# Introducción

La Universidad Nacional Agraria (UNA), es una institución de enseñanza superior, la más antigua y de mayor experiencia en la especialidad agrícola en Nicaragua. Durante sus años de existencia, ha trabajado en pro de una transformación sistemática, cumpliendo la misión de formar profesionales; así como también, desarrollar programas de investigación y extensión agropecuaria, que le permitan responder a los diferentes modelos de desarrollo que el país ha experimentado.

Adicionalmente, con el objetivo de brindar un mejor servicio a las diferentes Facultades, la *UNA* realizó un proceso de modernización y actualización de su infraestructura de red de computadoras en la sede Managua. Actualmente, es de su interés evaluar los controles establecidos en el área de las redes, 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.

# Antecedentes

En Nicaragua las auditorías en informáticas han tenido lugar, producto de la globalización, desde la década de los 90 cuando los sistemas computacionales adquirieron mayor complejidad en las instituciones públicas y privadas. Con el tiempo surgieron consultorías privadas que ofrecen el servicio de aplicación del COBIT para auditorías en informática.

Durante el II semestre del año 2013, como proyecto de curso de la asignatura de Ingeniería de Software III, de la carrera de Ingeniería en Computación, se realizó un auditoria informática de red (basada en los criterios y objetivos de control de COBIT 4.1), en la sub-red del edificio de administración de la *UNA* sede Managua, ubicada en el km 12 carretera panamericana norte, dicha auditoría fue realizada por los bachilleres: Eduardo Villalobos, Ingrid Silva y Mijaíl Estrada, generando un informe de auditoría (Villalobos, Silva, & Mijaíl , 2013) entregado a satisfacción al Ing. Marlon Serrano, Administrador de Red de la *UNA*.

Cabe señalar que el trabajo de auditoría en el año 2013, representó tan sólo el 10% de la estructura de red de la *UNA;* motivo por el cual la auditoria de red descrita en el presente trabajo monográfico se desarrollará sobre el 80% de la estructura física y lógica de la red global de la sede Managua, el 10% restante se omitirá por fines de conveniencia entre ambas partes, puesto que éste último término porcentual representa a la Facultad de Ciencias Animales (*FACA*) conocido también como Hacienda “Santa Rosa” ubicada en un recorrido de 3.2 km desde el núcleo principal de la sede Managua. Por la dificultad al acceso y la poca relevancia que se le da, en lo que a tráfico de datos respecta, él área en cuestión no será incluida en la auditoría informática.

El proceso de auditoría actual, se debe manejar de forma independiente al trabajo concluido en 2013 y se hace mención con fines ilustrativos para reflejar el hecho que ha habido un precedente en el trabajo monográfico.

# Justificación

La Oficina de Tecnología de la Información y Comunicación (OTIC) en la Universidad Nacional Agraria es la encargada de regir en el funcionamiento de la informática derivadas en las disciplinas aplicadas a las necesidades de la universidad. Sin embargo, no cuentan con un área específica cuyo perfil esté diseñado a la auditoría en informática interna.

Basados en una necesidad de competitividad, eficacia y eficiencia la UNA resolvió dar los permisos necesarios para que se suplan, a través de hallazgos auditados, las demandas de documentación con datos específicos de los campos a mejorar y modelos a seguir fundamentados en normas internacionales de calidad y buenas prácticas. Se estima que el escrito detallado con las recomendaciones influirá en la toma de decisiones posteriores para el uso y manejo de las TIC dentro de la universidad.

El producto final, posterior a la auditoría, será plasmado en un documento físico con copia electrónica para la consulta directa de la parte interesada, pertenecientes al área de redes dependientes de OTIC - UNA.

Los auditores deben cumplir con algunos requerimientos generales para proporcionar a los directivos y a los poseedores de los procesos de negocios, seguridad y asesoría respecto a los controles en una organización: ofrecer una seguridad razonable de que se está cumpliendo con los objetivos de control correspondientes; identificar dónde se encuentran las debilidades significativas en dichos controles; justificar los riesgos que pueden estar asociados con tales debilidades, y finalmente, aconsejar a estos ejecutivos sobre las medidas correctivas que deben adoptarse.

Las Directrices de Auditoría COBIT permiten cotejar los procesos específicos de TI con los Objetivos de Control COBIT recomendados para auxiliar a los directivos identificar en qué casos los controles son suficientes, o para asesorar los respecto a los procesos que requieren ser mejorados.

# Objetivos

## ***Objetivo General***

Realizar una Auditoria de Red física y lógica del 80% de las instalaciones de la Universidad Nacional Agraria - sede Managua - utilizando el estándar internacional COBIT a fin de identificar el estado actual de la red y emitir recomendaciones necesarias que permitan a la institución mejorar su infraestructura de red.

## ***Objetivos específicos***

1. Analizar la gerencia de redes, a fin determinar que su función de gestión en la red esté claramente definida.
2. Verificar que las actividades de control de red determinen el cumplimiento de normas internacionales de estandarización para los mecanismos de hardware e instalación de la misma.
3. Investigar las medidas de protección de la información y procesos de la red.
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 los procesos de la red.

# Marco teórico

## ***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).

## ***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.

## ***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 Vizuete, 2006).

Los controles informáticos pueden ser preventivos, detectivos o correctivos.

### 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.

### Controles Detectivos

Siguen los controles preventivos y están diseñados para captar errores que escapan 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.

### 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 detectivos, pero muy frecuentemente se encuentran controles detectivos 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).

## ***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).

## ***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:

1. ***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.

1. ***Encuestas***

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

1. ***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.

## ***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.

## ***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.

## ***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

## ***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).

* 1. ***Auditoría de la red física***

Casi el 50% del campo auditable en el área de red de computadoras (puesto que el otro 50% representa a la parte lógica de la red), está orientado a la estructura física de la red (LAN[[1]](#footnote-1), MAN[[2]](#footnote-2), WAN[[3]](#footnote-3)) 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 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).

* 1. ***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 en carga 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)).

## ***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.

## ***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. (Figura Estructura 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.

### ***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.

### ***Objetivos de control para Auditoría de red*** (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
* DS1 Definir y Administrar niveles de servicio
* DS2 Administrar servicios de terceros
* DS3 Gestión de la calidad y del desempeño del sistema
* 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

### ***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



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.

***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.

# Diseño metodológico

|  |  |
| --- | --- |
| Tipo de investigación: | Empírica |
| Enfoque de investigación: | Cualitativa |
| Nivel de investigación: | Descriptivo |
| Sujetos que intervienen: | Áreas de redes de la Universidad Nacional Agraria sede Managua. |
| Técnicas de recolección de datos: | Cuestionarios escritos, entrevistas y recolección de evidencias según sugerencias diseñadas en CobiT. |
| Instrumentos: | Entrevistas, información documental y observación. |
| Procesamiento de datos: | Herramientas automatizadas como Word y Excel. |

A lo largo del proceso se evaluarán aspectos concernientes a las redes de computadoras. El tiempo con que ocurren las actividades es actual, realizándose para éstos un corte transversal para la secuencia de los datos obtenidos: La naturaleza de éste estudio es aplicativa.

El área de estudio será en la Universidad Nacional Agraria sede Managua, ubicada en el km 12 carretera panamericana norte, previamente seleccionada basándose en el hecho de que utilizan tecnología de red en su gestión de comunicaciones.

En cuanto a los instrumentos utilizados para la recolección de datos, se hará uso de cuestionarios escrito, entrevistas y recolección de evidencias según sugerencias diseñadas en CobiT. El procesamiento de la información se ha hecho mediante tablas que recogen los datos cuantitativos; como producto de la tabulación de las tablas y la información se reflejan resultados en gráficos y recomendaciones notorias. Este conjunto de instrumentos, permiten elaborar una valoración cualitativa sobre los aspectos a evaluar en este trabajo.

Para alcanzar los objetivos planteados, se hizo un plan de trabajo que permita el cumplimiento de los mismos en una secuencia ordenada, para lo cual se llevarán a cabo las siguientes actividades:

1. Consultar bibliografía referente al tema para recopilar información.
2. Reconocer elementos que intervienen en la evaluación de la red física y lógica al ejecutar un proceso de Auditoría Informática basado en CobiT.
3. Examinar los objetivos de control que conllevan durante una Auditoría Informática aplicada a la red.
4. Documentar los resultados del proceso de evaluación ejecutado en la Universidad Nacional Agraria.
5. Redactar el informe final que contendrá las recomendaciones pertinentes que se deberá aplicar a la institución con la finalidad de mejorar sus prácticas respecto a la calidad de la red física y lógica.

# 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.

Asociación de Auditoría y Control de Sistemas de Información. (2014). *ISACA.* Obtenido de http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx

Canales Mena, E. (2006). *Auditoría física en la Facultad de Ingeniería Química.* Tesis inédita de Ingeniería, Universidad Nacional de Ingeniería, Managua.

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

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 Vizuete, 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.

Porras Rodríguez, D. (Junio de 2014). Auditorías Integradas: situación actual en Nicaragua. *Nexo, 27*(1), 17.

Tanenbaum, A. (2003). *Redes de computadoras* (Cuarta ed.). (E. Núñez Ramos, Ed.) México D.F., México: Pearson Educación.

Universidad Nacional Agraria. (2014). *UNA*. Obtenido de http://www.una.edu.ni/index.php/institucional/resena-historica

Villalobos, E., Silva, I., & Mijaíl , E. (2013). *Informe de Auditoria para la asignatura de Ing. de Software 3 "Auditoría de red en el edificio de Administración de la UNA".* Managua: UNI.

1. LAN: Local Area Network – Red de área Local [↑](#footnote-ref-1)
2. MAN: Metropolitan Area Network – Red de área Metropolitana [↑](#footnote-ref-2)
3. WAN: Wide Area Network – Red de área Extendida [↑](#footnote-ref-3)