Institución.
- Realizar capacitaciones donde se consideren los procedimientos, roles y responsabilidades en caso de un incidente o desastre, tomando en cuenta los resultados de las pruebas de contingencia.
- Definir una estrategia administrada de distribución del plan de continuidad de TI, la cual asegure que los planes sean distribuidos de forma apropiada y segura, que se encuentren disponibles para las partes involucradas, autorizadas y apropiadas, en el momento y lugar que lo necesiten, de igual forma que sean accesibles bajo cualquier escenario de desastre.
- Revisar periódicamente los planes de contingencia para adaptarlos a las necesidades reales del negocio.

Entregar y Dar Soporte
Garantizar la Seguridad de los Sistemas

DS5

Dominio:	Entregar y Dar Soporte
Proceso:	DS5: Garantizar la Seguridad de los Sistemas
Objetivo de control:	Mantener la integridad de la información y de proteger los activos de TI, mediante un proceso de administración de la seguridad que incluya el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI.
Enfoque:	Definir las políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.



Herramienta de recopilación de la información	<div data-bbox="727 302 870 331" data-label="Text"> <p>Entrevista</p> </div> <div data-bbox="915 195 1065 338" data-label="Image"> </div> <div data-bbox="919 348 1081 449" data-label="Text"> <p>P22 - Aseguramiento de la seguridad de los sistemas ...</p> </div>
Hallazgos	
<ul style="list-style-type: none"> • No se define ni se asignan responsabilidades de seguridad. • El plan de seguridad de redes no existe, a pesar que siguen por intuición ciertas normas de seguridad. El plan no es algo que está debidamente documentado. • No se hace uso de software que permita controlar la utilización indiscriminado de disquetes, CD o Memorias USB en la organización, no se establecen grupos de PC aislados, que manejen información sensible, en los que sólo se pueda usar disquetes, CD o Memorias USB cifrados para cada grupo en particular. • Las sesiones de trabajo de la LAN no permiten un cierre de sesión automática luego de un lapso de inactividad. • No se realizan pruebas, vigilancia ni monitoreo de acceso al centro de servidores. • No hay mecanismos de detección de intrusos en caso de un ataque. 	

Conclusiones:

La necesidad de mantener la integridad de la información, datos, mecanismos de red y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye el monitoreo de seguridad y pruebas periódicas así como acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva



administración de la seguridad protege todos los activos de TI para minimizar el impacto en la institución causado por vulnerabilidades o incidentes de seguridad.

La inversión en tiempo y recursos que supone la seguridad de la información se ve ampliamente recuperada con las ventajas que, de manera indiscutible conlleva su implantación, la misma, proporciona una imagen institucional de compromiso con la seguridad, promueve la confianza en las relaciones con terceros y mejorar la imagen pública o la imagen frente a usuarios del ente académico.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición de la UNA y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

Modelo de Madurez:



Estado Actual: Inicial/Ad Hoc

La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.



Recomendaciones:


- Desarrollar un plan de seguridad para TI (esto incluye las redes de computadoras), que tome en cuenta:
 - Los requerimientos de información de la institución.
 - La configuración de la red.
 - Los planes de acción sobre riesgos de la información.
 - La cultura de seguridad de la organización.
- Asegurar que los planes y procedimientos establecidos sean comunicados a los usuarios y las partes interesadas.
- Garantizar que se cumplan las políticas y procedimientos de seguridad.
- Revisar las políticas de seguridad a intervalos regulares, o cuando hay cambios significativos para asegurar la adecuación y efectividad.
- Realizar pruebas y monitoreo proactivamente, de la implementación de seguridad de la red.

Entregar y Dar Soporte
Administrar la Configuración

DS9

Dominio:	Entregar y Dar Soporte
Proceso:	DS9: Administrar la Configuración
Objetivo de control:	Garantizar la integridad de las configuraciones de hardware y software estableciendo y manteniendo un repositorio de configuraciones completas y precisas, incluyendo la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite.



Enfoque:	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.
Herramienta de recopilación de la información	Entrevista  P26 - Gestión de la configuración (DS9).rtf
Hallazgos	
<ul style="list-style-type: none"> • No existe un repositorio central establecido para contener toda la información relevante acerca de los elementos de configuración. • El almacenamiento de referencia de los elementos de configuración por cada servicio y sistema como un punto de control al cual se puede retornar luego de efectuar cambios, es mínimo y no está presente en la mayoría de los casos. • No hay un mapa auxiliar, al que puedan consultar, que muestre los detalles de la red instalada, cualquier trabajo de electricidad o albañilería podría terminar en rupturas de un segmento de la red. • Se estima que tan sólo el 20% de las computadoras del recinto universitario esté bajo medidas de seguridad, de manera tal que dificulte la extracción indebida de placas madres o del mismo ordenador. • No se evita la introducción de software no autorizado a las computadoras de la institución, las pocas que cuentan con este mecanismo no superan el 10% del total. • No hay un tiempo establecido para que se realicen inspecciones del cableado, los conectores, los routers, bridges¹³ y gateways. • Los usuarios pueden tener acceso a terminales de configuración con privilegio de administrador del sistema operativo, en el caso de Windows está habilitado el CMD para 98% de las computadoras de las Universidad 	

¹³ Para más detalles en la definición, consultar el Glosario de términos.



Conclusiones:

Uno de los elementos más importantes cuando se monta un red de computadoras es nada más ni nada menos que su configuración; si los elementos de configuración están correctamente alineados con las normas internacionales y las buenas prácticas que den como resultado la total eficiencia en la funcionalidad lógica de la red, entonces se está cumpliendo el objetivo planteado por la institución al brindar buen servicio al cuerpo educativo y administrativo.

Bajo los hallazgos descritos con anterioridad la falencia principal de la red puede radicar en la vulnerabilidad de la configuración lógica de la red. Existen ciertos patrones o parámetros que no fueron considerados al momento de diseñar, implementar o reestructurar la red de computadoras.

Modelo de Madurez:



Estado Actual: Repetible pero Intuitivo

La gerencia esta consiente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos




interrelacionados, tales como administración de cambios y administración de problemas.

Recomendaciones:

- Definir las políticas de administración de la configuración, el documento debe de tener un alineamiento con la misión y visión de la *UNA*.
- Diseñar un esquema de control y monitoreo de los elementos de red; toda la configuración y estructura debe ser revisada periódicamente cada 3 meses, por lo menos.
- Establecer un límite de acceso al usuario en cuento al sistema operativo, a pesar que gran parte de la comunidad educativa de la *UNA* no cuenta con conocimientos informáticos que pongan en riesgos la integridad de red de la Universidad, no se debe dejar al azar tales eventualidades.
- Se debe documentar los elementos de configuración necesarios para posteriores usos, éste a la vez debe de tener las medidas de seguridad necesaria para el almacenamiento de ese tipo de datos, incluyendo el control de acceso a éste tipo de información.
- Establecer un punto de control al cual se puede retornar luego de efectuar cambios en el sistema operativo o en la configuración de red.
- Usar herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad en la red.
- Determinar los mecanismos para la detección del origen de las fallas en la configuración; una vez investigada la causa, debe ser documentada.
- Efectuar un rastreo de activos y el monitoreo de activos individuales de TI, para la protección de robo, de mal uso y de abusos.

Entregar y Dar Soporte
Administración del Ambiente Físico

DS12

Dominio:	Entregar y Dar Soporte
Proceso:	DS12: Administración del Ambiente Físico
Objetivo de control:	Proteger el equipo de cómputo y del personal, mediante instalaciones bien diseñadas y bien administradas, que incluya la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.
Enfoque:	Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.
Herramienta de recopilación de la información	<div>Entrevista</div>  <p>P29 - Gestión del entorno físico (DS12).rtf</p>
Hallazgos	
<ul style="list-style-type: none"> • Para el diseño y selección del centro de datos no se consideraron los riesgos asociados con los desastres naturales u ocasionados por el hombre. • No se han definido esquemas de perímetro de seguridad. • No existen restricciones para ingresar a las instalaciones de la Universidad (siempre y cuando no se tenga una actitud o apariencia sospechosa para delinquir), una vez dentro de la misma, no se limita el acceso a los diferentes locales. • No se toman en cuenta medidas de protección contra factores ambientales. 	



- Los equipos y dispositivos especializados para controlar el ambiente son insuficientes.
- No son supervisadas las condiciones ambientales que afectarían adversamente las instalaciones de tratamiento de la información.
- Los accesos a los locales informáticos no son adecuados para una rápida llegada de bomberos, emergencia médica o policía.
- En el local donde se alojan los servidores centrales no cuenta con la temperatura recomendada por el proveedor para mantener un óptimo desempeño de los servidores.
- En algunas áreas, como centros de cómputo, los routers y switches están a simple vista y eventualmente de fácil acceso o manipulación para el usuario (*Véase figura 5 y 8 en la sección de anexos*).
- Los dispositivos de red, en un 85% de los casos, no son debidamente limpiados o protegidos contra el polvo e influencia de insectos (como las arañas), probablemente se deba a que el personal de limpieza no tiene acceso o se encuentra inalcanzable respecto a altura de ubicación.
- Muchos de los estabilizadores de energía o backups han cumplido su vida útil.

Conclusiones:

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones de la institución ocasionadas por daños al equipo de cómputo y al personal.



Evaluar y controlar permanentemente la seguridad física del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de la organización.

Modelo de Madurez:



Estado Actual: **Inicial/Ad Hoc**

La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal

Recomendaciones:

- Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la administración del entorno físico.
- Evaluar la completitud y efectividad de los controles de gerencia sobre los procesos, personas, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.
- Obtener aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.




- Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicios externos cumplen con los requerimientos legales, regulatorios y obligaciones contractuales.
- Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.
- Mantener extinguidores de fuego en cada sala de cómputo.

Entregar y Dar Soporte

Administración de Operaciones

DS13

Dominio:	Entregar y Dar Soporte
Proceso:	DS13: Administración de Operaciones
Objetivo de control:	Procesar información completa y apropiada, a través de una administración efectiva del procesamiento de datos y del mantenimiento de hardware, incluyendo definiciones de políticas y procedimientos de operaciones, protección de datos de salida sensitivos, monitoreo de la infraestructura y mantenimiento preventivo del hardware.
Enfoque:	Cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura.
Herramienta de recopilación de la información	<div>Entrevista</div>  <p>P30 - Gestión de operaciones (DS13).rtf</p>
Hallazgos	
<ul style="list-style-type: none"> • Los procedimientos operacionales cubren los cambios de turnos (traspaso formal de actividades, actualizaciones de estado, problemas 	



operacionales y procedimientos de escalamiento) para asegurar la continuidad de las operaciones, sin embargo no hay una documentación digital ni escrita de los procedimientos a seguir en este tipo de acciones.

- No existe una bitácora donde el personal de operaciones anote los registros de sus actividades.
- No existe un reglamento escrito y actualizado que precise las responsabilidades de las personas y el procedimiento de firma (quiénes y cómo), según el documento de que se trate.
- No se llevan a cabo reuniones de evaluación y seguimiento para analizar las acciones, correcciones y eventualidades en la administración de operaciones.
- No hay una calendarización definida para el cumplimiento de tareas, hitos o actividades en la administración de operaciones.
- Los informes estadísticos del flujo y tráfico de red son limitados, prácticamente no se llevan en un registro histórico de por lo menos dos años.
- El sistema eléctrico ya dio su vida útil, no se ha brindado mantenimiento total a la infraestructura eléctrica dentro de un margen de 10 años.

Conclusiones:

El área de administración de la Universidad es la encargada de proveer a toda la *UNA* los elementos que atañen a las operaciones y mantenimiento de los bienes y materiales propios de la universidad. *OTIC-UNA* es la encargada de coordinar los presupuestos, con el área previamente mencionada, o las debidas acciones de corrección y mantenimiento para el buen funcionamiento de TI.

Toda adquisición de equipos de red debe ser aprobado por el área de administración (salvo los casos de las Facultades que pueden hacer uso de su presupuesto interno para adquirir equipos de cómputos); una vez aprobado gran parte de los equipos, como los servidores, switch, routers, cableado, etc. pasan a ser supervisión inmediata de *OTIC-UNA*.



Modelo de Madurez:



Estado Actual: **Repetible pero Intuitivo**

La organización está consciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de habilitación para el operador y hay algunos estándares de operación formales.

Recomendaciones:


- Definir e implementar procedimientos estándar para las operaciones de TI.
- Redactar y mantener un registro de actividades del personal.
- Definir procedimientos para retomar automáticamente las aplicaciones en caso de una interrupción accidental.
- Elaborar un reglamento escrito y actualizado que precise las responsabilidades de las personas.
- Elaborar un documento con la clasificación formalmente establecida de las aplicaciones usadas, según orden decreciente de su nivel de sensibilidad.



- Mantener un registro de actividades del personal que por lo menos incluya lo siguiente:
 - Nombre de la persona.
 - Errores.
 - Acciones correctivas.
 - Área específica donde fue llevada a cabo la actividad.
 - Detalles de presupuesto.
- Hacer uso de calendarización formal para el seguimiento o detalles propuestos de actividades.

Monitorear y Evaluar ME1

Monitorear y Evaluar el Desempeño de TI

Dominio:	Monitorear y Evaluar
Proceso:	ME1: Monitorear y Evaluar el Desempeño de TI
Objetivo de control:	Establecer un procedimiento de monitoreo que garantice la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos, tomando medidas expeditas cuando existan desviaciones.
Enfoque:	Monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño.
Herramienta de recopilación de la información	<div>Entrevista</div>  <div>Detalle de Recomendaciones (M1).rtf</div>
Hallazgos	
<ul style="list-style-type: none"> • No existe un marco general de monitoreo. • No se han definido medidas, metas y comparaciones de referencias balanceados. 	



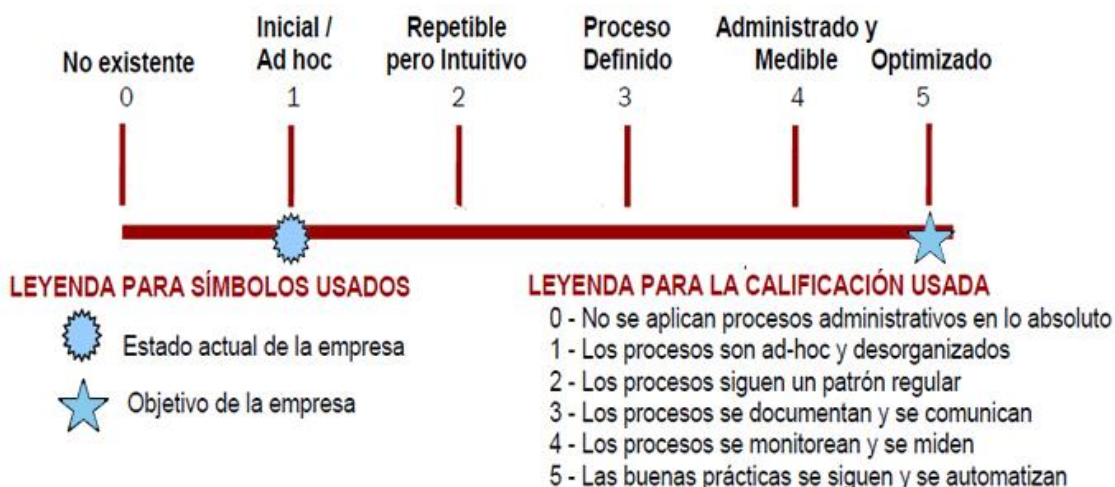
- No existen indicadores de desempeño.
- No se cuentan con procesos para recopilar datos oportunos y precisos para informar acerca del progreso respecto a los objetivos establecidos.
- No existen procesos de monitoreo como tableros de control.
- No existen informes administrativos para la revisión del progreso de la institución.
- No se evalúa el uso de las mejores prácticas internacionales para la adecuación aplicable a la red de computadoras.

Conclusiones:

Una meta o un objetivo sin seguimiento o monitoreo posterior a su implementación es ineficaz y no tiene sentido; el modelo planteado dentro de la UNA técnicamente no está monitoreado por la alta dirección involucrada directamente a la red de computadora.

Es vital para la institución dar seguimiento a las nuevas tendencias implementadas en ámbito de red y modernizar lo que una vez está obsoleto para mantener la competitividad, no sólo nacional, sino internacional en términos educativos.

Modelo de Madurez:



Estado Actual: **Inicial/Ad Hoc**



La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna pérdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.

Recomendaciones:

- Establecer un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI.
- Integrar el marco de trabajo con el sistema de administración del desempeño institucional.
- Trabajar con la institución para definir un conjunto balanceado de objetivos de desempeño y tenerlos aprobados por OTIC-UNA y otros interesados relevantes.
- Desarrollar un método de monitoreo que se ejecute en tiempo real y adecuado a las necesidades de la Universidad.
- Se debe proporcionar reportes administrativos para ser revisados por la alta dirección, estos reportes deben de contener:
 - Grado en el que se han alcanzado los objetivos planteados.
 - Entregables obtenidos.
 - Metas de desempeño alcanzadas.
 - Riesgos mitigados.
- Es necesario identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.



VI. Conclusiones

La evaluación del sistema de control interno realizada permitió determinar falencias e identificar oportunidades de mejora, las cuales se encuentran reflejadas en las conclusiones y recomendaciones que son de fácil adopción por parte de los involucrados en los procesos, aspectos muy necesarios en los niveles de control para lograr una administración más eficaz.

Se verificó que las actividades de control de la red de computadoras determinen el cumplimiento de normas internacionales de estandarización en los mecanismos de hardware e instalación de la misma, encontrando hallazgos relevantes que reflejan la falta de buenas prácticas al momento de implementar normas internacionales. Si bien es cierto, en la praxis la red de computadoras es plenamente funcional, no significa que los detalles importantes omitidos en la implementación de la configuración, basado en normas internacionales, no sean necesarias.

El uso de Cobit 4.1 fue fundamental para establecer las bases de la auditoría, por lo tanto se determinó que la Universidad Nacional Agraria es perfectamente auditable en materia de Informática; los instrumentos de medición, como encuestas, entrevistas, observación y evidencias fotográficas dieron como resultado la emisión de un informe de auditoría que fue plasmado a lo largo de éste trabajo monográfico.

La evaluación por grados de madurez de los procesos de TI en la Universidad Nacional Agraria, ha permitido determinar la posición en la que se encuentra ubicada la organización, emitiendo de esta manera las recomendaciones a ser tomadas en cuenta a corto y largo plazo¹⁴.

¹⁴ Véase también el Anexo 3: “Niveles de Madurez de la Universidad Nacional Agraria”



VII. Recomendaciones

Finalizando con el proceso de revisión a los controles de informática de la *UNA*, se recomienda aplicar las siguientes sugerencias que ayudarán a la red de computadoras a tener el mejor desempeño y competitividad internacional:

1. Se sugiere tomar en cuenta las recomendaciones planteadas en los diferentes controles auditados en el transcurso de la auditoría y que están debidamente documentados a lo largo de éste trabajo monográfico.
2. La *UNA* necesita alinear los objetivos de la institución con los objetivos de TI. De esta forma la organización puede mejorar su desempeño al acoplar las nuevas tecnologías de la información y comunicación y el aumento de sus niveles de servicio.
3. La organización necesita comprender cómo los servicios de TI apoyan y afectan soluciones críticas del negocio, para esto es necesario formular los objetivos y metas de TI de tal forma que se alineen a los objetivos y metas de la Universidad.
4. Estudiar la implementación de un marco de trabajo basado en mejores prácticas. Esto permitirá a la institución ganar valor en los servicios de TI, optimizando la calidad, la respuesta y la fiabilidad de los servicios de TI.
5. Promover un comité de TI conformado por funcionarios de alto nivel de las distintas áreas operativas, a fin de recoger las necesidades para formular, aprobar y/o actualizar un marco de trabajo de TI.
6. Incluir un auditor de TI dentro del departamento de auditoría interna que se encargue de evaluar los controles implementados y se encargue de garantizar la integración de controles en los nuevos desarrollos.
7. La Gerencia de TI deberá tomar en consideración cada uno de los procesos que se encuentran en un grado de madurez "No Existente"; ya que los mismos se encuentran en un estado crítico y son los que requieren atención inmediata.



VIII. Glosario de Términos

Antivirus: Programa que detecta la amenaza de software maliciosos, conocidos como virus, pudiendo neutralizar los efectos.

Aplicaciones: Programa preparado para una utilización específica, como el pago de nóminas, formación de un banco de términos léxicos, etc.

Auditoría: Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. Conjunto de métodos y técnicas con los que se preocupa identificar y evaluar algo.

Auditoría Informática: Evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoria, incluyendo el uso de software.

Bridge: Puente de red. Es el dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Cable: Cordón formado con varios conductores aislados unos de otros y protegido generalmente por una envoltura que reúna la flexibilidad y resistencia necesarias al uso a que el cable se destine.

Cisco: Es una empresa global con sede en San José, California, EU; principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CMD: Es el intérprete de comandos de los sistemas basados en Windows NT. Viene del inglés Command Prompt, que en español es Símbolo del sistema.

Control Interno: Cualquier actividad o acción realizada manual y/o automáticamente prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

Data Warehouse: Es una colección de datos orientada a un determinado ámbito, integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza.



Dato: Información dispuesta de manera adecuada para su tratamiento por un ordenador.

Dominio: Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI.

Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Gateway: Puerta de enlace. Es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.

Gestión: Diligencias conducentes al logro de un negocio o de un deseo cualquiera.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Hallazgo: Debilidades, deficiencias o brechas apreciables respecto a un criterio o estándar previamente definido.

IEEE: Instituto de Ingeniería Eléctrica y Electrónica. Es una asociación mundial de ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

ISP: Proveedor de acceso a Internet normalmente bajo una cuota monetaria y contratación, generalmente se establece conexión a través de acceso telefónico o banda ancha (cable o ADSL).

Información: Conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

Mantenimiento Correctivo: Es aquel mantenimiento que se realiza con el fin de corregir o reparar un fallo en el equipo o instalación.



Mantenimiento Preventivo: Consiste en llevar a cabo un seguimiento del funcionamiento a nivel hardware y software de un sistema. Se vigila constantemente el estado de este y se llevan a cabo medidas preventivas para evitar fallos.

Objetivo de Control: Una declaración del resultado o propósito que se desea alcanzar al implementar. Procedimientos de control en un proceso en particular.

Paquete: Conjunto de servicios que se ofrecen o de requisitos que se exigen.

POA: El plan operativo es un documento oficial en el que los responsables de una organización o fragmento del mismo, enumeran los objetivos y las directrices que deben cumplir en el corto plazo.

Políticas: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Procedimiento: Es un método de ejecutar una serie común de pasos definidos que permite realizar un trabajo en forma correcta.

Router: Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Red: Sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a otra.

Riesgo: Es la vulnerabilidad de los bienes de una institución ante un posible o potencial perjuicio o daño.



Seguridad Física: Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Seguridad Lógica: Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Servicios: Función o prestación desempeñadas por organizaciones y su personal.

Servidor: En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Sistemas Operativos: Es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema.

Subredes: Son un método para maximizar el espacio de direcciones ipv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una red interna mayor. En cualquier clase de dirección, las subredes proporcionan un medio de asignar parte del espacio de la dirección host a las direcciones de red, lo cual permite tener más redes. La parte del espacio de dirección de host asignada a las nuevas direcciones de red se conoce como número de subred.

TI: Tecnología de información. Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizado y utilizado en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad



IX. Bibliografía

- Alonso Rivas, G. (1988). *Auditoría Informática*. Madrid, España: Díaz de Santos.
- Arebalos, A. (Marzo-Abril de 2010). América Latina y la penetración de Internet. *Mercados y tendencias*(38), 110.
- Canales Mena, E. (2006). *Auditoría física en la Facultad de Ingeniería Química*. Tesis inédita de Ingeniería, Universidad Nacional de Ingeniería, Managua.
- Cartaya, M. (2009). *Riesgo de Auditoría*. Caracas, Distrito Capital, Venezuela: COFAE.
- Controlaría General de la República. (Julio de 2009). *Manual de Auditoría Gubernamental. Auditoría Informática, VIII, 5*. Managua, Nicaragua.
- Del Peso Navarro, E., & Piattini, M. (2003). *Auditoría Informática: Un enfoque práctico* (Segunda Ampliada ed.). Madrid, España: RA-MA.
- Echenique García, J. (2002). *Auditoría en Informática* (Segunda ed.). México D.F., México: McGraw Hill.
- Espinola, M. (2007). *Cobit 4.0 y el control de proyectos TIC*. Obtenido de www.gestionpublica.cl/gerenciapublica/tema/35/cobit-4.0-y-control-de-proyectos-tic
- Federación Internacional de Contabilidad. (2007). *Riesgos de Auditoría: Conceptos y Componentes. NIA 200*, 102.
- Instituto Mexicano de Contadores Públicos, A.C. (2004). *Normas Internacionales de Auditoría* (Séptima ed.). México D.F., México, México.
- IT Governance Institute. (2007). *Cobit* (4.1 ed.). Illinois, Estados Unidos: ISACA.
- Maiwald, E. (2005). *Fundamentos de seguridad de redes* (Segunda ed.). México D.F., México: McGraw Hill.
- Mosquera Vizuite, D. (2006). *Auditoría informática, guía didáctica* (Primera ed.). Loja, Ecuador: Universidad Técnica Particular de Loja.
- Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales* (Primera ed.). México D.F., México: Pearson Educación.
- Piattini, M., & Del Peso, E. (2001). *Auditoría Informática: Un enfoque práctico* (Segunda ed.). México D.F., México: Alfaomega.
- Piura López, J. (2006). *Metodología de la Investigación científica: Un enfoque integrador* (Primera ed.). Managua, Managua, Nicaragua: PAVSA.
- Tanenbaum, A. (2003). *Redes de computadoras* (Cuarta ed.). (E. Núñez Ramos, Ed.) México D.F., México: Pearson Educación.
- Universidad Nacional Agraria. (Octubre de 2015). Obtenido de www.una.edu.ni



X. Anexos



Anexo 1. Objetivos de control de CobIT

Planificar y Organizar			
PO1	Definir un Plan Estratégico de TI		
1.1	Administrar el valor de TI	1.4	Plan estratégico de TI
1.2	Alineación de TI con el negocio	1.5	Planes Tácticos de TI
1.3	Evaluación del desempeño y la capacidad actual	1.6	Administración del portafolio de TI
PO2	Definir la Arquitectura de la Información		
2.1	Modelo de Arquitectura de información empresarial	2.3	Esquema de clasificación de datos
2.2	Diccionario de datos empresarial y regla de sintaxis de datos	2.4	Administración de integridad
PO3	Determinar la Dirección Tecnológica		
3.1	Planeación de la dirección tecnológica	3.4	Estándares tecnológicos
3.2	Plan de infraestructura tecnológica	3.5	Consejo de arquitectura de TI
3.3	Monitoreo de tendencias y regulaciones futuras		
PO4	Definir los procesos, organizaciones y relaciones de TI		
4.1	Marco de trabajo de procesos de TI	4.9	Propiedad de datos y sistemas
4.2	Comité estratégico de TI	4.10	Supervisión
4.3	Comité directivo de TI	4.11	Segregación de funciones
4.4	Ubicación organizacional de la función de TI	4.12	Personal de TI
4.5	Estructura organizacional	4.13	Personal clave de TI
4.6	Establecimiento de roles y responsabilidades	4.14	Políticas y procedimientos para personal contratado
4.7	Responsabilidad de aseguramiento de calidad de TI	4.15	Relaciones
4.8	Responsabilidad, sobre el riesgo, la seguridad y el cumplimiento		
PO5	Administrar la inversión en TI		
5.1	Marco de trabajo para la administración financiera	5.4	Administración de costos de TI
5.2	Prioridades dentro del presupuesto de TI	5.5	Administración de beneficios
5.3	Proceso presupuestal		
PO6	Comunicar las aspiraciones y la dirección de la gerencia		
6.1	Ambiente de políticas y de control	6.4	Implantación de políticas para TI
6.2	Riesgo corporativo y marco de referencia de control interno de TI	6.5	Comunicación de los objetivos y la dirección de TI
6.3	Administración de políticas para TI		
PO7	Administrar recursos humanos de TI		



7.1	Reclutamiento y retención del personal	7.5	Dependencia sobre los individuos
7.2	Competencias del personal	7.6	Procedimientos de investigación del personal
7.3	Asignaciones de roles	7.7	Evaluación del desempeño del empleado
7.4	Entrenamiento del personal de TI	7.8	Cambios y terminación de trabajo
PO8	Administrar la Calidad		
8.1	Sistema de administración de la calidad	8.4	Enfoque en el cliente de TI
8.2	Estándares y prácticas de calidad	8.5	Mejora continua
8.3	Estándares de desarrollo y de adquisición	8.6	Medición, monitoreo y revisión de la calidad
PO9	Evaluar y administrar los riesgos de TI		
9.1	Alineación de la administración de riesgos de TI y del negocio	9.4	Evaluación de riesgos de TI
9.2	Establecimiento del contexto del riesgo	9.5	Respuesta de riesgos
9.3	Identificación de eventos	9.6	Mantenimiento y monitoreo de un plan de acción de riesgos
PO10	Administrar proyectos		
10.1	Marco de trabajo para la administración de programas	10.8	Recursos del proyecto
10.2	Marco de trabajo para la administración de proyectos	10.9	Administración de riesgos del proyecto
10.3	Enfoque de administración de proyectos	10.10	Control de cambios del proyecto
10.4	Compromiso de los interesados	10.11	Planeación del proyecto y métodos de aseguramiento
10.5	Declaración de alcance de proyecto	10.12	Medición del desempeño, reportes y monitoreo del proyecto
10.6	Inicio de la fases del proyecto	10.13	Cierre del proyecto
10.7	Plan integrado del proyecto		
Adquirir e implementar			
AI1	Identificar soluciones automatizadas		
1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	1.3	Estudio de factibilidad y formulación de recursos de acción alternativos
1.2	Reporte de los análisis de riesgos	1.4	Requerimientos, decisión de factibilidad y aprobación
AI2	Adquirir y mantener software aplicativo		
2.1	Diseño de alto nivel	2.6	Actualizaciones importantes en sistemas existentes



2.2	Diseño detallado	2.7	Desarrollo de software aplicativo
2.3	Control y posibilidad de auditar las aplicaciones	2.8	Aseguramiento de la calidad del software
2.4	Seguridad y disponibilidad de las aplicaciones	2.9	Administración de los requerimientos de aplicaciones
2.5	Configuración e implementación de software aplicativo adquirido	2.10	Mantenimiento de software aplicativo
AI3	Adquirir y mantener infraestructura tecnológica		
3.1	Plan de adquisición de infraestructura tecnológica	3.3	Mantenimiento de la infraestructura
3.2	Protección y disponibilidad del recurso de infraestructura	3.4	Ambiente de prueba de factibilidad
AI4	Facilitar la operación y el uso		
4.1	Plan para soluciones de operación	4.3	Transferencia de conocimiento a usuario finales
4.2	Transferencia de conocimiento a la gerencia del negocio	4.4	Transferencia de conocimiento al personal de operaciones y soporte
AI5	Adquirir recursos de TI		
5.1	Control de adquisición	5.3	Selección de proveedores
5.2	Administración de contratos con proveedores	5.4	Adquisición de recursos de TI
AI6	Administrar cambios		
6.1	Estándares y procedimientos para cambios	6.4	Seguimientos y reportes del estatus de cambio
6.2	Evaluación de impacto, priorización y autorización	6.5	Cierre y documentación del cambio
6.3	Cambios de emergencia		
AI7	Instalar y acreditar soluciones y cambios		
7.1	Entrenamiento	7.6	Pruebas de cambio
7.2	Plan de prueba	7.7	Prueba de aceptación final
7.3	Plan de implantación	7.8	Promoción a producción
7.4	Ambiente de prueba	7.9	Revisión posterior a la implantación
7.5	Conversión de sistemas y datos		
Entregar y dar soporte			
DS1	Definir y administrar los niveles de servicio		
1.1	Marco de trabajo de la administración de los niveles de servicio	1.4	Acuerdos de niveles de operación
1.2	Definición de servicios	1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio



1.3	Acuerdos de niveles de servicio	1.6	Revisión de los acuerdos de niveles de servicio y de los contratos
DS2	Administrar los servicios de terceros		
2.1	Identificación de todas las relaciones con los proveedores	2.3	Administración de riesgos del proveedor
2.2	Gestión de relaciones con proveedores	2.4	Monitoreo del desempeño del proveedor
DS3	Administrar el desempeño y la capacidad		
3.1	Planeación del desempeño y la capacidad	3.4	Disponibilidad de recursos de TI
3.2	Capacidad y desempeño actual	3.5	Monitorio y reporte
3.3	Capacidad y desempeño futuros		
DS4	Garantizar la continuidad del servicio		
4.1	Marco de trabajo de continuidad de TI	4.6	Entrenamiento del plan de continuidad de TI
4.2	Planes de continuidad de TI	4.7	Distribución del plan de continuidad de TI
4.3	Recursos críticos de TI	4.8	Recuperación del plan de continuidad de TI
4.4	Mantenimiento del plan de continuidad de TI	4.9	Almacenamiento de respaldos fuera de las instalaciones
4.5	Pruebas del plan de continuidad de TI	4.10	Revisión post reanudación
DS5	Garantizar la seguridad de los sistemas		
5.1	Administración de la seguridad de TI	5.7	Protección de tecnología de la seguridad
5.2	Plan de seguridad de TI	5.8	Administración de llaves criptográficas
5.3	Administración de identidad	5.9	Prevención, detección y corrección de software malicioso
5.4	Administración de cuentas de usuario	5.10	Seguridad de la red
5.5	Pruebas, vigilancia y monitoreo de la seguridad	5.11	Intercambio de datos sensitivos
5.6	Definición de incidente de seguridad		
DS6	Identificar y asignar costos		
6.1	Definición de servicios	6.3	Modelación de costos y cargos
6.2	Contabilización de TI	6.4	Mantenimiento del modelo de costos
DS7	Educar y entrenar a los usuarios		
7.1	Identificación de necesidades de entrenamiento y educación	7.3	Evaluación del entrenamiento recibido
7.2	Impartición de entrenamiento y educación		



DS8	Administrar la mesa de servicio y los incidentes		
8.1	Mesa de servicios	8.4	Cierre de incidentes
8.2	Registro de consultas de clientes	8.5	Análisis de tendencias
8.3	Escalamiento de incidentes		
DS9	Administrar la configuración		
9.1	Repositorio y línea base de configuración	9.3	Revisión de integridad de la configuración
9.2	Identificación y mantenimiento de elementos de configuración		
DS10	Administrar los problemas		
10.1	Identificación y clasificación de los problemas	10.3	Cierre de problemas
10.2	Rastreo y resolución de problemas	10.4	Integración de las administraciones de cambios, configuración y problemas
DS11	Administrar los datos		
11.1	Requerimientos del negocio para la administración de los cambios	11.4	Eliminación
11.2	Acuerdos de almacenamiento y conservación	11.5	Respaldo y restauración
11.3	Sistema de administración de librerías de medios	11.6	Requerimientos de seguridad para la administración de datos
DS12	Administración al ambiente físico		
12.1	Selección y diseño del centro de datos	12.4	Protección contra factores ambientales
12.2	Medidas de seguridad física	12.5	Administración de instalaciones físicas
12.3	Acceso físico		
DS13	Administrar las operaciones		
13.1	Procedimientos e instrucciones de operación	13.4	Documentos sensitivos y dispositivos de salida
13.2	Programación de tareas	13.5	Mantenimiento preventivo del hardware
13.3	Monitoreo de la infraestructura de TI		
Monitorear y evaluar			
ME1	Monitorear y evaluar el desempeño de TI		
1.1	Enfoque del monitoreo	1.4	Evaluación del desempeño
1.2	Definición y recolección de datos de monitoreo	1.5	Reportes al consejo directivo y a ejecutivos
1.3	Método de monitoreo	1.6	Acciones correctivas
ME2	Monitorear y evaluar el control interno		
2.1	Monitoreo del marco de trabajo de control interno	2.5	Aseguramiento del control interno
2.2	Revisiones de auditoria	2.6	Control interno para terceros



2.3	Excepción de control	2.7	Acciones correctivas
2.4	Control de autoevaluación		
ME3	Garantizar el cumplimiento con requisitos externos		
3.1	Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales	3.4	Aseguramiento positivo del cumplimiento
3.2	Optimizar la respuesta a requerimientos externos	3.5	Reportes integrados
3.3	Evaluación del cumplimiento con requerimientos externos		
ME4	Proporcionar gobierno de TI		
4.1	Establecimiento de un marco de gobierno de TI	4.5	Administración de riesgos
4.2	Alineamiento estratégico	4.6	Medición del desempeño
4.3	Entrega de valor	4.7	Aseguramiento independiente
4.4	Administración de recursos		



Anexo 2. Modelo genérico de Madurez

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura 2. El modelo genérico de madurez brinda una mejor comprensión de evaluación y calificación tanto para el Auditor como para las partes interesadas.



Anexo 3. Niveles de Madurez de la Universidad Nacional Agraria

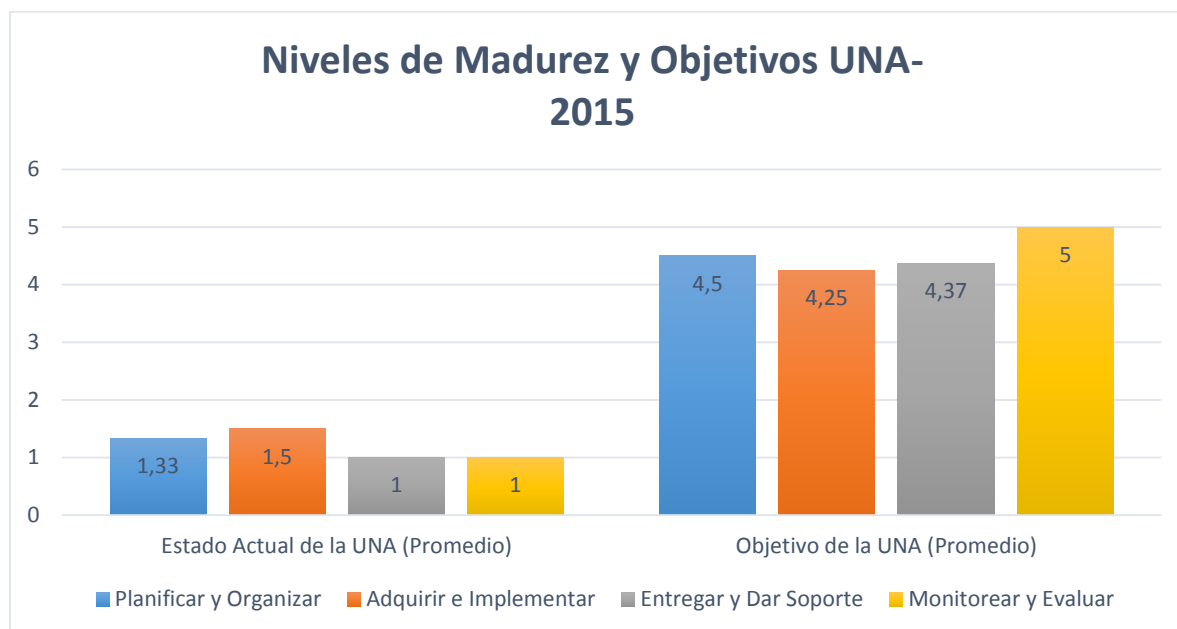


Figura 3. Gráfica Niveles de Madurez UNA. Estado actual Vs Objetivo de la UNA



Figura 4. Esquema de Modelo de madurez UNA reflejando el estado actual en la recta de valoración.



Anexo 4. Encuesta a los usuarios

1. ¿Considera que los servicios de redes le brindan los resultados esperados?
SI NO ¿por qué?
2. De forma general. ¿Cómo considera usted el servicio brindado por el área de redes?
A. Deficiente B. Aceptable C. Satisfactorio D. Excelente
¿Por qué?
3. ¿Qué piensa de la asesoría y atención que imparte el personal del área de redes a los usuarios?
A. No se proporciona C. Satisfactoria
B. Es insuficiente D. Excelente
4. ¿Qué piensa de la seguridad, proporcionada por el área de redes, en el manejo de la información, datos y archivos del cual usted hace uso?
A. Nula D. Excelente
B. Riesgosa E. Lo Desconozco
C. Satisfactoria
¿Por qué?
5. Para usted, ¿Existen fallas o elementos en los que el área de redes debe mejorar?
¿Cuáles?
6. Según su criterio, ¿Sigue algún procedimiento formal para dar un uso adecuado a la red de la Universidad y los elementos que contiene (Internet, dispositivos, información, etc)?
SI NO
¿A qué se debe?
7. En términos de rapidez, ¿cómo evalúa la velocidad de la red interna en la Universidad?
A. Muy Lento B. Lento C. Normal
D. Optima

Anexo 5. Evidencias de Auditoría



Figura 5. Switch y estabilizador ubicado a 2.4 mts sobre el piso en el edificio de administración. Muestra de cómo no se ejecutan las buenas prácticas de limpieza de los dispositivos y sus alrededores.

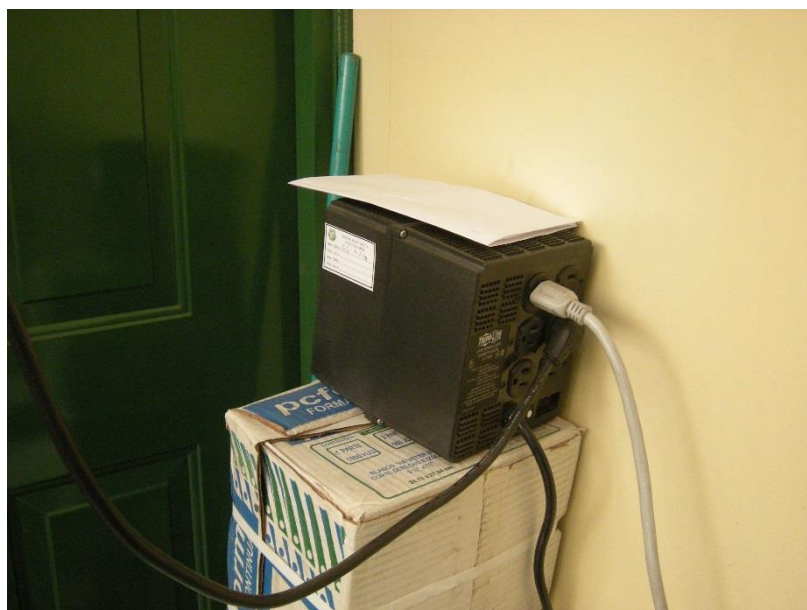


Figura 6. Estabilizador eléctrico sobre cajas apiladas con alto riesgo de caída, pudiendo provocar inestabilidad en los dispositivos conectados.

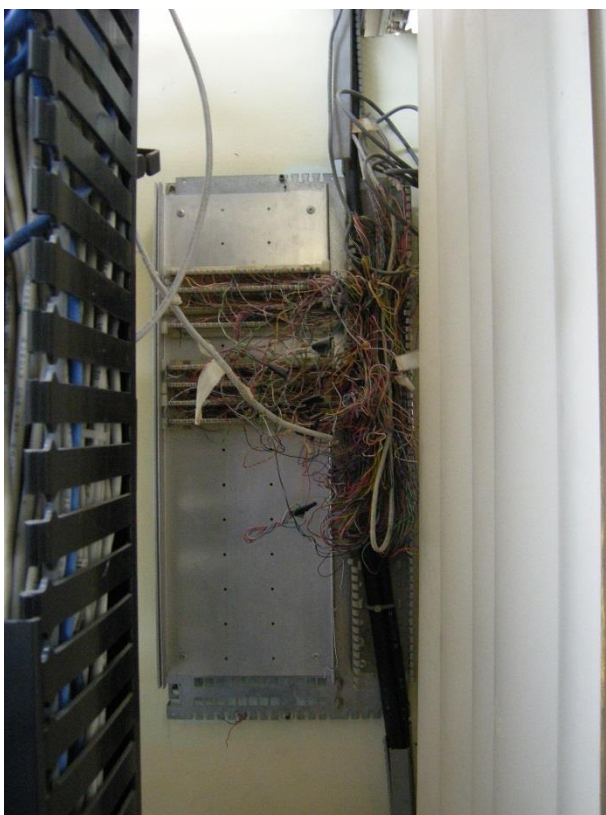


Figura 7. Conexión cableada de electricidad en bajo voltaje en desuso, pero no dada de baja, no hay gestión de los elementos de red obsoletos.



Figura 8. Gabinete de un nodo principal en la oficina del Administrador, el acceso no es debidamente controlado.



Figura 9. Aire acondicionado apagado en horas laborales y con presencia de dispositivos de red que requieren cuarto frío.



Figura 10. Antena principal de conexión remota con el ISP, ubicado sobre el edificio CENIDA.

Backbone

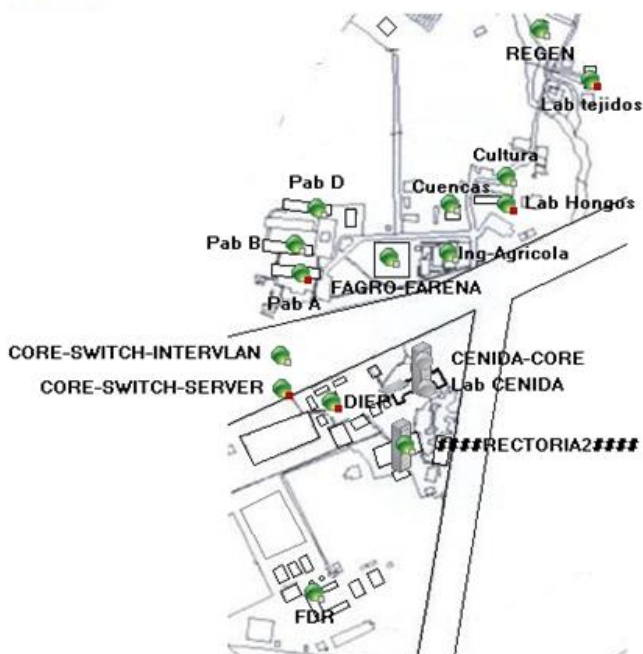


Figura 11. El sistema Orion permite a los administradores de la red monitorear los nodos de la infraestructura. Los puntos verdes representan un estado habilitado de trabajo.



Figura 12. Mapa de red plasmado en una pizarra acrílica, fácilmente visible por quienes acceden al cuarto de servidores.

Distorsión intencional para evitar manipulación de números IP de forma indebida.



Figura 13. Cable UTP Categoría 5, instalados de forma incorrectas, sin mantenimiento y violando las normas de buenas prácticas para su debido manejo.



Anexo 6. Ejemplo de Cuestionario Meycor Cobit

Formulario de Evaluación de Procesos

13 - Adquisición y mantenimiento de la infraestructura tecnológica (AI3)

Dominio: Adquisición e Implementación

1) 1.1) ¿Se elabora un plan para la adquisición, implementación y mantenimiento de la infraestructura tecnológica que satisface los requerimientos técnicos y funcionales de negocio establecidos y que es acorde con la dirección tecnológica de la organización?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

1.2) ¿Este plan considera una flexibilidad futura para la ampliación de la capacidad, los costos de transición, los riesgos técnicos y la vigencia de la inversión para las mejoras de tecnología?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

1.3) ¿Se evalúan los costos de complejidad y la viabilidad comercial del proveedor y el producto al incorporar una nueva capacidad técnica?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

1.4) ¿Tiene en cuenta la adquisición de software de base, aspectos tales como costo/beneficio, compatibilidad, demandas de los usuarios, capacitación y necesidades futuras? ¿Es la elección el resultado de un estudio de factibilidad formalizado en un informe técnico?

Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

1.5) ¿Se toma en cuenta, en la selección del hardware, aspectos tales como:

a) Antecedentes del proveedor

b) Nivel del servicio de mantenimiento técnico



c) Capacidad de tolerancia a las fallas de la tecnología a adquirir contra el grado de criticidad de las aplicaciones a procesar

d) Previsiones de redundancia de equipos cuando es presupuestariamente posible

e) Equipos similares existentes en la plaza?

Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

1.6) ¿Existe una práctica de realización de test de aceptación para el software de base a ser adquirido de terceros?

Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2) 2.1) ¿Se implementan medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de infraestructura a fin de proteger los recursos y garantizar la disponibilidad e integridad?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.2) ¿Se definen y comprenden claramente las responsabilidades por el uso de los componentes de infraestructura sensibles por parte de los encargados de desarrollar e integrar los mismos?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.3) ¿Se evalúa y monitorea el uso de estos componentes de infraestructura sensibles?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.4) ¿El acceso a las herramientas de auditoría del sistema tales como el software o los archivos de datos son protegidos para prevenir cualquier uso erróneo o compromiso posible?



Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.5) ¿El equipamiento, la información o el software pueden ser retirados de la organización sin la autorización apropiada?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.6) ¿El personal está al tanto de estos chequeos puntuales o auditorías?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.7) ¿Está debidamente controlado el uso de utilidades del sistema, incluidas en las instalaciones informáticas, que pueden eludir las medidas de control del sistema o de las aplicaciones?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.8) ¿Existe algún control de la red para asegurarse que las conexiones de computadoras y los flujos de información no rompen con la política de control de accesos de las aplicaciones del negocio? Esto es a menudo esencial para las redes compartidas con usuarios que no son de la organización.

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.9) ¿Existe algún proceso formal para hacer públicamente disponible la información de la organización?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____



2.10) ¿La computadora o el dispositivo de la comunicación tiene la capacidad de tener un reloj en tiempo real? Éste se debe fijar a un estándar convenido tal como tiempo coordinado universal u hora estándar local.

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.11) ¿Las terminales inactivas en áreas públicas están configuradas para despejar la pantalla o apagarse automáticamente luego de un determinado período de inactividad?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.12) ¿Los accesos a puertos de diagnóstico son controlados? Por ej., protegidos por un mecanismo de seguridad.

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.13) ¿Los controles de ruteo están basados en el mecanismo de identificación positiva del origen y del destino? Ejemplo: Conversión de dirección de Red (NAT: Network Address Translation)

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.14) ¿Los usuarios y los proveedores están enterados de los requisitos y los procedimientos de seguridad para proteger equipos desatendidos, así como su responsabilidad de poner tal protección en práctica?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.15) ¿Se realizan chequeos puntuales o auditorías periódicas con el fin de detectar traslados no autorizados de propiedad?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable



Comentario: _____

2.16) ¿Hay controles implantados para proteger la integridad de la información públicamente disponible contra acceso no autorizado?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.17) ¿Esto incluye controles tales como Firewalls, reforzamiento del sistema operativo, herramienta para la detección de intrusos para supervisar el sistema, etc.?

Clasificación: **ISO 17799**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.18) ¿Se revisa la selección de los parámetros de control del software de base periódicamente ajustándose cuando varía la carga del trabajo y el ambiente de control de la organización?

Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.19) ¿Se cuenta con software de base especializado en seguridad tales como:

- a) Software de control de acceso y registración de pistas de auditoría
- b) Software de seguridad de bibliotecas de programación y seguimiento del ciclo de vida del desarrollo de sistemas
- c) Software comparador para la automatización de la tarea de control de cambios
- d) Software criptográfico
- e) Software detector de rutinas no usualmente ejecutadas (posible caballo de Troya)
- f) Software antivirus?

Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

2.20) ¿Se supervisa constantemente el funcionamiento del hardware, verificando al mismo tiempo su situación contractual en lo relativo a si está en el período de garantía o bajo contrato de mantenimiento o sin cobertura de este último?



Clasificación: **Orientación Específica**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

3) 3.1) ¿Se desarrolla una estrategia y un plan para el mantenimiento de la infraestructura y se garantiza que los cambios son controlados en línea con el procedimiento de gestión de cambios de la organización?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

3.2) ¿Se incluyen revisiones periódicas en relación a las necesidades del negocio, la gestión de correcciones y las estrategias de mejora, los riesgos, las evaluaciones de vulnerabilidades y los requerimientos de seguridad?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

4) 4.1) ¿Se establecen entornos de prueba y desarrollo para apoyar la viabilidad eficaz y eficiente y la integración de las pruebas de las aplicaciones y la infraestructura en las primeras etapas del proceso de adquisición y desarrollo?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

4.2) ¿Se consideran las funciones, las configuraciones de hardware y software, las pruebas de integración y desempeño, la migración de entornos, el control de las versiones, las herramientas y datos de configuración, y la seguridad?

Clasificación: **COBIT**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____

4.3) ¿Existen bibliotecas que sólo almacenan programas fuente?

Clasificación: **AS/400**

() Bueno () Bueno Regular () Malo () No Aplicable

Comentario: _____



Anexo 7. Ejemplo de formulario de evaluación

Condiciones ambientales y de entorno físico

1. ¿El edificio donde se encuentran los dispositivos y terminales de red están a salvo de:

Inundación?	()
Terremoto?	()
Fuego?	()
Sabotaje?	()
2. ¿El Centro de cómputo da al exterior? SI NO
3. ¿Tiene el cuarto de servidores una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad? SI NO
4. ¿Está el centro de cómputo en un lugar con alto tráfico de personas? SI NO
5. ¿Se tienen paredes, cuyo material de construcción despiden polvo? SI NO
6. ¿Existe lugar suficiente para los equipos? SI NO
7. ¿El piso es antiestático? SI NO
8. ¿La temperatura con la que trabajan los equipos es la recomendada por el proveedor? SI NO
9. ¿Los ductos de aire son los suficientemente anchos para permitir el paso de intrusos? SI NO
- En caso afirmativo:
10. ¿Los ductos de aire cuentan con alarma contra intrusos? SI NO
11. ¿Los ductos de aires están limpios? SI NO



12. ¿Se controla la humedad de acuerdo a las especificaciones del proveedor? SI NO

13. ¿Cada cuánto tiempo? _____

Seguridad de Autorización de accesos

14. ¿Se han adoptado medidas de seguridad en la dirección de informática? SI NO

15. ¿Existe una persona responsable de la seguridad? SI NO

16. ¿Se controla el trabajo fuera del horario? SI NO

17. ¿Se registran las acciones de los operadores para evitar que realicen alguna que puedan dañar el sistema? SI NO

18. ¿Se identifica a las personas que ingresan? SI NO

19. ¿De qué forma? _____

20. ¿Cómo se controla el acceso?

- Vigilante ()
- Recepcionista ()
- Tarjeta de control de acceso ()
- Puerta de combinación ()
- Puerta con cerradura ()
- Puerta electrónica ()
- Puerta sensorial ()
- Registro de entradas ()
- Alarmas ()
- Tarjetas magnéticas ()
- Control biométrico ()
- Identificación personal ()

21. ¿Existe vigilancia en el cuarto de servidores las 24 horas del día? SI NO

22. ¿Existe un registro de los acceso al cuarto principal de servidores? SI NO