UNIVERSIDAD DE COSTA RICA

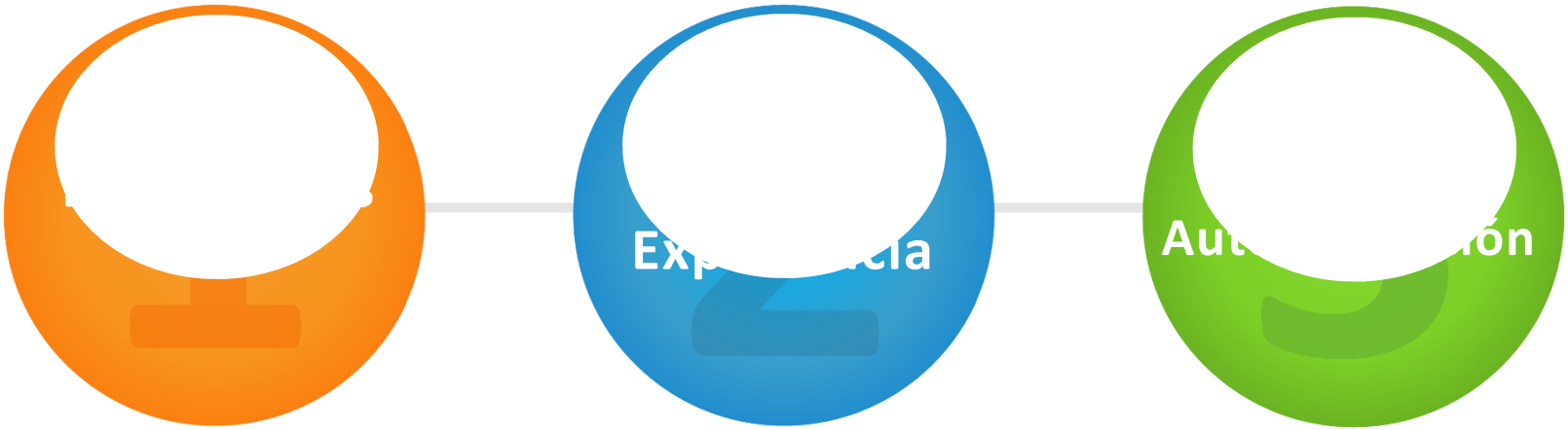
CONTRALORÍA UNIVERSITARIA

MSI. Roberto Porras León
Jefe Sección de Auditoría de Sistemas y TI
roberto.porras@ucr.ac.cr

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

¿Que pasaría si…?

Contenidos



1 Las Normas

Un vistazo a las “Normas técnicas para la gestión y control de las Tecnologías de Información (N-2-2007-CO-DFOE)”

Contraloría Universitaria – MSI. Roberto Porras León

¿Para qué normas específicas de TI?

Las tecnologías de información (TI) constituyen uno de los principales instrumentos que **apoyan la gestión de las organizaciones** mediante el manejo de grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Las TI deben gestionarse dentro de un marco de control que procure el logro de **los objetivos** que se pretende con ellas y que dichos objetivos estén **debidamente alineados** con la estrategia de la organización.

El poder de negociación de las TI

Su uso ha implicado, al menos, tres situaciones relevantes: la dedicación de porciones importantes del presupuesto de las organizaciones, con el costo de oportunidad que ello conlleva, principalmente en organizaciones con recursos limitados y actividades sustantivas esenciales para la sociedad; un marco jurídico cambiante tendente a buscar su paralelismo con las nuevas relaciones que se dan a raíz del uso de esas TI; y una presión importante de proveedores y consumidores por la implementación de más y mejores servicios apoyados en estas tecnologías.

Gestión de las Tecnologías de Información

- Conjunto de acciones fundamentadas en políticas institucionales que, de una manera global, intentan dirigir la gestión de las TI hacia el logro de los objetivos de la organización.
- Alineación entre los objetivos de TI y los de la organización, el balance óptimo entre las necesidades de TI de la organización y las oportunidades que sobre ello existen, la maximización de los beneficios
- El uso responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación de dichas TI.
- Tales acciones se relacionan con los procesos (planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento), recursos tecnológicos (personas, sistemas, tecnologías, instalaciones y datos), y con el logro de los criterios de fidelidad, calidad y seguridad de la información. También se entiende como “Gobernabilidad de TI”.

Gestión de las Tecnologías de Información

- Planificar y Organizar
- Adquirir e Implementar
- Entrega de servicios y Soporte
- Seguimiento
- Pero existen actividades que son transversales

  a esos grandes dominios de gestión:

  - Administración de riesgos
  - Gestión de la seguridad de la información
  - Asegurar la continuidad de las operaciones
  - Gestión de la calidad
  - Administración de proyectos

Estructura general de las Normas

Capítulo 1: Normas de aplicación general

Capítulo 2: Planificación y organización

Capítulo 3: Implementación de TI

Capítulo 4: Prestación de servicios y mantenimiento

Capítulo 5: Seguimiento

El qué hacer y el cómo hacerlo

- Las normas lo que plantean son criterios mínimos de control (objetivos de control)
- Objetivos de control: Meta a alcanzar basada en el uso las mejores prácticas.
- El cómo depende de las características propias de TI de cada organización.

Planificar y Organizar

Indica la dirección a seguir.

- Cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos de la Unidad.
- Planear, comunicar y administrar una visión estratégica de TI.
- Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada

¿Cómo saber si estamos alcanzando los objetivos de Planificar y Organizar?

1. ¿Están alineadas las estrategias de TI con las de la Unidad?
2. ¿La Unidad está alcanzando un uso óptimo de sus recursos de TI?
3. ¿Entienden todas las personas dentro de la Unidad los objetivos de TI?
4. ¿Se entienden y administran los riesgos de TI?
5. ¿Es apropiada la calidad de los servicios y sistemas de TI para las necesidades de la Unidad?

¿Qué nos pide la norma en este dominio?

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación: **2.1: Planificación de las TI.**

La organización debe optimizar la integración, uso y estandarización de sus sistemas de información: **2.2: Modelo de arquitectura de información**

Tener una perspectiva clara de su dirección y condiciones en materia tecnológica para optimice el uso de su infraestructura tecnológica: **2.3: Infraestructura Tecnológica**

Asegurar la independencia de la Función de TI respecto de las áreas usuarias: **2.4: Independencia y recurso humano de la Función de TI**.

Optimizar el uso de los recursos financieros invertidos en la gestión de TI: **2.5: Administración de Recursos Financieros**.

Adquirir e Implementar

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del la Unidad.

¿Cómo saber si estamos alcanzando los objetivos de Adquirir e implementar?

1. ¿Es probable que los nuevos proyectos de adquisición de infraestructura y desarrollo de sistemas generen soluciones que satisfagan las necesidades de la Unidad?
2. ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
3. ¿Se ha tomado todas las medidas para asegurar que los nuevos sistemas e infraestructura funcionen adecuadamente una vez sean implementados?
4. ¿Los cambios no afectarán a las operaciones actuales de la Unidad o se ha previsto los ajustes necesarios?

¿Qué nos pide la norma en este dominio?

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. **3.1. Consideraciones generales de la implementación de TI.**

La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos. **3.2. Implementación de software.**

La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. **3.3. Implementación de infraestructura tecnológica.**

La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. **3.4. Contratación de terceros para la implementación y mantenimiento de software e infraestructura.**

Entrega de servicios y soporte

Cubre la entrega en sí de los servicios requeridos:

- La prestación del servicio,
- La administración de la seguridad y de la continuidad,
- El soporte del servicio a los usuarios,
- La administración de los datos y de las instalaciones operativas.

¿Cómo saber si estamos alcanzando los objetivos de Entrega y Soporte?

1. ¿Se están entregando los servicios de TI de acuerdo con las prioridades de la Unidad?
2. ¿Están optimizados los costos de TI?
3. ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
4. ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

¿Qué nos pide la norma en este dominio?

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. **4.1. Definición y administración de acuerdos de servicio.**

La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. **4.2. Administración y operación de la plataforma tecnológica.**

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura. **4.3. Administración de los datos.**

¿Qué nos pide la norma en este dominio?

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna. **4.4. Atención de requerimientos de los usuarios de TI.**

La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. **4.5. Manejo de Incidentes.**

La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. **4.6. Administración de servicios prestados por terceros.**

Seguimiento y Monitoreo

Los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Esto incluye:

- La administración del desempeño.
- El monitoreo del control interno.
- El cumplimiento regulatorio.
- La aplicación del gobierno de TI.

¿Cómo saber si estamos alcanzando los objetivos de Seguimiento y Monitoreo?

1. ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
2. ¿El responsable de TI garantiza que los controles internos son efectivos y eficientes?
3. ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas de la Unidad?
4. ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

¿Qué nos pide la norma en este dominio?

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. **5.1. Seguimiento de los procesos de TI.**

Establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas. **5.2 Seguimiento y evaluación del control interno en TI.**

La actividad de la Auditoría Interna respecto de la gestión de las TI debe orientarse a coadyuvar, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia. **5.3 Participación de la Auditoría Interna.**

Normas de aplicación general

1.1 Marco estratégico de TI: Políticas y prácticas de TI

1.2 Gestión de la calidad: los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo

1.3 Gestión de riesgos: responder adecuadamente a las amenazas que puedan afectar la gestión de las TI.

Normas de aplicación general

1.4. Gestión de la seguridad de la información: garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información

1.4.1 Implementación de un marco de seguridad de la información

1.4.2 Compromiso del personal con la seguridad de la información

1.4.3 Seguridad física y ambiental

1.4.4 Seguridad en las operaciones y comunicaciones

1.4.5 Control de acceso

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica

1.4.7 Continuidad de los servicios de TI

Normas de aplicación general

1.5 Gestión de proyectos: administrar sus proyectos de TI de manera que logre sus objetivos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos

1.6 Decisiones sobre asuntos estratégicos de TI: Comité Gerencial de Informática

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI: Cumplir las regulaciones.

2 La Experiencia

Experiencia de la aplicación de las normas en la UCR en relación con el trabajo de los RIDs

¿Qué revisa la auditoría?

El estudio comprende el análisis de los siguientes temas de control interno relacionados con la gestión de TI, a saber:

- Organización, funciones y responsabilidades de la función de TI.
- Programación, coordinación, ejecución, supervisión y reporte de las labores realizadas en el ámbito de la gestión de TI.
- Administración de los recursos de TI.
- Gestión de los servicios brindados por la función de TI.
- Identificación y gestión de riesgos de la plataforma tecnológica.
- Gestión de la seguridad de la información.

Los principales hallazgos

"1. El administrador de recursos informáticos desconcentrados carece de planes de trabajo formales, y no presenta informe de labores."

Posibles riesgos:

La ausencia de un plan de trabajo formal y el respectivo informe de las labores del RID, puede conllevar a la materialización de los siguientes riesgos: problemas de rendimiento, pérdida de confianza del personal de TI, desviaciones o degradación de servicios o incapacidad para brindar servicios con tiempos de respuesta oportunos.

¿Cómo mejorar este aspecto?

"Establecer y dar seguimiento a un programa de trabajo anual o con la frecuencia que se considere pertinente que ayude a fortalecer la gestión de TI."

Dentro de temas a abordar se pueden considerar al menos los siguientes:

- Los proyectos del área de TI.
- Las actividades cotidianas de soporte y mantenimiento.
- La capacitación.
- Las actividades fuera de la dependencia universitaria.
- Las vacaciones.

Además, para verificar el grado de cumplimiento de dicho plan de trabajo, solicitar el informe de labores respectivo.

Los principales hallazgos

"2. Ausencia de procedimientos formales para la gestión y control de la plataforma tecnológica."

- *Procedimiento para la gestión del sitio web de la Unidad.*
- *Mantenimiento correctivo y preventivo de equipos.*
- *Control de cambios a la infraestructura tecnológica.*
- *Soporte a usuarios.*

Posibles riesgos:

- *dificultades para garantizar la continuidad de su operación*
- *servicios de información desactualizados*
- *dificultades para gestionar adecuadamente la infraestructura.*

¿Cómo mejorar este aspecto?

"Establecer los procedimientos necesarios para la gestión y control de la plataforma tecnológica."

Entre los aspectos que deberían considerarse están los siguientes:

- El mantenimiento preventivo y correctivo de los equipos.
- La gestión de cambios y actualizaciones de software y antivirus.
- El procedimiento para la actualización del sitio web.
- La estrategia para la atención de solicitudes de los usuarios.

Esto con la finalidad de estandarizar la forma en que se gestiona y controla la operación de la plataforma tecnológica de la Unidad.

Los principales hallazgos

"3. No se han establecido parámetros apropiados para la definición y evaluación de los servicios de TI, se carece de acuerdos de servicios específicos.

- No se han documentado,
- No existen criterios formales de evaluación
- Faltan mecanismos formales de seguimiento para medir su calidad.

Posibles Riesgos:

- una atención inoportuna de problemas ocurridos en la operación de las TI,
- degradación de los servicios de TI,
- tiempo de respuesta inadecuado.

¿Cómo mejorar este aspecto?

"Definir los servicios que la Unidad requiere por parte del RID."

Para esto considerar al menos lo siguiente:

- Nombre del Servicio.
- Responsabilidades asociadas.
- Tiempo de respuesta.
- Características del servicio.
- Documentación de apoyo.

Con esto se pretende que la prestación de servicios de TI garantice de manera razonable una entrega y prestación eficaz de los servicios de TI requeridos por la dependencia universitaria.

Los principales hallazgos

"4. No se evidencia la existencia de un análisis de los riesgos tecnológicos a los que está expuesta la Unidad."

Posibles riesgos:

- Pérdida de continuidad de los servicios de TI.
- Acceso no autorizado a información sensible y confidencial.
- Obsolescencia tecnológica.
- Virus computacionales.

¿Cómo mejorar este aspecto?

"Realizar un análisis de riesgos tecnológicos a los que está expuesta la Unidad e incorporarlos en el Sistema de Valoración de Riesgos de la Oficina de Planificación Universitaria."

Entre los aspectos que se sugiere incorporar al análisis están los siguientes:

- Riesgos de la innovación tecnológica.
- Riesgos de acceso o acceso no autorizado a la información relevante para la Unidad.
- Riesgos de disponibilidad o pérdida de continuidad de servicios de TI.
- Riesgo de infraestructura u obsolescencia tecnológica.

Con este análisis se pretende que la dependencia universitaria identifique, analice y evalúe los riesgos a los que está expuesta, con el propósito de gestionarlos para que no se afecte en el cumplimiento de sus objetivos.

Los principales hallazgos

"5. Ausencia de documentación formal referente a las medidas de seguridad de la información aplicadas en la Unidad."

- Clasificación de la información.
- Medidas de contingencias
- Procedimiento de respuesta a incidentes de seguridad.
- Medidas de seguridad física y lógica.
- ***Posibles Riesgos:***
- Inadecuada protección de la información

¿Cómo mejorar este aspecto?

"Solicitar al RID, que con base en el análisis de riesgos tecnológicos valide y documente las medidas de seguridad de la información utilizadas en la actualidad en su dependencia."

Para tal efecto considerar al menos lo siguiente:

- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La continuidad de los servicios de TI.

Lo anterior, con la intención de evitar la pérdida de continuidad de servicios y mejorar la protección de la información crítica de acuerdo a las prioridades establecidas por el Director de la Unidad.

Otros hallazgos típicos

"6. Los extintores utilizados para la protección ante un incendio tienen la carga vencida."

"7. No se cuenta con un plan formal de respaldos de la información generada y de interés para la Unidad."

"8. No se lleva un adecuado control de inventarios de los recursos de TI."

"9. Se desconoce la normativa sobre de TI de la UCR y de la CGR."

3 La Autoevaluación

Guía para aplicar una autoevaluación del cumplimiento de las normas

Los 6 pasos

Paso 1: Conoce a tu Unidad

Paso 2: Conócete ti mismo

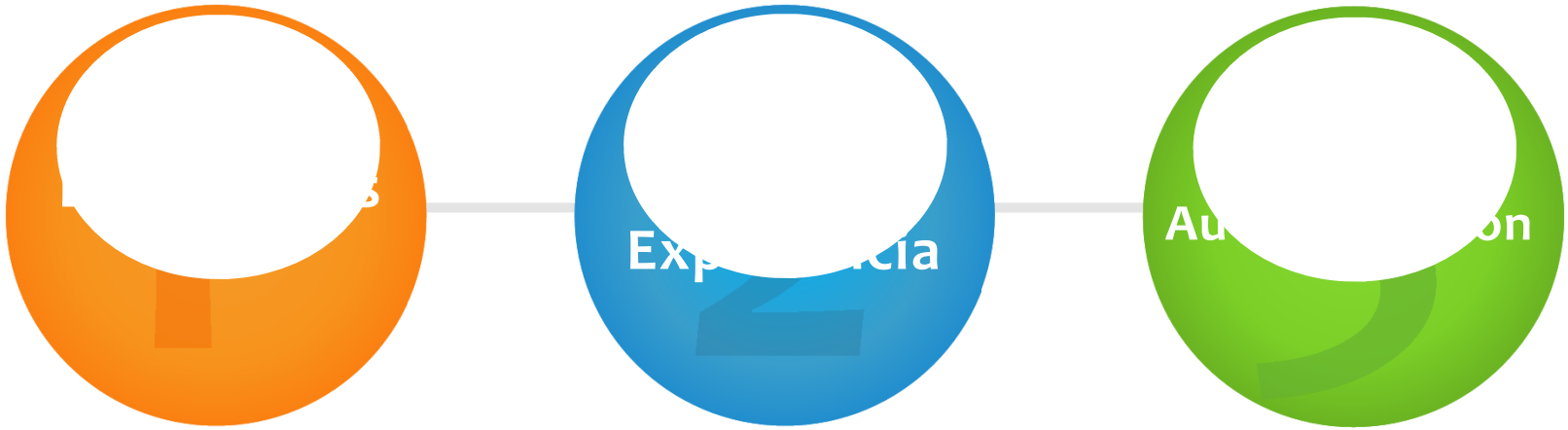
Paso 3: Aplicar el Cuestionario de Control Interno

Paso 4: Opinar respecto a lo evaluado

Paso 5: Recomendar oportunidades de mejora

Paso 6: Planear, Hacer, Revisar, Actuar

Resumen



Preguntas o Comentarios

UNIVERSIDAD DE COSTA RICA

CONTRALORÍA UNIVERSITARIA

MSI. Roberto Porras León
Jefe Sección de Auditoría de Sistemas y TI
roberto.porras@ucr.ac.cr

MUCHAS GRACIAS