

16 de enero de 2015  
AU-012-2015

Señores y Señoras  
Consejo Universitario  
Universidad Técnica Nacional

Asunto: Remisión Informe de Contadores  
Públicos

Cordial saludo:

En cumplimiento con el Plan de Trabajo para el año 2014 de la Auditoría Universitaria, se remite para su conocimiento el Informe sobre los Procesos de la Dirección de Informática de la Universidad Técnica Nacional, elaborado por el Despacho Carvajal & Colegiados, Contadores Públicos Autorizados y el Resumen Ejecutivo del Informe.

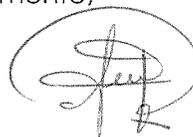
Este Informe fue remitido para cumplimiento de las recomendaciones al Ing. Jairo Bonilla Castro, Director de Informática y puesto en conocimiento a la superior inmediata Licda. Doris Aguilar Sancho, Directora General Administrativa (1).

La Auditoría Universitaria recomienda al Consejo Universitario lo siguiente:

“Solicitar al Director de Informática emitir un informe escrito al menos en forma cuatrimestral, sobre el grado de avance en la implementación de estas recomendaciones.”

Agradezco mantener informada a esta Auditoría sobre las acciones adoptadas al respecto.

Atentamente,



Lic. Jorge Luis Pizarro Palma, Máster  
Auditor General

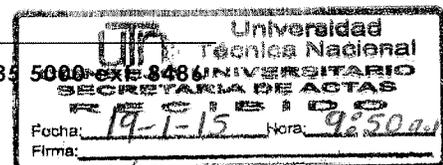


DIRECCIÓN DE INFORMÁTICA  
Rosario Alpizar G.  
16 ENERO 2015 11:53:51

C: Licda. Doris Aguilar Sancho, Directora General Administrativa  
Ing. Jairo Bonilla Castro, M.Et, Director de Informática Universitaria  
Archivo

Manuelle

<sup>1</sup> Oficio AU-011-2015 de fecha 16 de enero 2015.



## Resumen Ejecutivo

### Informe de Contadores Públicos Procesos de la Dirección de Informática de la Universidad Técnica Nacional

#### Origen del estudio

El presente estudio fue programado en el Plan Anual de Trabajo de la Auditoría Universitaria del año 2014, para su realización se contrataron los servicios del Despacho Carvajal & Colegiados, Contadores Públicos Autorizados (1).

#### Objetivo del estudio

1. Realizar un diagnóstico de la situación actual de los procesos de la Dirección de Informática de la Universidad Técnica Nacional (UTN), comparando los mismos con lo establecido en el marco de referencia de los procesos del Manual de mejores prácticas TIC's referenciadas en los Objetivos de Control para Tecnologías de Información y Relacionadas (Control Objectives for Information and related Technology), COBIT en lo que resulte aplicable, en relación con el gobierno de las tecnologías de información (TI), y las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la Contraloría General de la República (CGR).

#### Conferencia de resultados

La comunicación preliminar de resultados, conclusiones y recomendaciones del estudio se efectuó el día 6 de enero 2015, con la presencia de la Licda. Doris Aguilar Sancho, Directora General Administrativa y el Ing. Jairo Bonilla Castro, Director de Informática de la UTN.

Ese día se entregó el borrador del presente Informe en forma física, con el propósito de que a más tardar el 16 de enero 2015 se formularan y remitieran por escrito a la Auditoría Universitaria las observaciones que se consideraran

---

<sup>1</sup> Contratación Directa 2014CD-000183-UTN "Consultoría y Servicios de Auditoría" y Orden de Compra 4158.

pertinentes sobre su contenido y los plazos para implementar las recomendaciones.

Se indicó en caso de no aceptar las recomendaciones o comentarios en este Borrador de Informe, se debe aportar la evidencia documental respectiva, así como, en caso que la Administración no establezca el plazo de implementación de estas recomendaciones, se considerará como plazo máximo hasta el primer semestre del año 2015.

Con oficio DI-05-2015 del 16 de enero 2015, el Director de Informática estableció los plazos de ejecución de las recomendaciones y presentó sus observaciones al Informe de Contadores Públicos Autorizados, cuyo análisis consta en el **Anexo** a este Informe.

### Secciones del Informe

El Informe que se adjunta se divide en las siguientes secciones o apartados a saber:

1. Estructura organizativa de la Dirección de Informática, sobre las capacidades de su personal y los procesos que soporta, para verificar si se está llevando a cabo el cumplimiento de su misión del modo más adecuado, cuyo resultado se determina una recomendación.
2. Proceso de planificación de la Dirección de Informática, para verificar si la elaboración de los planes de trabajo orientan toda su actividad a la consecución de objetivos y si estos se llevan a cabo por medio de la incorporación de las mejores prácticas, cuyo resultado determina dos recomendaciones.
3. Estado actual de las prácticas de administración de la Dirección de Informática relacionadas con el gobierno de TI y de los servicios de tecnología de información, cuyo resultado determina dos recomendaciones.
4. Gestión de la Dirección de Informática a los procesos de selección, adquisición, implementación y mantenimiento de la operación de la infraestructura tecnológica y de los sistemas de información, cuyo resultado determina dos recomendaciones.
5. Calificación de Riesgos en los Hallazgos, muestra el nivel de riesgo asociado con los hallazgos identificados por el Despacho Carvajal & Colegiados.
6. Asuntos de interés a informar, trata sobre comentarios generales sobre estudios o evaluaciones llevadas a cabo por terceros en relación a la implementación de las Normas de TI emitidas por la CGR.

## 7. Conclusión general.

### Principales resultados

En cuanto a la estructura organizativa de la Dirección de informática, no existe evidencia de una validación formal de la estructura interna de la Dirección de Informática por parte de la alta Dirección de la institución, este hallazgo se considera en Riesgo Medio. La Dirección de TI cuenta con una dirección central y puestos de jefatura en cada una de las Sedes, éstas están supeditadas a los Decanos de Sede. Esta situación pone en riesgo la correcta gestión de las tecnologías de la información de la Universidad.

El proceso de planificación de la Dirección de Informática, presenta deficiencias en los procesos establecidos por TI en cuanto a objetivos acordados en el Plan Institucional de Desarrollo Estratégico, este hallazgo se considera con un nivel de Riesgo Medio. El que la Dirección de TI no cuente con una estructura consolidada ni con los mecanismos suficientes para ejecutar, controlar y reportar los avances en cuanto a los objetivos que se estipulan en el Plan Estratégico, presenta un gran riesgo en la gestión de gobernabilidad de TI. Otro hallazgo es la indeterminación del valor de TI en la operación diaria o estratégica de la Universidad, este se considera en Riesgo Medio. Si bien la Dirección de TI aporta aspectos de valor en la obtención de objetivos estratégicos o de operación diaria, el ciclo de vida de entrega, y los aspectos que evidencien el valor generado no se lograron visualizar, por no tener un marco que permita la cuantificación del valor entregado por las soluciones de la Dirección de TI, para con el logro de objetivos estratégicos.

La revisión de las prácticas de administración de la Dirección de Informática, determina la inexistencia de un marco o metodología clara de administración de riesgos para TI, este hallazgo se encuentra en un nivel de Riesgo Alto. La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional. El no contar con una estructura de riesgo institucional completamente definida, no le permite a los departamentos asociados, entre ellos el de TI, la creación de un marco de gestión o estrategias de administración. Otro hallazgo es la falta de una definición institucional e integrada de procesos y sistemas críticos en relación a las tecnologías de la información, lo cual, se encuentra en Riesgo Alto. No todos los procesos

llevados a cabo por la institución se encuentran mapeados o documentados, lo que imposibilita al área encargada poder lograr la definición de un inventario de procesos. Además de no contar con la documentación o claridad en la definición de procesos, no hay una visión integral en cuales aspectos de gestión operativa son críticos para la institución.

En cuanto a la gestión de la Dirección de Informática a los procesos se determina la falta de definición de planes, metodologías, procedimientos y políticas, claves para la gestión integral de la Dirección de TI, este hallazgo se considera en Riesgo Alto. Las diversas situaciones de gestión operativa diaria, agregando aspectos de estructura organizacional, no han permitido a la Dirección de TI, en conjunto con áreas relevantes de la institución, la definición de estos documentos para la gestión de recursos informáticos. Otro hallazgo se refiere a la inexistencia de procesos de control de desempeño o monitoreo de desempeño, lo cual, se encuentra en Riesgo Medio. La falta de madurez en los procesos de gestión y administración del desempeño en tareas específicas o integrales, administración de recurso humano y desempeño de la infraestructura tecnológica, que puedan estar relacionadas con la obtención de metas y objetivos institucionales. El no contar con estos aspectos de control y monitoreo de desempeño desde una perspectiva institucional y departamental enfocado en TI, no permite determinar de una manera eficiente y eficaz, el cumplimiento de los objetivos y metas estratégicas ya sea del recurso humano o del recurso tecnológico existente.

### **Recomendaciones**

Las recomendaciones están dirigidas para su ejecución al Director de Informática, cuyos plazos de ejecución se encuentran supeditados a decisiones previas de la alta Dirección Universitaria.

Para efectos de la Auditoría Universitaria, se establece como plazo de seguimiento de estas recomendaciones el primer semestre del año 2015.

**ANEXO ÚNICO**

OBSERVACIONES Y PLAZO DE RECOMENDACIONES DEL AUDITADO  
AL INFORME DE CONTADORES PÚBLICOS  
PROCESOS DE LA DIRECCIÓN DE INFORMÁTICA - UTN

Tema VII.1	<u>ESTRUCTURA DE LA ORGANIZACIÓN DE LA DIRECCIÓN DE TI</u>	
Nombre del hallazgo 7.1.1 y Nivel de riesgo	NO EXISTE EVIDENCIA DE UNA VALIDACIÓN FORMAL DE LA ESTRUCTURA INTERNA DE LA DIRECCIÓN DE TI POR PARTE DE LA ALTA DIRECCIÓN DE LA INSTITUCIÓN  RIESGO MEDIO	
Recomendación 1 (7.1.1)	Establecer una línea de trabajo, en la cual, la estructura interna de la Dirección de TI esté acorde a las necesidades actuales de la Universidad y permita que la toma de decisiones, la operación diaria y la operación estratégica sea la correcta para lograr los objetivos estipulados en los planes de TI y de la institución.	
¿Se acoge?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
Observaciones de la Administración	Existe una estructura interna de la Dirección Informática aprobada por: la Comisión Institucional de Gestión Informática en sesión del 6 de noviembre del 2014, ACUERDO 14-2014.	
Plazo Propuesto por la Dirección de Informática	El plazo está fuera del alcance de la Dirección de Informática ya que se cumple la recomendación con el cumplimiento de: • Aprobación del PETIC por parte del Consejo Universitario. • Implementación de la unificación Universitaria (Informe CICAP)	
Argumentos de la Auditoría	La estructura interna de la Dirección de Informática no ha sido aprobada formalmente por la máxima autoridad universitaria, el Consejo Universitario; esa situación origina que el personal de TI ubicados en las Sedes, se encuentren supeditados a los Decanos de Sede. Para efectos de la Auditoría Universitaria, se establece como plazo de seguimiento de esta recomendación el primer semestre del año 2015.	

Tema VII.2	PROCESO DE PLANIFICACIÓN DE LA DIRECCIÓN DE TI	
Nombre del hallazgo 7.2.1 y Nivel de riesgo	DEFICIENCIAS EN LOS PROCESOS ESTABLECIDOS POR TI EN CUANTO A OBJETIVOS ACORDADOS EN EL PIDE  RIESGO MEDIO	
Recomendación 2 (7.2.1)	Incorporar dentro del Plan Estratégico de TI, o los Planes Tácticos de TI, la creación de políticas, procedimientos, manuales o guías de gestión, que permitan a la Dirección de TI obtener una mejor forma de control y monitoreo del logro de los objetivos, que el Plan Estratégico de la organización le solicita a la Dirección.	
¿Se acoge?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
Observaciones de la Administración	Se está en proceso de aprobación de los PETIC, el cual está alineado al Plan Estratégico Universitario. Cumpliendo así con las políticas generales de gestión. Con la aprobación del PTAC. Se establece el cumplimiento de los objetivos estratégicos. Con respecto a los manuales, procedimientos y guías de control, se desarrollarán durante el proceso de implementación de las normas técnicas.	
Plazo Propuesto por la Dirección de Informática	Según cronograma de implementación aprobado por la Comisión Institucional de Gestión Informática. (CIGI)	
Argumentos de la Auditoría	La Dirección TI se encuentra pendiente de desarrollar y actualizar la documentación de los sistemas y los procedimientos internos TI, también está pendiente la aprobación del PETIC. La Dirección TI debe especificar el número o nombre de actividad y el plazo de cumplimiento de esta recomendación establecido en dicho cronograma.	
Nombre del hallazgo 7.2.2 y Nivel de riesgo	INDETERMINACIÓN DEL VALOR DE TI EN LA OPERACIÓN DIARIA O ESTRATÉGICA DE LA UNIVERSIDAD  RIESGO MEDIO	
Recomendación 3 (7.2.2)	Incentivar a las dependencias de la institución a que creen o utilicen un marco de referencia y control para determinar la entrega de valor por parte de la Dirección de TI para con las metas y objetivos del negocio. Los aspectos que se deben de tomar en cuenta como mínimo son: ✓ Validación del ciclo de entrega de soluciones y como estas deben de presentarse y exponerse para determinar el valor generado para la institución. ✓ Marcos de optimización de costos en las soluciones entregadas, o procesos diarios que permitan un ahorro sustancial en las operaciones financieras de la institución y aporte el mismo o más valor que las soluciones que requieren un	

	gasto mayor de recurso económico. ✓ Determinar los mecanismos de valor intrínseco que la Dirección de TI puede dar a la operación de las tecnologías en relación a la obtención de beneficios más allá de los financieros.	
¿Se acoge?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
Observaciones de la Administración	Estas recomendaciones se cumplen con el punto 1.5 Gestión de Proyectos, del proceso de Implementación de las Normas Técnicas de la Contraloría y con la implementación de 5.1 Seguimiento de los procesos de TI. Es importante destacar la importancia de contratación del personal del área de Gestión de Proyectos, ya que actualmente no se cuenta con el área propuesta y no hay personal que cubra dichas funciones.	
Plazo Propuesto por la Dirección de Informática	Se cumple según cronograma de implementación aprobado por la Comisión Institucional de Gestión Informática. (CIGI), cuando a la Dirección de Informática se le asigne el personal para cubrir el área de Gestión de Proyectos.	
Argumentos de la Auditoría	La Dirección TI cita normativa que debe cumplir. La Dirección TI debe especificar el número o nombre de actividad y el plazo de cumplimiento de esta recomendación establecido en dicho cronograma.	

Tema VII.3	<u>ESTADO ACTUAL DE LAS PRÁCTICAS DE ADMINISTRACIÓN DE LA DIRECCIÓN DE TI</u>	
Nombre del hallazgo 7.3.1 y Nivel de riesgo	INEXISTENCIA DE UN MARCO O METODOLOGÍA CLARA DE ADMINISTRACIÓN DE RIESGOS PARA TI  RIESGO ALTO	
Recomendación 4 (7.3.1)	<p>Iniciar con la generación de un marco de gestión de riesgos que contenga como mínimo:</p> <ul style="list-style-type: none"> <li>✓ Conciencia de los riesgos por parte de la alta administración de la Universidad.</li> <li>✓ Un claro entendimiento del deseo de riesgo que tiene la Universidad.</li> <li>✓ Comprender los requerimientos de cumplimiento.</li> <li>✓ Transparencia de los riesgos significativos para la Universidad y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.</li> </ul>	
¿Se acoge?	SI <input type="checkbox"/>	NO <input checked="" type="checkbox"/>

Observaciones de la Administración	Si existe un marco regulador de gestión de riesgos en la Dirección de Planificación, el cual administra y evalúa semestralmente todos los riesgos de la Universidad incluyendo los riesgos en materia de TI. En forma adicional se está en proceso de implementación de la norma 1.3 sobre gestión de riesgos de TI.
Plazo Propuesto por la Dirección de Informática	La Dirección TI no establece plazo.
Argumentos de la Auditoría	<p>No es de recibo la no aceptación de la recomendación. Efectivamente existe un marco regulador de gestión de riesgos SEVRI llevado a cabo por la Dirección de Planificación, sin embargo, la Dirección TI reconoce que está en proceso de implementar la normativa sobre gestión de riesgos TI. La Dirección TI no aportó la evidencia documental respectiva de la identificación, priorización y administración de los riesgos instituciones en TI, de manera tal, que demuestre la exposición al riesgo por no disponer de personal experto en labores TIC, riesgos en la gestión en la seguridad de la información, riesgos en la implementación de las TIC, riesgos por no disponer en forma completa de la documentación de los sistemas informáticos y los procedimiento TI, riesgos en la implementación del proceso de transferencia tecnológica que minimice la dependencia de la Universidad con respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica y operación de las aplicaciones informáticas.</p> <p>La Dirección TI no establece plazo de cumplimiento de esta recomendación y dado que en la conferencia de resultados se indicó que en ausencia de ese plazo, se establecería el plazo propuesto por la Auditoría Universitaria, por ende la implementación de esta recomendación es para el primer semestre 2015.</p>
Nombre del hallazgo 7.3.2 y Nivel de riesgo	<p>FALTA DE UNA DEFINICIÓN INSTITUCIONAL E INTEGRADA DE PROCESOS Y SISTEMAS CRÍTICOS EN RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>RIESGO ALTO</p>
Recomendación 5 (7.3.2)	Iniciar un proceso de mapeo o inventario de procesos en cada uno de los departamentos que usan recursos tecnológicos. Además de realizar en este levantamiento de procesos una definición integral entre las áreas en asociación con las direcciones estratégicas, de cuáles de los procesos determinados son críticos para la institución y dependen en gran o completa medida de las tecnologías de la información.

¿Se acoge?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
Observaciones de la Administración	Se está en proceso de actualización del Plan de Contingencias de TI.	
Plazo Propuesto por la Dirección de Informática	Se cumple según cronograma de implementación aprobado por la Comisión Institucional de Gestión Informática. (CIGI) en el proceso de implementación del Plan de Contingencias. 4.2 Administración y operación de la plataforma tecnológica.	
Argumentos de la Auditoría	La Dirección TI debe especificar el número o nombre de actividad y el plazo de cumplimiento de esta recomendación establecido en dicho cronograma.	

<u>Tema VII.4</u>	<u>GESTIÓN DE LA DIRECCIÓN DE TI</u>	
Nombre del hallazgo 7.4.1 y Nivel de riesgo	FALTA DE DEFINICIÓN DE PLANES, METODOLOGÍAS, PROCEDIMIENTOS Y POLÍTICAS, CLAVES PARA LA GESTIÓN INTEGRAL DE LA DIRECCIÓN DE TI  RIESGO ALTO	
Recomendación 6 (7.4.1)	Iniciar con los procesos de creación y gestión de los documentos antes mencionados, que le permitan a la Universidad mejorar en aspectos de administración de sus recursos tecnológicos y la integración institucional con los demás departamentos.	
¿Se acoge?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
Observaciones de la Administración	Esta recomendación se cumple con la implementación de las Normas de TI. Plan Operativo. Se cumple hasta que la Dirección de Informática se establezca como área estratégica. Plan Táctico. Está en proceso de Aprobación.	
Plazo Propuesto por la Dirección de Informática	Los documentos pendientes se cumplirán según cronograma de implementación aprobado por la Comisión Institucional de Gestión Informática.	

Argumentos de la Auditoría	La Dirección TI debe especificar el plazo de cumplimiento para atender cada uno de los documentos identificados en el hallazgo de auditoría.
Nombre del hallazgo 7.4.2 y Nivel de riesgo	INEXISTENCIA DE PROCESOS DE CONTROL DE DESEMPEÑO O MONITOREO DE DESEMPEÑO  RIESGO MEDIO
Recomendación 7 (7.4.2)	Definir un marco de administración del desempeño, tanto en relación al recurso humano, como en relación a las tareas, procesos y procedimiento ejecutados por la Dirección de TI. Se deben de tener en cuenta aspectos como: <ul style="list-style-type: none"> <li>✓ Rastreo y monitoreo de la estrategia de implementación</li> <li>✓ La terminación de proyectos</li> <li>✓ El uso de los recursos tecnológicos</li> <li>✓ El desempeño de los procesos y la entrega del servicio</li> <li>✓ De ser posible uso de un cuadro de mando integral (Balanced Scorecard –BSC) que traduzca la estrategia en acción, para lograr las metas que se puedan medir más allá del registro convencional.</li> </ul>
¿Se acoge?	SI <input checked="" type="checkbox"/> NO <input type="checkbox"/>
Observaciones de la Administración	Se cumple con el desarrollo del catálogo de servicios y la directriz emitida sobre acuerdos de servicios.
Plazo Propuesto por la Dirección de Informática	Se cumple según cronograma de implementación aprobado por la Comisión Institucional de Gestión Informática. (CIGI) en el proceso de implementación 4.1 Definición y administración de acuerdos de servicio.
Argumentos de la Auditoría	La Dirección TI debe especificar el número o nombre de actividad y el plazo de cumplimiento de esta recomendación establecido en dicho cronograma.

*UNIVERSIDAD TÉCNICA NACIONAL*

---

⊕ **DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS  
PROCESOS DE LA DIRECCIÓN DE T.I. DE LA UTN.**

⊕ *Informe Final*

Alajuela, 15 de Enero del 2014.

*Señores*

*Universidad Técnica Nacional*

*Atención Lic. Jorge Pizarro Palma*

*Auditor General de la Universidad Técnica Nacional*

*Presente*

Estimado Licenciado Pizarro:

De acuerdo con los términos especificados en nuestra propuesta de servicios profesionales, denominada “Desarrollo de un trabajo que permita un diagnóstico de la situación actual de los procesos de la Dirección de T.I de la UTN, comparando los mismos con lo establecido en el marco de referencia de los procesos de COBIT, en relación con el Gobierno de T.I., y las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la CGR”.

Con base en nuestro trabajo realizado, observamos e identificamos una serie de aspectos relacionados con los procesos que componen el Gobierno de TI, los cuales sometemos a consideración de ustedes en este diagnóstico solicitado.

Muy atentamente,

***DESPACHO CARVAJAL & COLEGIADOS  
CONTADORES PÚBLICOS AUTORIZADOS***

Lic. Ricardo Montenegro Guillén  
Contador Público Autorizado No. 5607  
Póliza de Fidelidad N° R-1153  
Vence el 30 de setiembre del 2015

MCC. Fabián Cordero Navarro  
CISA #1189851

## Tabla de contenido

I. INTRODUCCIÓN .....	4
II. OBJETIVOS .....	4
III. ALCANCE .....	4
IV. PERIODO DEL ESTUDIO.....	5
V. LIMITACIONES DEL ESTUDIO .....	5
VI. METODOLOGÍA .....	5
VII. RESULTADOS DEL TRABAJO EFECTUADO.....	5
HALLAZGO 7.1.1:.....	7
HALLAZGO 7.2.1:.....	8
HALLAZGO 7.2.2:.....	9
HALLAZGO 7.3.1:.....	10
HALLAZGO 7.3.2:.....	11
HALLAZGO 7.4.1:.....	12
HALLAZGO 7.4.2:.....	16
CONCLUSIÓN GENERAL .....	16

## **“DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS PROCESOS**

### **DE LA DIRECCIÓN DE INFORMÁTICA DE UTN”**

#### **TRABAJO REALIZADO**

## **I. INTRODUCCIÓN**

El presente trabajo ha sido desarrollado para la Auditoría General de la Universidad Técnica Nacional de acuerdo con los términos establecidos en nuestra propuesta de servicios profesionales, relacionados con “un Diagnóstico de la situación actual de los procesos de la Dirección de TI de la UTN, comparando los mismos con lo establecido en el marco de referencia de los procesos de COBIT, en relación con el Gobierno de TI y las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la CGR”.

## **II. OBJETIVOS**

Desarrollo de un trabajo que permita un diagnóstico de la situación actual de los procesos de la Dirección de TI de la UTN, comparando los mismos con lo establecido en el marco de referencia de los procesos de COBIT, en relación con el Gobierno de TI y las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la CGR.

## **III. ALCANCE**

El alcance del trabajo realizado se llevó a cabo de acuerdo con las siguientes actividades, las cuales están relacionadas de forma directa con los procesos de gestión del Gobierno de TI:

1. Evaluar la estructura organizativa de la Dirección de TI, las capacidades de su personal y los procesos que soporta, para verificar si se está llevando a cabo el cumplimiento de su misión del modo más adecuado.
2. Evaluar el proceso de planificación de la Dirección de TI, para verificar si la elaboración de los planes de trabajo orientan toda su actividad a la consecución de objetivos y si estos se llevan a cabo por medio de la incorporación de las mejores prácticas.
3. Evaluar el estado actual de las prácticas de administración de la Dirección de TI relacionadas con el gobierno de TI y de los servicios de tecnología de información.
4. Evaluar la gestión de la Dirección de TI a los procesos de selección, adquisición, implementación y mantenimiento de la operación de la infraestructura tecnológica y de los sistemas de información.

#### IV. PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de noviembre y diciembre del 2014.

#### V. LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones en el presente trabajo.

#### VI. METODOLOGÍA

Para el desarrollo del presente trabajo establecimos citas y llevamos a cabo sesiones de trabajo y entrevistas con el Director de TI y con el personal tanto de la Dirección de TI de la Universidad, como con el personal de TI de la Sede Central y Sedes regionales.

#### VII. RESULTADOS DEL TRABAJO EFECTUADO

Seguidamente presentamos nuestros hallazgos y recomendaciones producto de la revisión y evaluación efectuada de acuerdo con el alcance establecido en el presente trabajo:

**VII.1 Estructura de la organización de la Dirección de TI**, las capacidades de su personal y los procesos que soporta, para verificar si se está llevando a cabo el cumplimiento de su misión del modo más adecuado.

**HALLAZGO 7.1.1: NO EXISTE EVIDENCIA DE UNA VALIDACIÓN FORMAL DE LA ESTRUCTURA INTERNA DE LA DIRECCIÓN DE T.I. POR PARTE DE LA ALTA DIRECCIÓN DE LA INSTITUCIÓN. RIESGO MEDIO**

**CONDICIÓN:**

En el proceso de revisión, se determinó que la estructura organizativa de la Dirección de TI, puede presentar fallas de índole operativos, especialmente por la dependencia de otras áreas de la Universidad, que no son parte de la Dirección de TI y tienen injerencia en las decisiones técnicas y de estandarización de normas.

Actualmente la Dirección de TI cuenta con una dirección central y puestos de jefatura en cada una de las Sedes.

Las jefaturas de las Sedes están supeditadas a los Decanos de Sede.

**CRITERIO:**

Normas técnicas para la gestión y el control de las Tecnologías de Información

2.4 Independencia y recurso humano en la función del TI

El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.

Además, debe brindar el apoyo necesario para que dicha función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.

**CAUSA:**

La unión de las diferentes Sedes y el no establecimiento de políticas de gestión de personal que permitan una integración y estandarización de marcos metodológicos, normas, tecnología e infraestructura, en todas las Sedes.

**EFECTO:**

La no centralización de aspectos críticos como las tendencias tecnológicas, directrices técnicas o normativas, políticas y procesos operativos de las tecnologías, y acatamiento de órdenes, puede poner en riesgo la correcta gestión de las tecnologías de la información de la Universidad.

## RECOMENDACIÓN:

Establecer una línea de trabajo, en la cual, la estructura interna de la Dirección de TI esté acorde a las necesidades actuales de la Universidad y permita que la toma de decisiones, la operación diaria y la operación estratégica sea la correcta para lograr los objetivos estipulados en los planes de TI y de la institución.

**VII.2 Proceso de planificación de la Dirección de TI**, para verificar si la elaboración de los planes de trabajo permite orientar toda su actividad a la consecución de objetivos y si estos se llevan a cabo por medio de la incorporación de las mejores prácticas.

**HALLAZGO 7.2.1: DEFICIENCIAS EN LOS PROCESOS ESTABLECIDOS POR TI EN CUANTO A OBJETIVOS ACORDADOS EN EL PLAN INSTITUCIONAL DE DESARROLLO ESTRATÉGICO. RIESGO MEDIO**

## CONDICIÓN:

Se determinó que algunos de los procesos de la Dirección de TI no están del todo alineados con la planificación estratégica de la institución, especialmente en aspectos de control, medición, políticas y procedimientos que permitan conseguir los objetivos que el Plan Institucional de Desarrollo Estratégico propone (PAG 53, 64).

## CRITERIO:

Normas técnicas para la gestión y el control de las Tecnologías de Información.

### 1.1 Marco Estratégico de TI

El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

## CAUSA:

El no contar con una estructura consolidada, en la Dirección de TI de la Universidad, que incluya todas las Sedes y permita traducir los objetivos del negocio en aspectos de índole operativa. Es de suma importancia evidenciar, que pese a que se toman en cuenta objetivos donde se involucra a la Dirección de TI, no se obtuvo suficiente evidencia de que la Dirección de TI participara en la formulación de los objetivos del plan institucional.

**EFEECTO:**

El que la Dirección de TI no cuente con los mecanismos suficientes para ejecutar, controlar y reportar los avances en cuanto a los objetivos que se estipulan en el Plan Estratégico, presenta un gran riesgo en la gestión de gobernabilidad de TI.

**RECOMENDACIÓN:**

Incorporar dentro del Plan Estratégico de TI, o los Planes Tácticos de TI, la creación de políticas, procedimientos, manuales o guías de gestión, que permitan a la Dirección de TI obtener una mejor forma de control y monitoreo del logro de los objetivos, que el Plan Estratégico de la organización le solicita a la Dirección.

**HALLAZGO 7.2.2: INDETERMINACIÓN DEL VALOR DE TI EN LA OPERACIÓN DIARIA O ESTRATÉGICA DE LA UNIVERSIDAD. RIESGO MEDIO****CONDICIÓN:**

Si bien la Dirección de TI aporta aspectos de valor en la obtención de objetivos estratégicos o de operación diaria, el ciclo de vida de entrega, y los aspectos que evidencien el valor generado no se lograron visualizar.

**CRITERIO:**

Normas técnicas para la gestión y el control de las Tecnologías de Información

**5.1 Seguimiento de los procesos de TI**

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

**CAUSA:**

La Universidad no ha solicitado o creado una estructura o marco que le permita a la Dirección de TI entregar detalle en cuanto a la gestión del valor en las soluciones que se entregan para el cumplimiento de los objetivos estratégicos y operaciones diarias o de rutina.

**EFEECTO:**

El no tener un marco que permita la cuantificación del valor entregado por las soluciones de la Dirección de TI, para con el logro de objetivos estratégicos, no permite determinar de una manera certera que las soluciones que se estén brindando desde una perspectiva tecnológica sean las óptimas y sean las que la Universidad necesita para el cumplimiento de metas.

### RECOMENDACIÓN:

Incentivar a las dependencias de la institución a que creen o utilicen un marco de referencia y control para determinar la entrega de valor por parte de la Dirección de TI para con las metas y objetivos de negocio.

Los aspectos que se deben de tomar en cuenta como mínimo son:

- Validación del ciclo de entrega de soluciones y como estas deben de presentarse y exponerse para determinar el valor generado para la institución.
- Marcos de optimización de costos en las soluciones entregadas, o procesos diarios que permitan un ahorro sustancian en las operaciones financieras de la institución y aporte el mismo o más valor que las soluciones que requieren un gasto mayor de recurso económico.
- Determinar los mecanismos de valor intrínseco que la Dirección de TI puede dar a la operación de las tecnologías en relación a la obtención de beneficios mas allá de los financieros.

**VII.3 Estado actual de las prácticas de administración de la Dirección de TI,** relacionadas con el gobierno de TI y de los servicios de tecnología de información.

**HALLAZGO 7.3.1: INEXISTENCIA DE UN MARCO O METODOLOGÍA CLARA DE ADMINISTRACIÓN DE RIESGOS PARA TI. RIESGO ALTO**

### CONDICIÓN:

La Dirección de TI no cuenta con un marco o estructura de administración de riesgo tecnológico, que este alineado con la gestión de riesgo institucional.

Además el manejo de los escenarios de riesgo en la gestión diaria, proyectos especiales o prospecciones, no es aplicado ni gestionado.

### CRITERIO:

Normas técnicas para la gestión y el control de las Tecnologías de Información

1.3 Gestión de riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

**CAUSA:**

La organización no cuenta con una estructura de gestión de riesgo impregnada en toda la institución, la cual es necesaria para administrar correctamente los riesgos tanto operativos, institucionales y riesgos asociados con la operación de la organización.

**EFECTO:**

El no contar con una estructura de riesgo institucional completamente definida, no le permite a los departamentos asociados, entre ellos el de TI, la creación de un marco de gestión o estrategias de administración. Esto es crítico ya que no se pueden mitigar o controlar los riesgos.

**RECOMENDACIÓN:**

Iniciar con la generación de un marco de gestión de riesgos que contenga como mínimo:

- ✓ Conciencia de los riesgos por parte de la alta administración de la Universidad.
- ✓ Un claro entendimiento del deseo de riesgo que tiene la Universidad.
- ✓ Comprender los requerimientos de cumplimiento.
- ✓ Transparencia de los riesgos significativos para la Universidad y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

**HALLAZGO 7.3.2: FALTA DE UNA DEFINICIÓN INSTITUCIONAL E INTEGRADA DE PROCESOS Y SISTEMAS CRÍTICOS EN RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN **RIESGO ALTO****

**CONDICIÓN:**

No se determinó por parte de esta auditoría una definición clara e integral de los sistemas y procesos tecnológicos críticos definidos, que impacten a la Universidad en caso de que no se tenga controlados y monitoreados, ya sea por parte de las direcciones de la institución o por parte de la Dirección de TI.

**CRITERIO:**

Normas técnicas para la gestión y el control de las Tecnologías de Información

1.4.7 Continuidad de los servicios de TI

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.

#### **CAUSA:**

En primera instancia no todos los procesos llevados a cabo por la institución se encuentran mapeados o documentados, lo que imposibilita al área encargada poder lograr la definición de un inventario de procesos. Además de no contar con la documentación o claridad en la definición de procesos, no hay una visión integral en cuales aspectos de gestión operativa son críticos para la institución.

#### **EFECTO:**

El no contar con los procesos críticos definidos, especialmente los que tienen que ver con el uso de tecnologías de la información o sistemas informáticos, ocasiona que no exista claridad en que aspectos se deben de proteger y que estrategias debe de tomar la institución para salvaguardar sus activos y alcanzar las metas establecidas.

#### **RECOMENDACIÓN:**

Iniciar un proceso de mapeo o inventario de procesos en cada uno de los departamentos que usan recursos tecnológicos. Además de realizar en este levantamiento de procesos una definición integral entre las áreas en asociación con las direcciones estratégicas, de cuáles de los procesos determinados son críticos para la institución y dependen en gran o completa medida de las tecnologías de la información.

**VII.4 Gestión de la Dirección de TI a los procesos** de selección, adquisición, implementación y mantenimiento de la operación de la infraestructura tecnológica y de los sistemas de información.

**HALLAZGO 7.4.1: FALTA DE DEFINICIÓN DE PLANES, METODOLOGÍAS, PROCEDIMIENTOS Y POLÍTICAS, CLAVES PARA LA GESTIÓN INTEGRAL DE LA DIRECCIÓN DE TI. RIESGO ALTO**

#### **CONDICIÓN:**

No se evidenció la existencia de aspectos de gestión claves para una correcta administración del ambiente de tecnologías de información, limitando la estructura de control interno y monitoreo a procesos informales o no definidos del todo.

Los siguientes documentos o planes no fueron detectados:

- ✓ Plan operativo de TI
- ✓ Plan táctico de TI
- ✓ Plan de mantenimiento lógico y físico de TI
- ✓ Portafolio de proyectos
- ✓ Metodologías de riesgo
- ✓ Procedimientos y políticas de contratación de TI
- ✓ Plan de seguridad de TI
- ✓ Base de Datos de la Administración de la Configuración - CMDB
- ✓ Manual de cargos de TI
- ✓ Administración de costos e inversiones de TI

### **CRITERIO:**

Normas técnicas para la gestión y el control de las Tecnologías de Información

#### 2.1 Planificación de tecnologías de la información

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

### **CAUSA:**

Las diversas situaciones de gestión operativa diaria, agregando aspectos de estructura organizacional, no han permitido a la Dirección de TI, en conjunto con áreas clave de la institución la definición de estos documentos claves para la gestión de recursos informáticos.

### **EFECTO:**

El no contar con estos documentos que controlen y gestionen aspectos críticos en relación a la gestión de las tecnologías de información de la universidad, esto no permite la visualización de logro de objetivos o metas estratégicas de la organización y como la operación diaria y estratégica de TI va a impactar en el logro de estas.

### **RECOMENDACIÓN:**

Iniciar con los procesos de creación y gestión de los documentos antes mencionados, que le permitan a la universidad mejorar en aspectos de administración de sus recursos tecnológicos y la integración institucional con los demás departamentos.

**HALLAZGO 7.4.2: INEXISTENCIA DE PROCESOS DE CONTROL DE DESEMPEÑO O MONITOREO DE DESEMPEÑO. RIESGO MEDIO.**

**CONDICIÓN:**

No existe una estructura institucional, que se pueda aplicar a la Dirección de TI, que permita controlar o monitorear el desempeño, no solo del personal, sino de las tareas o metas en relación a la obtención de objetivos estratégicos u operativos.

**CRITERIO:**

Normas técnicas para la gestión y el control de las Tecnologías de Información

4.1 Definición y administración de acuerdos de servicio

La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la función de TI según sus capacidades.

El jerarca y la función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

- a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
- b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
- c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
- d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
- e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.
- f. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

**CAUSA:**

La falta de madurez en los procesos de gestión y administración del desempeño en tareas específicas o integrales, administración de recurso humano y desempeño de la infraestructura tecnológica, que puedan estar relacionadas con la obtención de metas y objetivos institucionales.

**EFEECTO:**

El no contar con estos aspectos de control y monitoreo de desempeño desde una perspectiva institucional y departamental enfocado en TI, no permite determinar de una manera eficiente y eficaz, el cumplimiento de los objetivos y metas estratégicas ya sea del recurso humano o del recurso tecnológico existente.

## RECOMENDACIÓN:

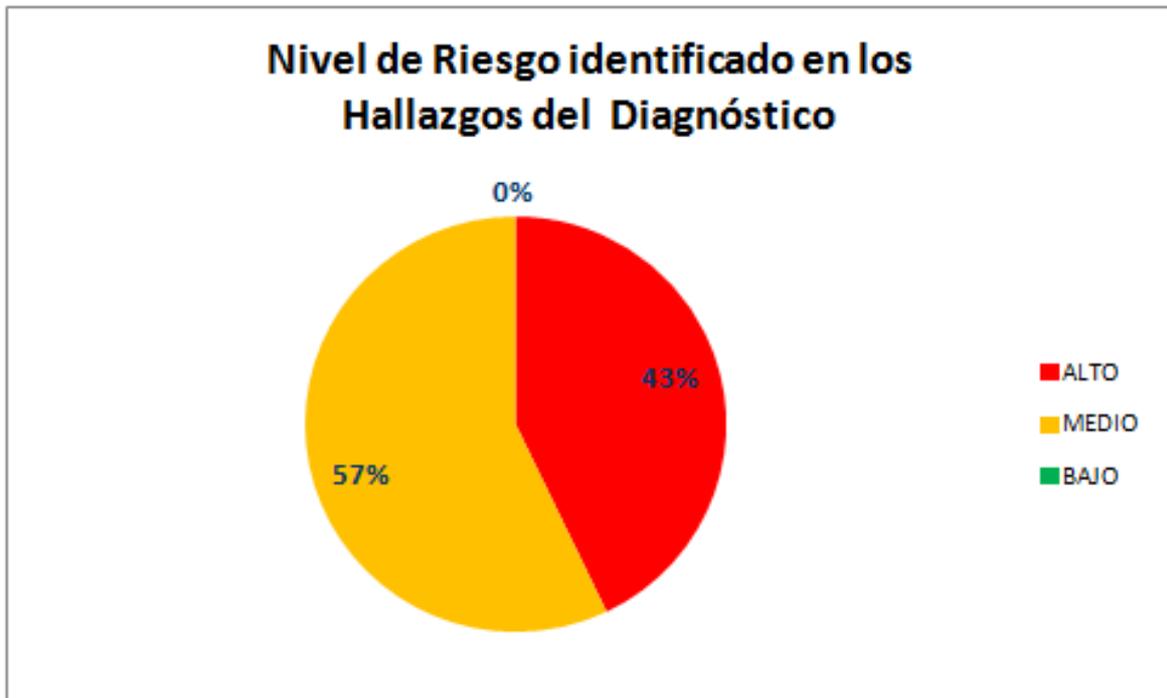
Definir un marco de administración del desempeño, tanto en relación al recurso humano, como en relación a las tareas, procesos y procedimiento ejecutados por la Dirección de TI.

Se deben de tener en cuenta aspectos como:

- ✓ Rastreo y monitoreo de la estrategia de implementación
- ✓ La terminación de proyectos
- ✓ El uso de los recursos tecnológicos
- ✓ El desempeño de los procesos y la entrega del servicio
- ✓ De ser posible uso de un cuadro de mando integral (*Balanced Scorecard* –BSC) que traduzca la estrategia en acción, para lograr las metas que se puedan medir más allá del registro convencional.

## VII.5 Calificación de Riesgos en los Hallazgos

El siguiente gráfico muestra los Riesgos asociados a los Hallazgos identificados en el presente Diagnóstico:



Es conveniente tomar en consideración los porcentajes altos de riesgo obtenidos en los hallazgos, debido a que se requerirá de un gran esfuerzo de la dirección de TI de la Universidad para lograr implementar las recomendaciones emitidas en este Informe, para implementar un Gobierno de TI adecuado.

## VIII. Asuntos de interés a informar

Durante el desarrollo de nuestro trabajo, tuvimos la oportunidad de conocer una serie de informes sobre estudios y evaluaciones llevadas a cabo por terceros en relación a la implementación de las Normas de TI de la Contraloría General de la República en la Universidad Técnica nacional.

Específicamente, se trata de los siguientes informes:

- 1. Revisión del estado actual de implementación de las Normas Técnicas de Control Interno relacionadas con las TIC - Consultores Grijalba Chinchilla y Compañía, S.A. Fecha final 9 Noviembre del 2012**

En dicho informe se solicita a la administración la elaboración de un Plan de Implementación de las Recomendaciones emitidas por dicha firma de consultoría.

- 2. Cronograma del Plan de Implementación de las Normas de la Contraloría con responsables**

Este Cronograma de Implementación fue elaborado por la Dirección de TI, en el cual se especifican las actividades necesarias para la implementación de las Normas de TI de la Contraloría General de la República. En dicho Plan se especificó una Fecha de Inicio del Segundo Semestre del 2013 y Fecha de Finalización del Segundo Semestre del 2017.

Ahora bien, es de suma importancia mencionar que los plazos han sido movidos en relación a los originales y no se ha cumplido con los procesos críticos necesarios para poder evidenciar una mejora sustancial.

Ademas es critico analizar la viabilidad de reducir la duración del plan de implementación, que actualmente tiene un periodo de 4 años plazo, pensando en la urgencia para la Universidad en la implementación de estos procesos, los cuales son las bases operativas de la gestión de TI.

- 3. En estos momentos se está desarrollando un Diagnóstico sobre la situación actual de las Normas de TI de la Contraloría y un Plan de Acción para su implementación con la firma consultora Deloitte.**

Sobre este particular, no podemos opinar, debido a que solo conocemos la oferta de desarrollo de este trabajo, así como nuestro trabajo no considera una opinión sobre estas contrataciones.

## CONCLUSIÓN GENERAL

Consideramos que es de suma importancia que la Dirección de TI de la Universidad se enfoque en implementar la Normativa de TI de la Contraloría, como lo especifica el Director de TI, de acuerdo a su propia opinión en el **“Diagnóstico Inicial de las Normas Técnicas de TI y Comunicación”**, llevado a cabo en el año 2013, donde concluye de forma categórica, lo siguiente:

De acuerdo con los análisis realizados, se establece que la normativa TI de la Contraloría debe ser aplicada en su totalidad en la Universidad.

Es viable y factible cumplir con la normativa en el plazo establecido en el cronograma, aunque se debe tomar en cuenta el apartado de limitaciones de este diagnóstico.

La Comisión Institucional de Gestión Informática (CIGI) es la responsable directa de la Implementación de la Norma de TI de la Contraloría General de la República.