04 de diciembre de 2015
OCU-R-166-2015

Doctor
Luis Bernardo Villalobos Solano, Decano
FACULTAD DE MEDICINA

Estimado señor:

La Sección de Auditoría de Sistemas y Tecnologías de Información de la Oficina de Contraloría Universitaria, lleva a cabo una serie de actividades de asesoramiento que incluyen la colaboración en procesos de autoevaluación relacionados con la gestión y control de las Tecnologías de Información (TI) en varias unidades y dependencias de la Institución.

En este documento encontrará un resumen del trabajo conjunto entre el Sr. Carlos Durán Vargas, RID de la Facultad, junto con el asesoramiento de los auditores de la Sección de Auditoría de Sistemas y Tecnologías de Información de nuestra Oficina, con el fin de identificar aquellas oportunidades de mejora en la gestión y control de las tecnologías de información que serán de gran beneficio para la Facultad.

Agradecemos el apoyo mostrado por su persona para el trabajo realizado y esperamos contar con su colaboración para la exitosa implementación de las mejoras que se mencionan en este documento, las cuáles deben ser coordinadas o ejecutadas por el RID, con la aprobación y apoyo del Decanato de la Facultad.

ANTECEDENTES

El proceso de evaluación por parte de la Sección de Auditoría de Sistemas y Tecnologías de Información de esta Oficina tiene como principal objetivo determinar si para la operación de la infraestructura tecnológica en la Facultad de Medicina se aplican los principales criterios de gestión y control interno establecidos por la normativa de Tecnologías de Información (TI) de la Contraloría General de la República[1] y buenas prácticas generalmente aceptadas, tales como: el marco de control recomendado en COBIT[2] (versión 5), ITIL[3] (versión 3) e ISO 27002[4].

El estudio incluyó el análisis de los siguientes temas relacionados con las Tecnologías de Información (TI), a saber:

---

[1] Normas técnicas para la gestión y el control de las Tecnologías de Información, N-2-2007-CO-DFOE.
[2] Objetivos de Control para la información y tecnología relacionada.
[3] Biblioteca de Infraestructura de Tecnologías de Información.
[4] Guía de buenas prácticas para la seguridad de la información.

Teléfonos: (506) 2511-1433 / (506) 2511-1418 • Fax: (506) 2224-3670

Sitio web: www.ocu.ucr.ac.cr • e-mail: contraloria.universitaria@ucr.ac.cr

a. Alineación, planificación y organización de TI.
b. Desarrollo, adquisición e implementación de TI.
c. Entrega, servicio y soporte de TI.
d. Supervisión, evaluación y valoración de TI.

Conforme a lo anterior, se realizaron dos reuniones de trabajo con el RID de la Facultad, entre los meses de junio y julio, en donde se revisaron varios aspectos, a saber:

- Se aplicó y analizaron las respuestas al cuestionario de evaluación de la gestión de TI.
- Se intercambiaron opiniones sobre las particularidades de la gestión y control de las Tecnologías de Información (TI) en la Facultad de Medicina.
- Se solicitó información, vía correo electrónico o personalmente, para fortalecer las respuestas dadas en el cuestionario de evaluación.
- Se realizó un recorrido por las instalaciones para identificar los componentes físicos de la infraestructura tecnológica, así como una inspección de los mecanismos que se utilizan actualmente para su gestión y control.

Adicionalmente, se tuvo la oportunidad de conversar con la Licda. Melissa Sequeira Nema, Jefa Administrativa de la Facultad y de quien depende directamente el RID, para darle a conocer la importancia de la labor de asesoría que realiza la Oficina de Contraloría Universitaria y solicitar el apoyo de la Administración a las diversas actividades que deben realizar en el RID, en el ámbito del proceso de evaluación.

RESULTADOS OBTENIDOS

Producto de las actividades de asesoramiento se han identificado oportunidades de mejora para las que se requiere el compromiso del Decanato de la Facultad y, en especial, del trabajo activo del RID y la colaboración del personal que participa en estos procesos, con el fin de fortalecer la gestión y control de la infraestructura tecnológica, obtener una mayor efectividad de los recursos informáticos y administrar eficazmente los riesgos tecnológicos asociados.

Se espera, por parte del RID, y con la aprobación del Decanato, la elaboración de un plan de acción para implementar las mejoras propuestas en este documento. Con base en las fechas establecidas en dicho plan, esta Contraloría programará una nueva visita para observar el grado de avance en la implementación de las mejoras.

Dado que este informe no reviste el carácter de auditoría sino que es el resultado de un proceso de asesoramiento, su redacción se orienta a identificar oportunidades de mejora para fortalecer la gestión de TI.

Esperamos que los aportes de esta Contraloría puedan sér de beneficio para el mejor desempeño de los procesos de gestión y control de las TI, que realiza el RID, en la Facultad.

OPORTUNIDADES DE MEJORA

En este apartado, se indican las actividades que se sugiere realizar, por parte del RID, con el apoyo y colaboración del Decanato de la Facultad. Debe tomarse en consideración que cada Dependencia Universitaria tiene diversos niveles de madurez en la gestión de TI, por lo que las oportunidades de mejora aquí planteadas deben entenderse en el sentido de seguir fortaleciendo los avances logrados hasta el momento y promover mayores logros en la gestión y control de las Tecnologías de Información.

1. **Diseñar una propuesta que incluya los objetivos, funciones, responsabilidades y servicios relativos a la función de TI, acorde con las necesidades de la Facultad, con el fin de ser evaluadas, revisadas e implementadas por el Decanato.**

   La gestión de TI es un conjunto de acciones que apoyan el logro de los objetivos de la Facultad. Detrás de esta función existen personas, infraestructura y procesos que dan soporte a los servicios ofrecidos. Dado lo anterior, se requiere que el personal tenga claro conocimiento acerca del rol que le corresponde desempeñar en la función de TI, en la operación de la infraestructura y los procesos tecnológicos que se llevan a cabo en esta Dependencia.

   La Facultad debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga una coordinación y comunicación efectivas con el Decanato, sea en forma directa o a través de la Jefatura Administrativa. Además, debe brindar el apoyo necesario para que dicha función de TI cuente con un grupo de colaboradores motivados, suficiente y competente y a los que se les haya definido, de manera clara y formal, su responsabilidad, límites de autoridad y funciones. Dicha propuesta debe quedar documentada y sujeta a su revisión y actualización, de acuerdo a las circunstancias.

2. **Elaborar una propuesta de clasificación de la información de la Facultad, que permita identificar aquella que se considera crítica, de acceso restringido o de acceso público, para efectos de determinar las medidas específicas de seguridad en el acceso y respaldo de la misma.**

   Considerar que esta clasificación tiene como propósito determinar cuáles serán las medidas de control o de seguridad que se deben implementar para proteger la información más sensible en contra del acceso no autorizado, al igual que sus mecanismos de respaldo, tanto internos como externos (respaldo secundario) como plan de contingencia.

   Dependiendo del tipo de información que se trate, deben establecerse diversos grados de protección, tales como claves de acceso o contraseñas. Algunos datos podrían requerir niveles de protección adicionales o de un tratamiento especial, por ejemplo del establecimiento de roles por cada tipo de usuario. Por esta razón, debe implementarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección para permitir o rechazar el acceso a la información.

Adicionalmente se debe tomar en cuenta el desarrollo de procedimientos o controles para el caso del desecho de dispositivos de almacenamiento que contengan información crítica o de acceso restringido. Esto aplica igualmente para el caso del mantenimiento en sitio, para el retiro de equipos para su reparación o sustitución, fuera de la Facultad, por parte de terceros.

3. **Diseñar una propuesta para el desarrollo de la infraestructura de TI en el corto, mediano y largo plazo, esto considerando los recursos disponibles y el aprovechamiento de los servicios ofrecidos por otras instancias institucionales.**

Esta acción permitirá priorizar las iniciativas de Tecnologías de Información y asegurar que los proyectos de TI se ejecuten de manera oportuna, correcta y que generen los resultados esperados desde el momento en que se inician, hasta que se concluyan. Por otra parte, permite gestionar el apoyo requerido de otras instancias institucionales.

Además, esta actividad proveerá un enfoque integrado de las áreas de administración de recursos, tiempo y costos, a la vez que brinda a los participantes o interesados mayor visibilidad del proceso y, en particular, promueve una gestión eficaz acerca del logro de los objetivos, metas y el avance alcanzado por cada uno de ellos.

4. **Identificar y evaluar las necesidades de capacitación para el personal de soporte técnico informático que permita cumplir con las funciones establecidas e incrementar el nivel de calidad de los servicios de TI requeridos por la Facultad.**

A modo de ilustración, usualmente los Administradores de Recursos Informáticos requieren formación y actualización técnica en temas tales como:

- Redes y comunicaciones.
- Sistemas operativos.
- Bases de Datos.
- Diseño de páginas Web.
- Ofimática.

Una vez identificados los requerimientos específicos de capacitación técnica, debe indicarse la prioridad de atención para cada uno, así como los beneficios potenciales esperados al recibir esta preparación complementaria. Se sugiere elaborar un plan de formación y llevar un registro sobre la ejecución de estas actividades de entrenamiento. Periódicamente debe entregarse al Decanato un informe de los logros obtenidos.

Pueden aprovecharse las oportunidades de capacitación y asesoría técnica que podría ofrecer el Centro de Informática en el campo de las Tecnologías de Información. Además, debe considerarse que no toda la capacitación requerida debe ser de pago obligatorio, hoy en día es posible también obtener mucha ayuda a través de fuentes complementarias, como lo es Internet, a través de sitios especializados y foros técnicos. Se sugiere incluir estos recursos alternativos como parte del plan de formación para los encargados de brindar servicios de soporte técnico en TI.

La implementación de esta práctica traerá como beneficio que el RID se encuentre suficientemente preparado para resolver con efectividad incidentes o eventos no deseados que podrían afectar la operación de la infraestructura tecnológica y consecuentemente, mejorar la calidad de los servicios que brinda la Facultad.

5. **Identificar y documentar las características de los servicios de TI que requiere la Facultad y establecer criterios de calidad para la entrega de los mismos.**

Para estos considerar al menos lo siguiente:

- Responsabilidades asociadas.
- Nombre del Servicio.
- Prioridad.
- Tiempo de respuesta.
- Disponibilidad horaria.
- 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 Facultad, obteniendo los siguientes beneficios:

- Determinar los parámetros para evaluar la calidad de cada servicio de TI.
- Priorizar la entrega de los servicios de TI a los interesados.
- Generar estadísticas acerca de la utilización de los diferentes servicios ofrecidos.
- Medir la satisfacción de los usuarios de los servicios recibidos.
- Informar al Decanato de la Facultad sobre los logros alcanzados en la entrega de servicios de TI.

6. **Establecer un proceso periódico de revisión, identificación, actualización y comunicación de los riesgos de TI, que se consideran críticos y que podrían afectar la prestación y calidad de los servicios de TI que requiere la Facultad, junto con las acciones para su mitigación.**

El proceso de análisis e identificación de riesgos inicia con la identificación de aquellos activos críticos (elementos de hardware, software, datos y personas que son necesarios para mantener los servicios que ofrece la Facultad), continúa con la evaluación de las amenazas (eventos que pueden afectar los activos atentando contra su integridad, funcionalidad o uso adecuado), clasificación de las amenazas, probabilidad de ocurrencia y el impacto en los activos. Por último se definen los controles para mitigar el riesgo.

Para la mitigación de los riesgos de TI, considerar la importancia de acceder a la experiencia del encargado o usuario responsable de la actividad, función o proceso analizado. Lo anterior, para identificar con claridad aquellos elementos de riesgo potencial y prever acciones para mitigar su impacto. La información obtenida debe ser comunicada al Decanato, incluyendo las justificaciones de las actividades prioritarias a ejecutar, así como su impacto para la Facultad y los recursos requeridos.

7. **Mantener un registro detallado y actualizado del inventario de activos informáticos de TI que incluya, entre otros, configuraciones, licencias de software, sistemas operativos e información de los proceso de compra de TI.**

Considerar que esta documentación es útil para tomar decisiones oportunas sobre los siguientes aspectos:

- Planificar la obtención de recursos de TI requeridos por la Facultad a través de los procesos de adquisición.
- Conocer en detalle sobre las configuraciones de hardware y software de cada equipo que opera en la Facultad.
- Identificar quien es el responsable por el activo informático.
- Estimar la vida útil de los recursos de TI y planificar su sustitución.
- Controlar eficazmente el préstamo o salida de equipos o periféricos fuera de las instalaciones de la Facultad.

8. **Formalizar los procedimientos que apoyan las actividades de gestión que realiza el personal que brinda los servicios de soporte de TI.**

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.
- La estrategia para la atención de solicitudes de los usuarios.
- Administración y actualización de sitios web.
- Administración de servidores.

La definición y formalización de este tipo de procedimientos facilita la ejecución de las actividades de soporte de TI, dado que describen las acciones que debe seguir el personal encargado para atender sus labores diarias, así como aquellas que se ejecutan en periodos especiales, por ejemplo: en periodos de vacaciones del personal docente o estudiantil, así como las tareas técnicas previas a los recesos de Semana Santa o fin de año.

9. **Elaborar una programación básica para la ejecución de las actividades técnicas de apoyo, por parte de los encargados de brindar los servicios de soporte de TI, de acuerdo con la periodicidad que se considere conveniente a los requerimientos de la Facultad y rendir un informe periódico al Decanato sobre los logros alcanzados.**

A continuación, se citan algunas de las actividades que podrían considerarse dentro de esta programación:

- El objetivo y descripción de la tarea o actividad técnica a ejecutar.
- La prioridad establecida para la ejecución de cada tarea técnica.
- La persona o equipo de trabajo técnico responsable por la ejecución de cada actividad.
- Los recursos materiales requeridos (herramientas, manuales, entre otros).
- Fechas estimada de inicio y conclusión de la actividad.
- Encargado de la supervisión.
- Resultados esperados y los obtenidos al final de la ejecución.

Conviene entregar al Decanato de la Facultad, una copia de la documentación relacionada con la programación de las actividades de Tecnologías de Información (TI) e informar oportunamente acerca de los logros obtenidos.

La implementación de esta práctica podría generar los siguientes beneficios:

- Garantizar que los roles y responsabilidades de los funcionarios de TI se ejerzan de manera estructurada, dentro de los límites autorizados y en cumplimiento de las directrices, metas y objetivos propuestos.
- Facilitar al Decanato la tarea de evaluación del personal que brinda los servicios de soporte de TI y el reconocimiento por su desempeño.
- Identificar y realizar oportunamente los cambios requeridos sobre la prioridad de las actividades técnicas que se deban realizar durante determinado periodo para cumplir con los objetivos establecidos.

10. **Identificar y evaluar las acciones para hacer frente a eventuales fallas e incidentes tecnológicos que puedan afectar los recursos prioritarios de sistemas de información: hardware, software, instalaciones, datos y la red interna de comunicaciones.**

Considerar que la definición de estas acciones para la atención de incidentes o fallas incluye un conjunto específico de medidas para responder ante un evento o incidente no deseado, lo que significa disponer de recursos suficientes y adecuados, definición clara y precisa de procedimientos que permitan después de la crisis, volver al funcionamiento normal tan rápidamente como sea posible y con el menor impacto para la Facultad.

Tomar en consideración que algunos de los eventuales incidentes o fallas que podrían afectar la operación de los sistemas de información, hardware, software o la red interna de comunicaciones, podrían traducirse, entre otras, en:

- Afectación de la imagen de la Facultad.
- Pérdida de productividad.
- Malestar y frustración de los usuarios.
- Reducción drástica en el nivel de calidad del servicio.
- Sobrecarga de trabajo para los colaboradores.
- Duplicación de labores sustantivas.
- Pérdida de información sensible y crítica

Se sugiere agrupar las acciones para la atención de fallas o incidentes, dentro de las dos categorías se describen a continuación:

- *Acciones de Prevención:* Comprende las acciones para la prevención de los incidentes que podrían perjudicar la operación normal de la infraestructura tecnológica instalada. Por ejemplo, dentro de este plan podría incluir:

  a. Procedimientos para la instalación y mantenimiento periódicos del hardware y software.
  b. Contar con procedimientos para el respaldo de información sensible o critica.
  c. Implantar medidas de seguridad físicas: sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.
  d. Aplicar sistemas de encriptación de la información, si se requiere.
  e. Implementación de acciones de protección para asegurar la confidencialidad de las contraseñas de acceso a los equipos y sistemas ("password"). Realizar cambios periódicos de contraseñas considerando la criticidad y sensibilidad de la información procesada por la dependencia.
  f. Monitoreo continuo de la red interna de comunicaciones.
  g. Mantener actualizado el sistema operativo y consola antivirus.

- *Acciones de Recuperación*: Incluye las acciones a seguir cuando un incidente transcendió el nivel de prevención, es decir, se comprueba que la operación de la infraestructura tecnológica fue afectada. En tal caso, se requieren ejecutar acciones para volver a la normalidad lo antes posible y con el mínimo impacto.

  a. Contar con respaldos fuera de sitio de acuerdo con la periodicidad requerida.
  b. Aplicar procedimientos para la recuperación de los respaldos de información.
  c. Respaldar el software de aplicaciones, en su última versión para facilitar la recuperación.
  d. Revisar y probar periódicamente los procedimientos de atención de incidentes.
  e. Contar con personal capacitado para la atención de incidentes y emergencias.

Debe tomarse en cuenta que ambas categorías de acciones constituyen herramientas útiles para garantizar que se contará con las condiciones de operación controlada en caso de presentarse incidentes o fallas en la operación de la infraestructura tecnológica que opera en la Facultad, y consecuentemente, que la afectación de la calidad de los servicios de TI será mínima si llega a presentarse un evento o incidente no deseado.

11. Documentar, aprobar y comunicar los procedimientos para el respaldo de la información.

La definición de estos procedimientos es útil para proteger la información ante pérdida o daño de la misma. Considerar lo siguiente:

- Definir formalmente y efectuar rutinas de respaldo.
- Custodiar los medios de respaldo en ambientes adecuados.
- Controlar el acceso a dichos medios.
- Establecer procedimientos de control para los procesos de restauración, que permitan verificar la integridad de los respaldos de información.

El contar con un procedimiento de respaldo adecuado pretende asegurar que estos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente por parte del personal responsable de esta tarea realizando las pruebas de recuperación respectivas.

12. Tomar las previsiones necesarias para que el personal de TI revise la normativa aplicable al ámbito de las tecnologías de información con el fin de analizar exhaustivamente su contenido y las posibilidades de implementación y aprovechamiento.

Dentro de la normativa a revisar se cita por ejemplo las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la Contraloría General de la República, así como aquellas que la Institución ha emitido o avalado para el fortalecimiento del ambiente de control relativo a las TI.

En su conjunto, es importante recordar que estas normas establecen criterios para orientar la gestión de las Tecnologías de Información dentro de un marco de control que procure el logro de las metas y objetivos que la Administración Activa pretende alcanzar por medio de su implementación. Además, conviene recordar que las Tecnologías de Información se han convertido en un instrumento esencial para la prestación de servicios ágiles y flexibles, por lo que los responsables de su gestión deben establecer, mantener, evaluar y perfeccionar un marco de control centrado en la aplicación continua de sanas prácticas de Tecnologías de Información (ejemplos: el marco de control recomendado en Cobit versión 5, ITIL versión 3 e ISO 27002).

Igualmente, resulta oportuno agregar, que en general, las organizaciones cada día más brindan o requieren servicios más complejos, flexibles, de calidad e innovadores, los que comúnmente serán soportados por las Tecnologías de Información, elemento que evoluciona constantemente; por lo que resulta necesario estructurar estos servicios bajo un esquema de sanas prácticas que permitan garantizar servicios consistentes y efectivos, y alineados con los objetivos y estrategias de la Institución.

Los aportes brindados en este documento de asesoría, pretenden contribuir con el fortalecimiento de los mecanismos de control sobre la gestión de la infraestructura tecnológica, con el fin de obtener una mayor eficiencia, seguridad y gobernabilidad de las Tecnologías de Información (TI) en la Facultad, y al mismo tiempo garantizar razonablemente que eventos e incidentes tecnológicos no deseados sean prevenidos, detectados y corregidos oportunamente.

En visitas posteriores, a través de la comunicación remota o de nuevos oficios de asesoría, estaremos apoyando los esfuerzos de la Facultad para mejorar la gestión de la infraestructura tecnológica, conocer el avance y los resultados obtenidos durante la implementación de las oportunidades de mejora.

Finalmente, agradeceremos nos remita el plan de acción previsto y sus comentarios a este documento de asesoría y nos ponemos a su disposición para aclarar cualquier inquietud o duda sobre su contenido.

Atentamente,

M.A.T.I. Luis Antonio Segura Suárez
Auditor Encargado

M.S.I. Roberto Porras León, Jefe
Auditoría de Sistemas y Tecnologías de Información

Código: 5-1-3-53-2015 (76)