



ESTÁNDARES Y BUENAS PRÁCTICAS: CUESTIÓN DE SUPERVIVENCIA

STANDARDS AND BEST PRACTICES: A MATTER OF SURVIVAL

Autora:

Zulema Furones Fernández. Universidad de Burgos. zulema@ubu.es

Resumen:

En este artículo se señalan algunos de los retos que tienen que afrontar las universidades desde la perspectiva de las Tecnologías de la Información (TI), así como las inquietudes que más preocupan a expertos en este ámbito.

La transformación digital implica un cambio en el papel que los responsables de TI desempeñamos en nuestras organizaciones, con foco en la detección y aprovechamiento de nuevas oportunidades basadas en la tecnología, actuando como facilitadores y dinamizadores del cambio. Pero para innovar e implantar nuevas estrategias, es fundamental saber gobernar las TI, considerar los riesgos y contar con un entorno adecuado de gestión y operativo: personas, procesos y herramientas tecnológicas.

La implantación de marcos de gobernanza y de gestión, estándares y buenas prácticas, es imprescindible para consolidar los procesos y estructuras que permitirán enfrentarnos a los retos con suficientes garantías de éxito.

Abstract:

This article aims to show some of the challenges that the universities have to face from the perspective of Information Technologies (IT), as well as the issues which concern the experts in this field.

The digital transformation means a change in the traditional role of the IT department director, who becomes more focused on the detection and adoption of new technology-based opportunities, acting as facilitator and leading the change. But IT governance is critical to innovate and implement new strategies, being aware of the risks and consolidating an adequate management and operating environment: people, processes and technological tools.



Implementing governance and management frameworks, standards, and best practices, are essential to consolidate the required processes and structures that will allow us to face the challenges with enough guarantees of success.

Palabras clave:

TI; Estándares; Universidad.

Keywords:

IT; Standards; University.

Hace unas semanas un compañero del Servicio de Informática y Comunicaciones se quejaba con cierto tono de reproche, de que nunca paremos, de que siempre estemos haciendo nuevos proyectos: ¡¡¡tenemos que parar y poner orden!!!

Reflexionando sobre el asunto, en la soledad del despacho del Jefe, tan criticado e incomprendido, a veces, pensaba que también a mí me gustaría salir de este bucle infinito, de esta espiral creciente de cambios y me preguntaba si hay algún CIO que pueda permitirse el lujo de parar, reconstruir tranquilamente los cimientos de los sistemas, las redes o las aplicaciones y volver a seguir en la brecha de la imparable demanda y evolución o disrupción, según los casos, de los servicios de TI.

En el informe *EDUCAUSE* de 2015¹, se subrayaba que en los últimos años el cambio se ha ido incrementado y a expandiéndose a diversos frentes, hasta convertirse en un estándar en sí mismo, derivado de los nuevos retos y tendencias: “Móvil - Cloud - Big Data- Valor de negocio- Ágil- Transformación- Social- Análisis de Datos- Aprendizaje Online”. En estas circunstancias el problema al que nos enfrentamos es que subyacente a toda esta situación de cambio continuo, hay que seguir con el trabajo del día a día, donde los retos son más complejos que nunca.

¹ <http://er.educause.edu/articles/2015/1/top-10-it-issues-2015-inflection-point>



“Nada ha cambiado y todo ha cambiado”. Parménides y Heráclito, siguen en nuestras vidas. Para nuestro amigo Parménides el cambio es una ilusión de los sentidos, un engaño. En realidad, debajo de las apariencias nada cambia jamás, todo es estable y fijo, sujeto a las reglas de la razón, siempre fiables, y siempre exactas. Por el contrario Heráclito afirmaba que la realidad es contradictoria, variable, y cambiante. Todo es dinámico, nada es permanente, el cambio es lo único real, lo único que no es ilusorio.

Dejando aparte las cuestiones filosóficas, para ilustrar la complejidad actual en la prestación de servicios TI, podemos hacer referencia al catálogo de servicios TIC elaborado por CRUE-TIC, en el que se pone de manifiesto que en las universidades españolas llegamos a ofrecer más de 100 servicios de TI, que dan soporte a los correspondientes servicios universitarios. Estos servicios se sustentan en aplicaciones, sistemas, infraestructuras y tecnologías que cambian y evolucionan a un ritmo frenético; continuamente surgen nuevas herramientas, versiones, bugs, parches, necesidad de actualizaciones, etc.

A medida que se incrementa la complejidad de los sistemas también lo hace el potencial de brechas de seguridad y la necesidad de asegurar el cumplimiento de, las cada vez más numerosas, normativas y regulaciones. Hay que establecer políticas de seguridad que permitan cumplir los requerimientos legales (LOPD², ENS³...) sin afectar al correcto funcionamiento de los servicios y al trabajo de los miembros de la Comunidad Universitaria.

La Universidad, cada vez más, demanda los servicios de TI en entornos 24x7. Los estudiantes se matriculan y acceden a las plataformas de e-learning a cualquier hora, muchos de madrugada, en ocasiones consecuencia de la creciente internacionalización; los investigadores presentan continuamente proyectos de investigación con plazos apurados, el correo electrónico y la red deben estar

² <https://boe.es/buscar/act.php?id=BOE-A-1999-23750>

³ <http://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>

siempre operativos, etc. Todo ello provoca que resulte extremadamente difícil encontrar ventanas de tiempo para actualizar los servicios.

Todos estos factores son los que han propiciado una tendencia imparable hacia la externalización y los servicios en la nube, que pueden aliviar, en parte, algunos de los problemas mencionados. No obstante, la externalización y la adopción de la nube deben hacerse con cierta cautela. No todos los servicios pueden o deben ser migrados a la nube. Se necesita contar con una clara estrategia y con capacidad en la organización para una correcta gestión de los proveedores. El CIO debe conocer y trasladar al equipo de gobierno, cuál es el riesgo asociado a cada nueva iniciativa en este contexto.

Se deben garantizar la prestación y la calidad de los servicios, independientemente de que el entorno subyacente físico, virtual o cloud se ejecute en un Centro de Datos propio o en la nube de algún proveedor. Conviene no olvidar que aunque se haya contratado externamente la prestación del servicio, éste sigue siendo responsabilidad de la institución.

El mayor alcance de las aplicaciones que aporta la nube también afecta a la seguridad. Ahora los responsables de TI tenemos que pensar en términos de gestión de identidades y control de accesos, ampliando los mecanismos de seguridad que pasan del ámbito local a un ámbito más amplio formado por las nubes de los diversos proveedores y los usuarios remotos.

Como referencias importantes se mencionan aquí la *Guía 823-Cloud_Computing del CCN*⁴, donde se indica que el proveedor de servicios cloud (CSP) está obligado a cumplir todas las medidas del Anexo II del ENS⁵ para el nivel de disponibilidad requerido por el cliente.

⁴ https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/823-Seguridad-en-entornos-cloud/823-Cloud_Computing_ENS.pdf

⁵ <http://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>

Otra referencia obligada es la *Guía para clientes que contraten servicios de Cloud Computing*, de la Agencia Española de Protección de Datos⁶.

Las guías anteriores ponen de manifiesto la necesidad de recabar información sobre las condiciones de prestación del servicio en la nube que se va a contratar al proveedor cloud y la importancia de recogerlas y explicitarlas en la relación contractual.

El último informe *EDUCAUSE 2016*⁷ coloca la Seguridad de la Información en el primer puesto de las 10 inquietudes más importantes relativas a las TI y subraya la necesidad de desarrollar un enfoque holístico y ágil de la seguridad de la información para crear una red segura, desarrollar políticas y reducir la exposición institucional a las amenazas de seguridad.

En dicho informe se menciona, a mi juicio, un aspecto de especial relevancia y es que si la unidad centralizada de TI en la organización no es lo suficientemente ágil en la supervisión e implementación de los servicios cloud, los usuarios de la organización tenderán a implantarlos por su cuenta y en este caso, lo más probable, es que no se consideren las adecuadas medidas y salvaguardas poniendo en riesgo datos personales o institucionales.

Por otro lado, las aplicaciones y servicios son muy heterogéneos pero deben integrarse e interoperar. Las arquitecturas orientadas a servicios y la gestión por procesos son una realidad aún lejana en la mayoría de nuestras universidades. A medida que crece la adopción del cloud, se va produciendo una mayor proliferación de entornos híbridos donde conviven los servicios en cloud privada con los ofrecidos en cloud pública y los on-premise. La orquestación de esta complejidad es otro de nuestros principales retos.

⁶http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

⁷<http://er.educause.edu/articles/2016/1/top-10-it-issues-2016>

Con la proliferación de dispositivos personales (tablets, smartphones) ha surgido un nuevo entorno de trabajo en el que las fronteras entre lo personal y lo profesional se diluyen. La tecnología personal (aplicaciones móviles, plataformas de almacenamiento cloud, herramientas de colaboración...) utilizada también en el entorno profesional, difumina la frontera entre ambos mundos y nos plantea un nuevo reto: establecer políticas asociadas al concepto "Bring your own device" redefiniendo y delimitando el soporte que vamos a prestar a los dispositivos y aplicaciones que los usuarios puedan traer al trabajo.

En este escenario de cambios, retos y oportunidades las unidades de TI continuamos ejecutando servicios críticos para cumplir con los fines de la universidad y proporcionando soporte a nuestros usuarios. Nuestro personal continúa apagando fuegos con más frecuencia de la deseada e incluso las operaciones habituales están sometidas a las fuerzas del cambio.

Como se puso de manifiesto en el curso de *Experto en Dirección de Servicios TI de Universidades*, organizado por la Universidad de Castilla la Mancha bajo el patrocinio de CRUE-TIC y cuya primera edición se impartió en el curso 2014-2015, existen algunos mecanismos para que los CIOs podamos dormir tranquilos en medio de este caos.

En los últimos años los estándares, marcos de referencia y buenas prácticas están proliferando y su uso se ha popularizado. Se busca que los procesos y las actividades de las organizaciones se gestionen de una forma estructurada, sistemática y medible. Algunas buenas prácticas como ITIL (*Information Technology Infrastructure Library*) datan de los años 90, no son un concepto nuevo, pero su implantación en las universidades es relativamente reciente.

Según apunta Francisco José Sampalo, compañero de la Universidad Politécnica de Cartagena, de los datos obtenidos en el informe *UNIVERSITIC-2015*⁸, cuyo objetivo es realizar un análisis detallado de la situación de las TIC en el Sistema

⁸ <http://tic.crue.org/publicaciones/informe-universitic-2015/>

Universitario Español (SUE), se desprende que un 56% de las Universidades tienen implantado ITIL como modelo para la gestión del servicio TI; un tercio aplica la ISO 9000 para la gestión del servicio TI, mientras que la cuarta parte dispone de un sistema de gestión de la seguridad de la información según la ISO 27000.

¿Podemos decir entonces que seguir estándares, marcos de referencia, y buenas prácticas es una tendencia? La respuesta, en mi opinión, es que su adopción es imprescindible: se trata más bien de una cuestión de supervivencia.

Por este motivo, muchos responsables de TI están adoptando la estrategia de utilizar marcos de referencia para la gestión de los servicios de TI. Como veremos más adelante existe un amplio abanico de posibilidades que cubren la mayor parte de las actividades relacionadas con la prestación y gestión de servicios de TI (IT service management): gestión de proveedores, gestión del riesgo, gestión de la seguridad, gestión de proyectos, etc.

En un primer momento podría parecer que estos marcos de referencia son excesivamente restrictivos y burocráticos; sin embargo, bien implementados, pueden proporcionar la estabilidad imprescindible en tiempos de cambio para crear estructuras y procesos sostenibles, que permitan la flexibilidad y la agilidad necesarias para adaptarse más fácilmente a las circunstancias cambiantes.

Los responsables de TI tenemos que evolucionar desde modelos de gestión centrados en la reducción de los costes operativos, para contribuir a una auténtica transformación digital de nuestras universidades promoviendo y usando las posibilidades de la tecnología para aportar valor a nuestros fines fundamentales: docencia, investigación y transferencia de conocimiento hacia la sociedad.

Concretamente uno de los principales retos a los que se enfrentan las universidades es el de cómo aplicar la tecnología en el ámbito de la docencia para mejorar los resultados académicos y las tasas de empleabilidad de los egresados, así como la captación y retención de los estudiantes.

Una posible solución a este reto pasa por incrementar la comunicación y fomentar una colaboración más estrecha entre los distintos colectivos de la Comunidad Universitaria, docentes, estudiantes y personal de TI, en la adopción de la tecnología, de forma que cada uno pueda aportar su experiencia en los ámbitos de su competencia y expresar sus inquietudes y necesidades, de forma que se puedan adoptar las soluciones tecnológicas más adecuadas y se tengan en cuenta las implicaciones en la seguridad de la información, la gestión de los datos y la arquitectura tecnológica de la organización.

Los equipos de gobierno de las universidades deben entender el potencial de las tecnologías de la información para contribuir a la transformación de la Universidad, pero es también fundamental saber que las inversiones en tecnología, por sí solas, no son suficientes para alcanzar los objetivos deseados y existe un importante trasfondo de cambio cultural, de procesos y recursos organizativos que es necesario impulsar y liderar para poder materializar todo ese potencial.

Afortunadamente, nuestras universidades cuentan con relevantes foros donde compartir experiencias, como CRUE-TIC y RedIRIS, que tratan de difundir el conocimiento y las mejores prácticas de algunas instituciones, permitiendo a las universidades conocerlas y adaptarlas, para innovar y crear nuevos servicios; se trata de un modelo de relación que permite la colaboración competitiva.

Para innovar, para poner en marcha las estrategias de la Universidad y poder cumplir con los objetivos establecidos, hay que saber gobernar las TI y contar con un adecuado entorno de gestión y operativo: personas, procesos y herramientas (tecnología). Es el nuevo concepto de dual TI que debe conjugar y equilibrar dos ámbitos complementarios: estrategia y operación.

Los responsables de TI debemos conocer y apoyarnos en un conjunto de prácticas que nos ayuden a gestionar las infraestructuras, las personas y los procesos, para mejorar la fiabilidad y el rendimiento de los sistemas de información y la entrega de nuestros servicios. La arquitectura de TI, la optimización de procesos, la gestión de



servicios y la gestión de riesgos, son algunos de los mecanismos que nos permiten afrontar el caos y esta moderna Torre de Babel de lenguajes, sistemas y tecnologías.

Carlos Manuel Fernández y Mario Piattini son coordinadores del libro *Modelo para el gobierno de las TIC basado en las normas ISO*⁹ de AENOR ediciones, donde se explican las diferencias entre gestión y gobierno de las TIC y se presentan algunas de las principales normas y estándares para ambos conceptos.

Hoy en día disponemos de una serie de marcos de gestión con reconocimiento internacional, para abordar la organización de las tecnologías de la información y las comunicaciones. Los departamentos de TI debemos trabajar en implantar estas buenas prácticas para conseguir un uso eficaz, eficiente y transparente de las TIC en nuestras organizaciones.

A continuación, con intención meramente divulgativa, se hace una breve recopilación de algunos de los estándares, marcos de referencias y buenas prácticas que pueden resultar de interés para los responsables de TI.

Gobierno de TI

El gobierno de TI puede definirse como el sistema por el que se dirige y controla la utilización actual y futura de las tecnologías de la información basado en una estrategia definida.

Los programas de gobernanza deben ser capaces de priorizar las inversiones estratégicas en TI dentro del conjunto de recursos institucionales compartidos, especialmente en tiempos de escasez presupuestaria, de forma que se apoye la innovación continua y el crecimiento de la organización, a la vez que se equilibra el conjunto del portfolio y se garantiza el soporte financiero de las operaciones necesarias.

⁹ <http://www.aenor.es/aenor/normas/ediciones/fichae.asp?codigo=10179>

En ausencia de un gobierno de TI institucional, los proyectos se priorizarán en función de aquellas áreas que tengan mayor influencia o más fácilmente consigan recursos económicos para sus prioridades, teniendo como consecuencia, en muchos casos, que proyectos importantes e incluso críticos carezcan de financiación si no tienen un buen patrocinador.

En ocasiones, la financiación para nuevos proyectos es relativamente fácil de conseguir, sin embargo, obtener financiación adicional para la sostenibilidad de las operaciones ya comprometidas puede resultar mucho más difícil. Es fundamental asignar recursos para cubrir tanto el coste de los nuevos desarrollos o la implantación de nuevas infraestructuras de TI, como su financiación durante su ciclo de vida completo.

Se necesitan, por tanto, estrategias rigurosas que ayuden al desarrollo de modelos de financiación que estén alineados con el cumplimiento de los objetivos de la universidad y garanticen la coherencia y la transparencia.

Existen muchos marcos para el gobierno de las TIC, pudiendo citar los siguientes:

- *ISO/IEC 38500:2015, Tecnología de la Información -- Gobierno de TI para la organización*¹⁰
- *COBIT 5 Framework, Un marco de negocio para el gobierno y la gestión de las TI de la empresa*¹¹
- *UNE-EN ISO 22301:2015: Protección y seguridad de los ciudadanos. Sistema de gestión de continuidad del negocio. Especificaciones. (ISO 22301:2012).*¹²

Según el modelo ISO/IEC 38500, la dirección de cualquier organización ha de gobernar las TI mediante tres tareas principales: evaluar, dirigir y monitorizar, aplicadas a seis principios: responsabilidad, estrategia, adquisición, rendimiento, cumplimiento y factor humano.

¹⁰ http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62816

¹¹ <http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>

¹² <http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0054336&pdf=>

COBIT® (Control Objective for Information and Related Technology) es un modelo de referencia para el Gobierno y la Gestión de las TIC creado por ISACA® y el IT Governance Institute, que aporta a directivos, auditores y usuarios de las TI un conjunto de indicadores, procesos y buenas prácticas, mundialmente aceptadas, que permiten maximizar los beneficios generados por el uso de las Tecnologías de la Información en las organizaciones, mediante la implantación de políticas apropiadas de gestión y el control de las mismas.

Conviene recalcar que el marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, que requieren diferentes estructuras organizativas y sirven a diferentes propósitos. Según la visión de COBIT 5 esta distinción clave entre gobierno y gestión es la siguiente:

- El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.
- La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Además, no hay que olvidar que el buen gobierno TI forma parte del buen gobierno corporativo y ambos deben funcionar de forma coordinada, apoyando a los sistemas de gestión de servicios, a la seguridad y a la continuidad de las actividades de la universidad.

Gestión de Servicios de TI

Los marcos de referencia en la gestión de servicios de TI (IT Service Management) ayudan a entender a las organizaciones de TI la interrelación entre los sistemas y servicios, facilitando el trabajo de los usuarios que se apoya en estos servicios y aplicando políticas y procedimientos que contribuyan a reducir el impacto de los fallos o de los cambios en las infraestructuras.

En este ámbito podemos destacar dos referencias importantes:

- UNE-ISO/IEC 20000-1:2011. Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS).¹³
- ITIL® Best Practice¹⁴

ITIL es un conjunto de mejores prácticas basadas en procesos, que ofrece soluciones para la gestión de servicios de TI. No es una metodología, sino una colección de buenas prácticas, es decir, unas recomendaciones. ITIL no indica cómo deben ser los procesos, sino que define los que deben existir y cada departamento de TI los puede adaptar según su modelo de negocio y sus particularidades. Los procesos se agrupan en cinco grupos: procesos de estrategia del servicio, procesos de diseño del servicio, procesos de transición del servicio, procesos de operación del servicio y procesos de mejora continua.

Se enfoca en el ciclo de vida del servicio ofreciendo una visión completa del funcionamiento de las tecnologías de la información, orientada a un departamento o unidad de TI, contemplando aspectos tan diversos como la gestión financiera, la gestión de los niveles de servicio, la gestión de la configuración o la gestión de los problemas e incidencias.

La sistematización y la documentación, unidas a la formación y la capacitación, hacen que una buena gestión de las TI permita ahorrar costes y ofrecer servicios más competitivos. La colaboración, coordinación y comunicación, junto con la cultura

¹³ <http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0048609>

¹⁴ <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>

del servicio y la orientación al cliente, son aspectos básicos para que los servicios de TI se perciban como fiables, confiables y transparentes.

Gestión de Seguridad y Gestión de Riesgos. Privacidad y legalidad

Mientras que los procesos institucionales soportados por las TIC traen nuevas ventajas y oportunidades, también conllevan un número creciente de riesgos. Cuestiones como la seguridad, la privacidad y el fraude preocupan cada vez más a las organizaciones. Estos y otros riesgos necesitan ser conocidos, gestionados y mitigados razonablemente. La Universidad, que tradicionalmente se ha movido en entornos no restrictivos respecto al uso de herramientas y recursos tecnológicos, no puede ser ajena a estas nuevas circunstancias.

Algunas de las principales normas y estándares en el ámbito de la Seguridad de la Información son:

- UNE-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos¹⁵
- ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management¹⁶
- ISO/IEC 27018:2014 Information technology. Security techniques . Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors¹⁷

Adicionalmente, en nuestro país existen unas regulaciones bastante completas y exigentes, como son la LOPD y el Esquema Nacional de Seguridad, este último de aplicación en el ámbito de la administración pública, incluyendo a las universidades.

¹⁵ <http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053761>

¹⁶ http://www.iso.org/iso/catalogue_detail?csnumber=56742

¹⁷ http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Conocer el riesgo al que están sometidos los sistemas de información resulta imprescindible para poder realizar una adecuada gestión de los mismos. Para ello, se deben realizar análisis periódicos con la ayuda de herramientas que permitan una medición objetiva del riesgo. Según los resultados de la valoración, se implantarán controles y se asignarán recursos, siguiendo una estrategia de gestión de riesgos definida. Las decisiones sobre la aceptación del nivel de riesgo obtenido en cada análisis de riesgos, las tiene que tomar la dirección de la empresa u organización que será responsable de asignar los recursos para reducir o mitigar el riesgo o tendrá que asumir las consecuencias si éste llegara a materializarse.

Respecto al cumplimiento de la legislación relativa a la protección de datos de carácter personal, es necesario comprender su sentido, objetivos y principios, poniendo en valor el derecho fundamental a la privacidad. Cabe destacar aquí el concepto de “Privacidad desde el diseño” (Privacy by design), que consiste en tener en cuenta la implementación de la seguridad desde las fases más tempranas del diseño de los procesos y del desarrollo de software.

En definitiva, se trata de conocer y aplicar los mecanismos y herramientas que nos ayuden a asegurar las dimensiones de seguridad (confidencialidad, autenticidad, disponibilidad, integridad y trazabilidad) de los sistemas de información, que constituyen la base imprescindible para realizar las actividades que contribuyen a la consecución de los fines de la universidad.

Conclusiones

El éxito y quizá incluso la supervivencia de la educación superior dependen más que nunca de la tecnología.

Según se indicaba en el informe *EDUCAUSE* de 2014¹⁸, muchos líderes institucionales creen que las soluciones tecnológicas son más fáciles y baratas de lo que realmente son. Ignorar la complejidad subyacente puede llevar a cometer errores que pongan en peligro la continuidad de las operaciones. Los responsables

¹⁸ <http://er.educause.edu/articles/2014/3/topten-it-issues-2014-be-the-change-you-see>



de TI tenemos que saber comunicar y transmitir más efectivamente a los equipos de gobierno de las universidades, la realidad, oportunidades y amenazas de las tecnologías de la información.

Las universidades necesitan adaptarse rápidamente a los cambios que la tecnología está provocando en los hábitos y comportamientos de la sociedad y para ello es fundamental innovar y desarrollar un espíritu emprendedor. Los responsables de las unidades de TI tenemos que poner el foco en la detección y aprovechamiento de nuevas oportunidades basadas en la tecnología, debemos influir, innovar y asesorar, actuando como facilitadores del uso en nuestra organización de los medios tecnológicos más adecuados.

Pero junto a este nuevo rol, es también imprescindible seguir gestionando, operando y controlando el departamento de TI, extendiendo los conceptos de gobierno, gestión del riesgo y cumplimiento normativo, a toda la universidad.

La creciente complejidad requiere modelos de gobierno y de gestión que permitan establecer las directrices, pautas y mecanismos para obtener el mayor valor de los recursos disponibles. Las nuevas iniciativas, estratégicas o no, tienen que abordarse con suficientes garantías de continuidad. Tenemos que proteger a nuestras universidades y asegurar el cumplimiento normativo. La utilización de marcos de referencia, estándares y buenas prácticas son imprescindibles para abordar estas tareas con suficientes garantías de éxito.

En este artículo se han señalado algunos de los aspectos relativos a los procesos y las tecnologías, pero no hay que olvidar que los recursos más importantes de cualquier organización son las personas. Los nuevos retos a los que nos enfrentamos no se pueden abordar con viejas estructuras organizativas y la captación y la retención del talento, no son cuestiones baladíes. Los mecanismos obsoletos de selección de personal y las RPTs (Relaciones de Puestos de Trabajo) que permanecen invariables durante años, encorsetan las posibilidades y frenan la evolución y la carrera profesional del personal.



Si la tecnología es el motor del cambio de las organizaciones, la motivación y la profesionalización de los técnicos de TI debería ser una cuestión de importancia estratégica para las universidades. El reconocimiento de este personal en nuestras organizaciones no suele estar a la altura de la cualificación requerida, la responsabilidad asumida y el nivel de exigencia del trabajo que diariamente se desarrolla.

La transformación digital de las universidades, requiere que las ruedas de la maquinaria de nuestras unidades de TI estén perfectamente engranadas y ajustadas para mantenerse continuamente girando. Y hablando de girar y de ruedas, no se puede olvidar mencionar aquí la base fundamental de cualquier proceso de mejora continua: Plan-Do-Check-Act (PDCA), que debe aplicarse de forma iterativa en el proceso de implantación de los marcos, normas y estándares mencionados.

BIBLIOGRAFÍA

- *COBIT 5 Framework*. ISACA, 2012.
- FERNÁNDEZ SÁNCHEZ, Carlos Manuel; PIATTINI VELTHUIS, Mario. *Modelo para el gobierno de las TIC basado en las normas ISO*. AENOR, 2012. ISBN 978-84-8143-790-4.
- GÓMEZ FERNÁNDEZ, Luis. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas*. AENOR, 2012. ISBN 978-84-8143-749-2.
- GRAJEK SUSAN and the 2013–2014 EDUCAUSE IT Issues Panel. Top-Ten IT Issues, 2014: Be the Change You See. [Fecha de consulta: 13/09/2016]. Disponible en <http://er.educause.edu/articles/2014/3/topten-it-issues-2014-be-the-change-you-see>



- GRAJEK SUSAN and the 2014–2015 EDUCAUSE IT Issues Panel. *Top 10 IT Issues, 2015-Inflexion Point*. [Fecha de consulta: 13/09/2016]. Disponible en <http://er.educause.edu/articles/2015/1/top-10-it-issues-2015-inflexion-point>
- GRAJEK SUSAN and the 2015–2016 EDUCAUSE IT Issues Panel. *Top 10 IT Issues-2016 Divest, Reinvest and Differentiate*. [Fecha de consulta: 13/09/2016]. Disponible en <http://er.educause.edu/articles/2016/1/top-10-it-issues-2016>
- *Guía de seguridad de las TIC (CCN-STIC-823) utilización de servicios en la nube MINHAP*. CCN, ENS, 2014. [Fecha de consulta: 13/09/2016]. Disponible en <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Eschema Nacional de Seguridad/823-Seguridad-en-entornos-cloud/823-Cloud Computing ENS.pdf>
- *Guía para clientes que contraten servicios de Cloud Computing*. Agencia Española de Protección de Datos, 2013. [Fecha de consulta: 13/09/2016]. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf
- *ISO/IEC 27005:2011 Information technology. Security techniques Information security risk management*. ISO/IEC JTC 1/SC 27, 2011.
- *ISO/IEC 27018:2014 Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. ISO/IEC JTC 1/SC 27, 2014.
- *ISO/IEC 38500:2015. Information technology. Governance of IT for the organization*. ISO/IEC JTC 1/SC 40, 2015.



- *ITIL® Best Practice. ITIL Service Strategy. ITIL Service Design. ITIL Service Transition. ITIL Service Operation. ITIL Continual Service Improvement. AXELOS, 2011.*
- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* [Fecha de consulta: 13/09/2016]. Disponible en <https://boe.es/buscar/act.php?id=BOE-A-1999-23750>
- PÍRIZ, Segundo (dir.). *UNIVERSITIC 2015. Análisis de las TIC en las Universidades Españolas.* Madrid, CRUE TIC, 2016. ISBN 978-84-6086245-1. [Fecha de consulta: 13/09/2016]. Disponible en <http://tic.crue.org/publicaciones/informe-universitic-2015/>
- *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* [Fecha de consulta: 13/09/2016]. Disponible en <http://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>
- *UNE-EN ISO 22301:2015. Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones.* . AENOR, 2015.
- *UNE-ISO/IEC 20000-1:2011. Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS).* AENOR, 2011.
- *UNE-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.* AENOR, 2014.