RESUMEN EJECUTIVO DE

LA AUDITORÍA COORDINADA SOBRE GOBERNANZA DE TI

OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

BID
Banco Interamericano de Desarrollo

TRIBUNAL DE CUENTAS DE LA UNIÓN TCU

República Federativa de Brasil

Tribunal de Cuentas de la Unión

MINISTROS

Aroldo Cedraz de Oliveira (Presidente)

Raimundo Carreiro (Vicepresidente)

Augusto Nardes

Walton Alencar Rodrigues

Benjamin Zymler

José Múcio Monteiro

Ana Arraes

Bruno Dantas

Vital do Rêgo

MINISTROS SUSTITUTOS

Augusto Sherman Cavalcanti

Marcos Bemquerer Costa

André Luís de Carvalho

Weder de Oliveira

MINISTERIO PÚBLICO ANTE EL TCU

Paulo Soares Bugarin (Procurador General)

Lucas Rocha Furtado (Subprocurador General)

Cristina Machado da Costa e Silva (Subprocuradora General)

Marinus Eduardo de Vries Marsico (Procurador)

Júlio Marcelo de Oliveira (Procurador)

Sérgio Ricardo Costa Caribé (Procurador)

RESUMEN EJECUTIVO DE

LA AUDITORÍA COORDINADA SOBRE GOBERNANZA DE TI

OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

BID
Banco Interamericano de Desarrollo

TRIBUNAL DE CONTAS DA UNIÃO TCU

Brasilia, 2015

<www.tcu.gov.br>

Resumen ejecutivo de la auditoría coordinada sobre gobernanza de TI / Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS); Coordinación Tribunal de Cuentas de la Unión de Brasil; Contraloría General del Estado Plurinacional de Bolivia ... [et al.]. -- Brasilia : Tribunal de Cuentas de la Unión de Brasil, 2015.

20 p.

Este trabajo conjunto contó con la participación de once Entidades Fiscalizadoras Superiores (EFS) de los siguientes países miembros de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS): Bolivia, Brasil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panamá, Paraguay y Perú.

1. Auditoría. 2.Tecnologia de la información. 3. Gobernanza. I. Brasil. Tribunal de Cuentas de la Unión. II. Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS).

Ficha catalográfica por la Biblioteca Ministro Ruben Rosa

Presentación

Estimado lector:

Es con gran satisfacción que presentamos el resultado de la auditoría coordinada por el Tribunal de Cuentas de la Unión (TCU) de Brasil sobre Gobernanza de Tecnología de la Información (TI).

Este tema trata sobre la parte de la gobernanza corporativa que busca asegurar que el uso de la TI agregue valor al negocio, con riesgos aceptables. Con ese objetivo, se busca evitar o mitigar deficiencias aún comunes en la gestión de una institución, tales como procesos de planificación inadecuados, recurrencia de proyectos sin éxito y contrataciones que no alcancen sus objetivos, reflejando una pérdida de calidad y de eficiencia.

Además, es importante destacar que la gobernanza adecuada del área de tecnología de la información en el sector público promueve la protección de informaciones críticas y contribuye a que las instituciones públicas logren sus objetivos institucionales.

Este trabajo conjunto contó con la participación de once Entidades Fiscalizadoras Superiores (EFS) de los siguientes países miembros de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS): Bolivia, Brasil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panamá, Paraguay y Perú.

En esta oportunidad fue posible evaluar, con el apoyo de los miembros de las entidades fiscalizadoras y el esfuerzo de los equipos técnicos involucrados, el nivel de madurez de la gobernanza de TI en instituciones públicas de los países participantes.

Los hallazgos encontrados demuestran el cuadro real sobre el tema en cuestión en instituciones públicas de las EFS participantes y los principales desafíos para la mejora de su grado de madurez.

Para concluir, destaco que las EFS, al promover evaluaciones conjuntas, fomentan el cumplimiento de los acuerdos internacionales y estimulan el perfeccionamiento de la gobernanza de TI, hecho que repercutirá en los servicios prestados por la Administración Pública y traerá beneficios a los países y sus ciudadanos.

¡Espero que tengan una buena lectura!

Ministro Aroldo Cedraz de Oliveira

Índice

1. Introducción

1.1. Se debe priorizar la temática de la gobernanza en el sector público para un esfuerzo de concienciación de la Administración Pública y de la sociedad acerca de los beneficios de adoptar las mejores prácticas internacionalmente reconocidas, que apoyan en el logro de los principales objetivos buscados por las instituciones públicas.

1.2. Los mecanismos de gobernanza involucrados hacen posible que se presten los servicios públicos con mayor efectividad, una vez que pasan a ser guiados por mecanismos que fundamentan la toma de decisión, observando los procesos, funciones, responsabilidades y límites implicados, sin olvidarse de rendir cuentas a la sociedad, bajo el paradigma de la transparencia.

1.3. En ese contexto, la gobernanza de tecnología de la información (TI) tiene lugar especial debido a su relevancia natural y a la creciente dependencia de las instituciones públicas de las nuevas tecnologías desarrolladas y puestas a la disposición de todos.

1.4. Empezando por el uso de equipos de procesamiento de datos, desde el inicio del siglo pasado, el uso de la tecnología de la información ha experimentado una aceleración exponencial, a partir de la década de 1970. Con el desarrollo de las microcomputadoras y su popularización, el mercado y los usuarios de TI han visto pasar una verdadera revolución. La utilización exclusiva de computadoras de gran dimensión *(mainframes)*, ha dado lugar a las redes y a los sistemas del tipo cliente-servidor.

1.5. A partir de la década de 1990, con la apertura de la Internet a todos los usuarios, una segunda revolución se puso en marcha. El uso de la TI ha alcanzado todos los segmentos de la sociedad y han surgido las más diversas aplicaciones que han hecho viables nuevas actividades y negocios. Los sistemas pasaron a ser orientados a la web y a los servicios prestados a los clientes y ciudadanos.

1.6. En la década actual, se puede decir que ocurre la tercera revolución con el uso intensivo de equipos móviles, de conexiones a la Internet de banda ancha y de procesamiento y almacenamiento en la nube. Con ello, los cambios originarios de las nuevas tecnologías ocurren más rápidamente, conllevan consecuencias cada vez más profundas y la competencia en la gestión de TI es factor clave para el éxito en cualquier sector de actividad.

1.7. Actualmente hay una dependencia profunda de la TI, que está revolucionando el modo como la Administración Pública orienta sus negocios. El uso optimizado de la TI es fundamental para que el sector público logre sus objetivos y cumpla su misión institucional.

1.8. Seguramente, los resultados de la Auditoría Coordinada sobre Gobernanza de TI podrán contribuir a la mejoría del grado de madurez en gobernanza de TI de la Administración Pública en los países miembros de la OLACEFS.

2. Antecedentes de la Auditoría Coordinada

2.1. La realización de auditorías coordinadas facilita compartir el conocimiento y la experiencia entre las Entidades Fiscalizadoras Superiores (EFS) en los temas elegidos. La Auditoría Coordinada sobre Gobernanza de TI se encuentra alineada con la meta estratégica 3 (Gestión del Conocimiento) del Plan Estratégico 2011-2015 de la OLACEFS.

2.2. Las EFS involucradas en las auditorías coordinadas pueden compartir los costos derivados del reclutamiento de consultores, de la elaboración de estudios preliminares y de la realización de paneles de referencia y seminarios. Las normas internacionales y las mejores prácticas también pueden ser divulgadas de forma más eficaz para cada auditor, por medio de la estrategia de auditoría coordinada. Además, la existencia de normas internacionalmente aceptadas sobre gobernanza de TI facilita compartir e intercambiar experiencias entre los equipos de auditoría de los diferentes países.

2.3. Con base en las experiencias exitosas de la Iniciativa para el Desarrollo de la Intosai (IDI), la OLACEFS está consolidando esta estrategia centrada en la capacitación, por medio de la adquisición de conocimientos y las competencias en cada etapa de las auditorías coordinadas.

2.4. La Auditoría Coordinada sobre Gobernanza de TI fue antecedida por otros tres trabajos que han utilizado la misma estrategia: Auditoría Coordinada en Hidrocarburos, Auditoría Coordinada sobre Recursos Hídricos y Auditoría Coordinada de Gestión de Áreas Protegidas (Biodiversidad).

3. Objetivo

3.1. La auditoría coordinada tiene como objetivo evaluar la situación de la gobernanza de la tecnología de la información (TI) en los países miembros

de la OLACEFS, a partir de las auditorías realizadas en instituciones representativas de diversos segmentos de la Administración Pública de cada país participante.

3.2. Este trabajo busca obtener informaciones que permitan la elaboración de estrategias para elevar el nivel de madurez de gobernanza de TI y la diseminación de los conocimientos y técnicas utilizadas en los trabajos de campo realizados. Durante la planificación de las auditorías se han previstos los siguientes resultados:

- La inducción de mejoras en la estructura y en los mecanismos de gobernanza de TI de las instituciones públicas de los países involucrados, cuyos progresos serán obtenidos a partir de las recomendaciones dirigir a las instituciones evaluadas en las auditorías.

- Identificación de las áreas que presentan debilidades y que puedan ser el blanco de acciones coordinadas en el ámbito de la OLACEFS con el objetivo de perfeccionamiento por medio de cooperación, intercambio de experiencias, identificación de buenas prácticas y capacitación.

- Diseminación de conocimientos y de las mejores prácticas de gobernanza de TI para la Administración Pública en el área de actuación de la OLACEFS.

4. Método utilizado

4.1. Para aumentar las posibilidades de éxito de la auditoría se han desarrollado diversas actividades preparatorias.

4.2. Entre febrero y mayo de 2014 se capacitaron, por medio de un curso a distancia, 43 auditores de 15 EFS participantes de la auditoría.

4.3. Los días 21 y 22 de julio de 2014 se realizó el Seminario Internacional de Auditoría sobre Gobernanza de TI en Brasilia, Brasil. Hubo 10 ponencias que trataban tres grandes tópicos: Gobernanza y Gestión de TI Seguridad de la Información y Planificación de TI. Además de los auditores brasileños, el evento contó con la participación de 21 auditores de las otras 10 EFS participantes en la auditoría coordinada, que pudieron discutir tópicos relacionados a la auditoría y conocer casos de éxito en la implantación de procesos de gobernanza de TI en entidades públicas brasileñas.

4.4. Los tres días siguientes se realizó una reunión técnica para definir la matriz de planificación para la realización de la auditoría. Con el propósito de definir las áreas de la gobernanza de TI a ser auditadas y organizar la ejecución de los trabajos, se eligieron cuatro grandes áreas de enfoque en los trabajos de campo: Estructura de Gobernanza de TI, Planificación de TI, Contratación de TI y Seguridad de la Información. La matriz de planificación contó con las siguientes preguntas de auditoría:

P1. ¿Los mecanismos y estructuras de gobernanza de TI han sido definidos e implementados adecuadamente en el ámbito de la institución?
P2. ¿Hay un proceso de planificación de TI?
P3. ¿Hay un proceso para adquisición de soluciones de TI?
P4. ¿Se realiza la gestión de la seguridad de la información?

4.5. Se definió la participación de 11 países en la auditoría: Bolivia, Brasil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panamá, Paraguay y Perú.

4.6. Desde agosto de 2014 se realizaron 41 auditorías en 11 diferentes países utilizando la misma matriz de planificación. Durante la ejecución de las auditorías se intercambiaron informaciones acerca del desarrollo del trabajo, por medio de correo electrónico y videoconferencias.

4.7. El periodo del 24 al 26 de marzo de 2015, en San José, Costa Rica, se realizó una reunión para consolidar los hallazgos de las auditorías realizadas en los países participantes y definir el contenido de este informe consolidado de la Auditoría Coordinada sobre Gobernanza de TI.

4.8. La definición de los tópicos evaluados y de los criterios de auditoría utilizados se fundamentó en la legislación de cada país, sus normas técnicas internacionales y en los modelos de buenas prácticas reconocidos internacionalmente.

4.9. Como criterio de auditoría, además de la legislación aplicable de cada país, se adoptaron los controles previstos en la norma ISO/IEC 27002:2013, código de buenas prácticas para gestión de la seguridad de la información; en la norma ISO/IEC 27005:2008, que trata de gestión de riesgos de seguridad de la información; en la norma ISO/IEC 38500:2008 y en el Cobit 5 de la Isaca, que proveen modelos de buenas prácticas para gobernanza de la tecnología de la información.

5. Gobernanza de TI

5.1. La gobernanza de TI es la parte de la gobernanza corporativa que busca asegurar que el uso de la TI agregue valor al negocio con riesgos aceptables. Con ese objetivo, la gobernanza de TI busca evitar o mitigar deficiencias en la gestión de una institución, tales como procesos de planificación inadecuados, presencia de proyectos de TI sin resultados y contrataciones de TI que no logran sus objetivos, reflejando en pérdida de calidad y eficiencia.

5.2. En la práctica, la gobernanza de TI se traduce en un conjunto de políticas, procesos, roles y responsabilidades asociados a estructuras y personas de la organización, de modo que se establezca claramente el proceso de toma de decisión y las directrices para la gestión y el uso de la TI, alineados con la visión, misión y metas estratégicas de la organización.

5.3. La norma ISO/IEC 38500, en el ítem 1.6.3, define gobernanza de TI como "*El Sistema por el que el uso actual y futuro de la TI es dirigido y controlado.*"

5.4. En complemento a este concepto el *IT Governance Institute* (ITGI), especifica que "*Gobernanza de TI es una estructura de relaciones y procesos para dirigir y controlar la TI a fin de lograr las metas de la institución por la agregación de valor, mientras se mantiene el equilibrio de los riesgos versus retorno sobre esta función y sus procesos.*"

5.5. El objetivo de la gobernanza de TI es asegurar que las acciones de TI estén alineadas con el negocio de la organización, agregándole valor. El rendimiento del área de TI debe ser medido, los recursos deben ser propiamente asignados y los riesgos inherentes deben ser mitigados. De este modo, es posible gestionar y controlar las iniciativas de TI en las instituciones para garantizar el retorno de inversiones y la adopción de mejorías en los procesos organizacionales.

5.6. La gobernanza adecuada del área de tecnología de la información en el sector público promueve la protección de informaciones críticas y contribuye para que las instituciones públicas logren sus objetivos institucionales. Además, garantizar la correcta aplicación de los recursos empleados en tecnología de la información se hace cada vez más importante, teniendo en cuenta la gran dependencia de la Administración Pública con relación a la TI.

6. Hallazgos clave

6.1. En relación a los mecanismos y estructuras de la gobernanza de TI, los dos principales hallazgos encontrados fueron la existencia de deficiencias en los mecanismos de gobernanza de TI y la inexistencia de un comité de TI.

Mecanismos y estructuras de gobernanza de TI

6.2. Se observó en prácticamente la mitad de las instituciones auditadas (un 46%) la existencia de mecanismos y estructuras de gobernanza de TI que no actuaban adecuadamente.

6.3. Muchas instituciones no poseen un proceso o plan de gestión de riesgos de TI aprobado formalmente y no evalúan el cumplimiento de las metas de TI planificadas, mecanismos fundamentales para dirigir y evaluar la gestión y el uso corporativos de TI.

6.4. Diversas entidades no disponen de un proceso de perfeccionamiento continuo de la gobernanza de TI. No fueron identificadas acciones con el objetivo de diagnosticar el nivel de madurez en gobernanza de TI, ni tampoco la definición de metas de gobernanza para los próximos ejercicios. Otra deficiencia observada, muy común, fue la ausencia de una estructura de personal formalmente asignado para la mejora de la gobernanza de TI.

6.5. En otras instituciones, a pesar de haber un Plan Director de TI (PDTI) aprobado, no se formalizó un sistema integrado de objetivos relacionados a la mejora de la gobernanza de TI, indicadores de rendimiento para cada objetivo, metas para cada indicador y mecanismos de monitoreo regular de esos indicadores. No se definieron y formalizaron en el PDTI metas de gobernanza de TI con base en parámetros de gobernanza, necesidades de negocio y riesgos relevantes, ni indicadores para el monitoreo y la evaluación del cumplimiento de esas metas.

6.6. Gran parte de las instituciones no está desarrollando acciones que busquen perfeccionar su nivel de gobernanza en TI. Tal inercia puede comprometer la necesaria evolución del nivel de madurez de la gobernanza de TI, así como, en un último análisis, puede perjudicar el logro de los objetivos de TI. De esa manera, se entiende como una oportuna recomendación que las instituciones elaboren y aprueben formalmente proceso de perfeccionamiento continuo de la gobernanza de TI, a ejemplo de las buenas prácticas presentes en el capítulo 3 de la guía de referencia de la implementación del Cobit 5, que contemple,

al menos, la definición de roles y responsabilidades dirigidas específicamente para la mejoría de la gobernanza de TI; realización de diagnósticos o autoevaluaciones de gobernanza y de gestión de TI; y definición y seguimiento de metas de gobernanza de TI y de las acciones necesarias para lograrlas, con base en parámetros de gobernanza, necesidades de negocio y riesgos relevantes.

6.7. Otro aspecto esencial para la gobernanza de TI es la existencia de un comité de TI, que determine las prioridades de inversión y la asignación de recursos en los diversos proyectos y acciones de TI. Además, es de fundamental importancia para la alineación entre las actividades de TI y el negocio de la organización, así como para la optimización de los recursos disponibles. El hecho de que este comité se encuentre compuesto por representantes del área de TI y de otras áreas de la organización hace posible que las decisiones de inversiones se obtengan a partir de una visión organizacional más abarcadora, lo que reduce los riesgos de gastos innecesarios o no beneficiosos para la organización.

6.8. Se verificó que en un 44% de las instituciones auditadas no había un comité de TI constituido con las atribuciones preconizadas en el Cobit 5. Cabe señalar que en Brasil donde la existencia de un comité es obligatoria, debido a normativas reglamentarias, había un comité en la totalidad de las ocho instituciones auditadas.

6.9. El hecho de que en aproximadamente menos de la mitad de las instituciones auditadas no exista un comité de TI funcionando indica que todavía no está consolidada la importancia de la participación de todos los sectores de la organización en las decisiones estratégicas de TI. La existencia del comité de TI, aliada a las planificaciones estratégicas institucionales y de TI, constituye un instrumento valioso en la orientación de las inversiones de TI, en el aumento del éxito de los proyectos de TI y en la disminución del riesgo de despilfarro de recursos.

6.10. Se puede destacar también que la existencia de una norma que obligue la constitución de un comité de TI en el ámbito de las instituciones favorece su adhesión a las buenas prácticas internacionales de gobernanza de TI.

Proceso de planificación de TI

6.11. Tres hallazgos se destacan en la cuestión del Proceso de Planificación de TI: la inexistencia de este proceso en muchas instituciones, la inexistencia de documentos de planificación estratégica y la ausencia de monitoreo de la planificación de TI por la alta administración.

6.12. Un porcentaje significativo de las instituciones auditadas (un 39%) no tiene un proceso de planificación de TI vigente. Ello significa que esas instituciones aunque posean eventualmente algún plan de TI, no tienen la cultura de planificar estratégicamente sus acciones y, en la mayoría de las situaciones, sólo reaccionan a las demandas y a los cambios que ocurren en su ámbito de actuación, dificultando la planificación de las acciones de TI.

6.13. La incorporación del proceso de planificación de TI minimiza la posibilidad de la asignación inadecuada de sus recursos. Además, ese proceso no permite que la organización sea dependiente de personas específicas. Asimismo, aunque ocurra la desvinculación de una cantidad significativa de profesionales, el área de TI podrá seguir la dirección planificada, concluir los proyectos en curso y seguir funcionando adecuadamente.

6.14. Solamente la implantación del proceso de planificación de TI permitirá a las instituciones públicas el uso más eficiente de los recursos de TI. La inexistencia de ese proceso en una parte significativa de las instituciones públicas requiere la actuación de las EFS en el sentido de concientizar a la alta administración y a los gestores de TI en la importancia de la planificación de TI.

6.15. Asimismo, la mayor parte de las instituciones que poseen un proceso de planificación de TI no producen documentos de planificación estratégica de TI.

6.16. Casi dos tercios (un 63%) de las instituciones auditadas no realizan planificación estratégica de TI. Se debe destacar, una vez más, la importancia de la planificación estratégica para la gobernanza de TI. Dado que para que la planificación estratégica de TI sea efectiva y proporcione los resultados esperados, la misma debe estar alineada a la planificación estratégica institucional. Por ello, su falta impide la alineación deseada y dificulta el establecimiento de directrices para el área de TI.

6.17. Evidentemente, no se debe confundir el hecho de no haber planificación estratégica con el hecho de no haber ninguna planificación. Los organismos y/o entidades pueden poseer algún tipo de planificación, normalmente un plan de acción anual. A pesar de necesarios, los planes de acción anuales son insuficientes porque no consiguen indicar caminos y estrategias, solo prevén cómo se asignarán los recursos disponibles en aquel año. Además, esos planes no son buenos instrumentos para seguir y apoyar los proyectos de mediana y larga duración, comunes en el área de TI. Otro problema que se observa normalmente se da cuando, debido a la ausencia de una planificación estratégica, se descontinúan esos proyectos, lo que conlleva a la utilización innecesaria de recursos.

6.18. La planificación estratégica de TI debe indicar los proyectos y servicios de TI que recibirán recursos, además de los costos, de las fuentes de recursos y de las metas a lograr. Debe ser una actividad regular y los documentos resultantes deben ser aprobados por la alta administración.

6.19. La planificación estratégica de TI debe posibilitar la definición, en cooperación con los principales interesados, de la forma con la que las metas de TI contribuirán al logro de los objetivos estratégicos de la organización, considerando los costos y riesgos asociados. El documento resultante de esa planificación debe incluir los servicios de TI, sus activos y la forma en la cual el área le dará soporte a los proyectos dependientes de tecnología de la información. El área de TI debe definir cómo se lograrán los objetivos, las métricas a utilizar y los procedimientos para obtener la aprobación formal de los interesados. El plan estratégico de TI debe contener el presupuesto para las inversiones y el mantenimiento de TI, las fuentes de recursos, la estrategia de adquisiciones, y los requisitos legales y regulatorios. El plan estratégico debe estar suficientemente detallado para permitir su desglose en planes tácticos de TI.

6.20. Es fundamental la diseminación de la cultura de la planificación estratégica en las instituciones públicas; las EFS deben exigir sus resultados.

6.21. Otro punto que merece atención es la ausencia de monitoreo de la planificación de TI por la alta administración.

6.22. En casi un tercio de las instituciones auditadas (un 29%) se constató que la alta administración no monitorea la ejecución de los planes de TI. En algunos casos, a pesar de la existencia de los planes, la organización no definió formalmente los mecanismos de control del cumplimiento de metas de gestión y de uso corporativos de TI. En otras situaciones, a pesar que el PETI contiene la definición de metas, no constan informaciones acerca de cómo se miden y se controlan esas metas.

6.23. En otras situaciones, no se establecieron formalmente objetivos de gestión y de uso corporativo de TI, tampoco indicadores de rendimiento y metas asociadas a aquellos. La alta administración no sigue los indicadores de resultados estratégicos de los principales sistemas de información. Además, no hay mecanismos de control del cumplimiento de las metas de gestión y de uso corporativos de TI, tampoco mecanismos de gestión de los riesgos relacionados a esos objetivos, así como no se aprobaron planes de auditoría interna para evaluar los riesgos considerados críticos para el negocio y la eficacia de los respectivos controles.

6.24. Las EFS deben recomendar a las instituciones que audita que sean establecidos, formalmente, mecanismos para que la alta administración siga el rendimiento de la TI y mecanismos de gestión de los riesgos relacionados a los objetivos de gestión y de uso corporativos de TI.

6.25. Además, se debe elaborar un plan anual de auditoría interna de la organización que contenga, entre otras actividades, acciones con el objetivo de evaluar los riesgos para el negocio y la eficacia de los respectivos controles con relación a la gestión y al uso de la TI corporativa.

Proceso para adquisición de soluciones de TI

6.26. Se observó la formalización del proceso de adquisición de soluciones de TI en la mayoría de las instituciones auditadas. Sin embargo, fue verificado que este proceso y el proceso subsecuente de la gestión de los contratos de TI no son monitoreados.

6.27. Además de la implantación del proceso de contratación de TI, es necesario el constante monitoreo de los resultados logrados para perfeccionar el proceso en sí y, también, minimizar las desviaciones y despilfarros. En un 39% de las instituciones auditadas no se realiza dicho monitoreo.

6.28. Se debe controlar la asignación y optimización de los recursos de acuerdo con los objetivos y las prioridades establecidas usando las metas y métricas acordadas. Enseguida, monitorear el rendimiento de los recursos en comparación con las metas, analizar la causa de eventuales desviaciones e iniciar medidas correctivas para solucionar las causas subyacentes.

6.29. Los objetivos del monitoreo constante del proceso de contratación son el perfeccionamiento del proceso; reforzamiento de la alineación entre el área de TI y las áreas de negocio; asignación eficiente de recursos y optimización de los recursos de TI de la organización.

6.30. En un 29% de las instituciones auditadas no se realiza el monitoreo del proceso de gestión de los contratos de TI. De la misma manera que es importante la existencia de un proceso de trabajo formalizado para contrataciones de TI, es esencial que los contratos originados de esas adquisiciones sean bien administrados y su proceso de gestión sea monitoreado.

6.31. Además del perfeccionamiento del proceso de gestión de contratos de TI, este monitoreo permitirá la verificación de los resultados logrados en cada contratación a partir de métricas preestablecidas.

6.32. Los objetivos del monitoreo constante del proceso de gestión de contratos son: el perfeccionamiento del proceso; la garantía de la atención de los recursos de TI necesarios para las diversas áreas de negocio; la asignación eficiente de recursos y la optimización de los recursos de TI de la organización.

Gestión de la seguridad de la información

6.33. Tradicionalmente, el área de la seguridad de la información presenta muchas deficiencias. En este trabajo deben ser destacados seis hallazgos: la ausencia de aprobación de la Política de Seguridad de la Información (PSI), la ausencia de designación formal de responsables para gestionar la seguridad de la información, la ausencia de la Política de Control de Acceso (PCA), la ausencia de un proceso de gestión de los riesgos de la seguridad de la información, la ausencia de un proceso de gestión de la continuidad de los servicios de TI y la ausencia del Plan de Continuidad de Negocios (PCN).

6.34. Se constató que, en un 46% de las instituciones auditadas, no se aprobó ni publicó la Política de Seguridad de la Información (PSI).

6.35. La PSI corresponde al documento que contiene las directrices de la organización en relación con el tratamiento de la seguridad de la información. De acuerdo con las orientaciones de la norma ISO/IEC 27002:2013, la política debe declarar explícitamente el compromiso de la alta administración con la seguridad de la información. Además, también debe contener definiciones de los términos relacionados dentro del ámbito de la organización y asignar los objetivos de control, sus controles, las estructuras que implementan esos controles, las responsabilidades y las políticas junto a las normas que regulan y complementan este documento, incluyendo referencias a la legislación y a los requisitos reglamentarios y contractuales. En general, este es el documento a partir del cual se derivan los más específicos para cada actividad de la gestión de la seguridad de la información.

6.36. Es fundamental que la alta administración establezca una política clara, alineada con los objetivos del negocio y demuestre apoyo y compromiso con la seguridad de la información por medio de la publicación y mantenimiento de la PSI para toda la organización.

6.37. Para implementar la PSI es esencial la designación formal de responsables por la gestión de la seguridad de la información.

6.38. En un 51% de las instituciones auditadas no había responsables, unidades o personas, designados para ejecutar la gestión de la seguridad de la infor-

mación. Debido a la grande y variada gama de actividades relacionadas a la gestión de la seguridad de la información, se hace imperiosa la designación formal de personas o unidades para desempeñar esas tareas.

6.39. Cada organización debe designar formalmente un responsable (unidad o persona) de la gestión de la seguridad de la información en su ámbito de actuación, de forma similar a las orientaciones presentes en el ítem 6.1.1 de la norma ISO/IEC 27002:2013.

6.40. Otro documento de gran importancia para la gestión adecuada de la seguridad de la información es la Política de Control de Acceso (PCA).

6.41. Se constató que en un 44% de las instituciones auditadas, no hay un documento formalmente aprobado y publicado que haya instituido una política de control de acceso a la información. La PCA debe ser establecida, documentada y analizada críticamente, basada en los requisitos de seguridad de la información y de los negocios.

6.42. Las reglas de control de acceso y derechos para cada usuario o grupos de usuarios deben estar contenidas expresamente en la PCA, considerando los controles de acceso lógico y físico de forma conjunta, de acuerdo con los requisitos de negocio a ser atendidos.

6.43. Las EFS deben recomendar a las instituciones que auditan a elaborar y aprobar formalmente una política de control de acceso a informaciones y recursos de TI, con base en los requisitos de negocio y de seguridad de la información de la organización, de forma similar a las orientaciones presentes en la sección 9.1.1 de la norma ISO/IEC 27002:2013.

6.44. Sumado a la situación crítica encontrada en una parte significativa de las instituciones auditadas, se constató que un 49% no posee un proceso de gestión de riesgos de seguridad de la información. Dicho proceso de gestión de riesgos de seguridad de la información comprende el análisis y/o la evaluación de riesgos, el tratamiento de este riesgo, la aceptación del riesgo, la comunicación del riesgo junto al monitoreo y al análisis crítico de los riesgos de seguridad de la información.

6.45. Las EFS deben recomendar a las instituciones que auditan que definan e implementen un proceso de gestión de riesgos de seguridad de la información, de forma similar a las orientaciones presentes en la norma ISO/IEC 27005:2008.

6.46. Otro aspecto en negligencia en una parte significativa de las instituciones auditadas es la gestión de la continuidad de los servicios de TI. Se constató que en un 54% de las instituciones auditadas no se implementó un proceso de gestión de continuidad de servicios de TI. El proceso de gestión de continuidad de los servicios de TI busca proteger los servicios de TI no permitiendo la interrupción de las actividades de la organización y haciendo posible que las informaciones más críticas estén disponibles de acuerdo con el nivel de servicio requerido.

6.47. Las EFS deben recomendar a las instituciones que auditan, elaborar y ejecutar un proceso de gestión de continuidad de los servicios de TI, de forma similar a las orientaciones presentes en el proceso DSS04 – Gestionar Continuidad del Cobit 5.

6.48. Como consecuencia casi directa de la ausencia del proceso de gestión de la continuidad de los servicios de TI, se detectó que la mayoría (un 59%) de las instituciones auditadas no posee un Plan de Continuidad de Negocios (PCN) aprobado y publicado. El objetivo del PCN es no permitir la interrupción de las actividades del negocio y proteger los procesos críticos contra fallas o desastres significativos, asegurando su retorno en un tiempo definido.

6.49. Las EFS deben recomendar a las instituciones que auditan, elaborar e implantar el Plan de Continuidad de Negocios, de forma similar a las orientaciones presentes en el proceso DSS04 – Gestionar Continuidad del Cobit 5.

7. Conclusión y desafíos

7.1. El principal objetivo de esta auditoría coordinada ha consistido en la evaluación de la situación de gobernanza de tecnología de la información en los países miembros de la OLACEFS, a partir de auditorías ejecutadas en las instituciones representativas de diversos segmentos de la Administración Pública de cada país. Se efectuaron un total de 41 auditorías en instituciones públicas de los 11 diferentes países participantes utilizando la misma matriz de planificación.

7.2. Con la finalidad de definir las áreas de la gobernanza de TI a ser auditadas y organizar la ejecución de los trabajos, se eligieron cuatro grandes áreas para el enfoque a nivel de auditoría de campo: Estructura de Gobernanza de TI, Planificación de TI, Contratación de TI y Seguridad de la Información.

7.3. Sobre las estructuras de gobernanza de TI, se observó que a pesar de que existen los mecanismos y las estructuras implementados en casi dos tercios (un 66%) de las instituciones auditadas, todavía existen muchas deficiencias. De las instituciones auditadas, en un 46% los mecanismos se presentaban fallas, en un 44% no existía un comité de TI y un 7% de los participantes del comité no poseía el perfil adecuado al rendimiento de las actividades. Del análisis de estas tendencias, se concluye que existen problemas en la mayoría de las instituciones, lo cual exige un perfeccionamiento de las estructuras de gobernanza de TI.

7.4. En lo que se refiere a la planificación de TI, se verificó que un 39% de las instituciones no posee un proceso implantado de planificación de TI, y que en casi 2/3 no se producen documentos de planificación estratégica de TI. Se debe destacar que la ausencia de planes estratégicos deja a las instituciones sin instrumentos para seguir y apoyar los proyectos de mediana y larga duración, comunes en el área de TI, lo que provoca la discontinuidad de esos proyectos y el consecuente despilfarro de recursos.

7.5. De las cuatro áreas analizadas, la contratación de TI es la que se encuentra más organizada y con menos deficiencias formales. Esta constatación, sin embargo, no significa que las contrataciones estén siendo realizadas de manera eficiente y efectiva. Se advirtió que en prácticamente un tercio de las organizaciones (un 34%) no existe un proceso de trabajo implementado para realizar las contrataciones de TI. Asimismo, en un 39% de las instituciones evaluadas el proceso implantado de contratación de TI no es monitoreado. A su vez, el proceso de gestión de contratos de TI no es seguido en un 29% de las instituciones. Se observó que todavía es necesario un mayor control sobre las contrataciones de TI.

7.6. En lo que se refiere a la seguridad de la información, se detectó la peor puntuación de las cuatro áreas de enfoque del presente trabajo, ya que han sido 13 diferentes hallazgos y algunos con números significativos de apariciones. Entre estos, se destacan la inexistencia de un plan de continuidad de negocios, totalizando un 59%, la ausencia de proceso de continuidad de servicios de TI con un 54% y la ausencia de la designación de responsables (área o personas) de la gestión de seguridad de la información en un 51%. Lo más significativo es que dos de los procesos básicos de la seguridad de la información, gestión de la seguridad de la información y gestión de la continuidad, todavía no han sido implantados en más de la mitad de las instituciones auditadas. Además, documentos y procesos esenciales tampoco han sido implantados o elaborados en casi mitad de las instituciones auditadas,

lo que refuerza aún más la necesidad de darle atención a la seguridad de la información. Se verificó la ausencia de un proceso de gestión de riesgos en un 49% de las entidades auditadas, de un proceso de inventario de activos en un 46%, de un comité de seguridad de la información en un 46%, de Política de Seguridad de la Información en un 46% y de Política de Control de Acceso, totalizando un 44% del total de instituciones evaluadas.

7.7. Ante el escenario presentado, se advierte que la situación de la gobernanza de TI en las instituciones públicas de los países miembros de la OLACEFS es bastante heterogénea en diversos aspectos. Por ejemplo, el tema contratación de TI, además de las diferencias naturales entre los diversos países participantes de la auditoría, se presenta, de alguna forma, reglamentado por normas necesarias, lo que, por un lado, representa algún desarrollo, a pesar de estar lejos de lo ideal. Del mismo modo, están los aspectos que tienen las buenas prácticas como referencia principal, a saber: estructuras de gobernanza de TI, planificación de TI y seguridad de la información. Esos exigen más atención. El aspecto en el que la situación de la gobernanza de TI está más crítica es la seguridad de la información.

7.8. En ese punto, el mayor desafío para las EFS es concientizar a las instituciones auditadas sobre la importancia de la gobernanza de TI y los beneficios que podrán obtener con la mejora en su grado de madurez. Se hace muy importante e, incluso, urgente la inversión de recursos para la implantación o perfeccionamiento del comité de TI (un 44%); del proceso de planificación de TI (un 39%); de la planificación estratégica de TI (un 63%); del monitoreo sobre el proceso de contratación de TI (un 39%); del plano de continuidad de negocios (un 59%); del proceso de continuidad de servicios de TI (un 54%); de la designación de responsables (área o personas) de la gestión de seguridad de la información (un 51%); del proceso de gestión de riesgos (un 49%); del proceso de inventario de activos (un 46%); del comité de seguridad de la información (un 46%); de la Política de Seguridad de la Información (46%) y de la Política de Control de Acceso (un 44%).

7.9. Para finalizar, se observó que las EFS pueden y deben actuar como inductores del proceso de perfeccionamiento de la gobernanza de TI, dado que existe un enorme campo para su actuación en la gobernanza de TI de la Administración Pública de los países miembros de la OLACEFS. Es por ello que, si esa actuación se realiza de forma consistente y permanente, los resultados serán prometedores, teniendo en cuenta que podrá haber mejoras generalizadas en todos sus aspectos. Hecho que repercutirá en los servicios prestados por la Administración Pública y conllevará beneficios a los países y sus ciudadanos.

8. Referencias

8.1. Norma ISO/IEC 27002:2013, Código de buenas prácticas para la gestión de la seguridad de la información;

8.2. Norma ISO/IEC 27005:2008, Gestión de riesgos de seguridad de la información;

8.3. Norma ISO/IEC 38500:2008, Gobernanza corporativa de tecnología de la información; y

8.4. Cobit 5, Modelo corporativo para gobernanza y gestión de TI de la organización.

9. Participantes

9.1. La organización de los trabajos ha sido realizada por auditores del TCU de Brasil. Las 41 auditorías han sido realizadas por 52 auditores de las once diferentes Entidades Fiscalizadoras Superiores:

- Contraloría General del Estado Plurinacional de Bolivia;
- Tribunal de Cuentas de la Unión de Brasil;
- Contraloría General de la República de Chile;
- Contraloría General de la República de Costa Rica;
- Contraloría General del Estado de la República del Ecuador;
- Corte de Cuentas de la República de El Salvador;
- Contraloría General de Cuentas de la República de Guatemala;
- Tribunal Superior de Cuentas de la República de Honduras;
- Contraloría General de la República de Panamá;
- Contraloría General de la República de Paraguay;
- Contraloría General de la República de Perú.

10. Agradecimientos

10.1. A la Secretaría de Relaciones Internacionales del TCU por todo el apoyo, profesionalismo y calidad de las actividades desarrolladas a lo largo del proceso.

10.2. Al Área de Asuntos Internacionales de la Contraloría General de la República de Costa Rica por su generosa acogida con motivo del taller realizado en San José el mes de marzo de 2015.

10.3. A las Áreas Internacionales de las demás EFS que han apoyado las actividades de esta auditoría coordinada de TI.

Responsable por el contenido
Secretaría de Relaciones Internacionales (Serint) del TCU

Responsable Editorial
Secretaría General de la Presidencia (Segepres) del TCU
Secretaría de Comunicación (Secom) del TCU
Núcleo de Creación y Edición (NCE) del TCU

Proyecto Gráfico, Diagramación y Portada
Núcleo de Creación y Edición (NCE) del TCU

TRIBUNAL DE CUENTAS DE LA UNIÓN
Secretaría de Relaciones Internacionales (Serint)
SAFS Qd 4 Lote 1 - Anexo III Sala 110
70042900 Brasília - DF
Tel.: (61) 61- 3316-7626
serint.sa@tcu.gov.br

Reclamos, sugerencias y elogios
Teléfono.: 0800 644 1500
ouvidoria@tcu.gov.br
Impreso por Sesap/Segedam

Misión
Mejorar la Administración Pública en beneficio de la sociedad por medio del control externo.

Visión
Ser referencia en la promoción de una Administración Pública efectiva, ética, ágil y responsable.