INFORME DE LA AUDITORÍA COORDINADA SOBRE GOBERNANZA DE TI

Sumario

1. Introducción

1.1. La temática de la gobernanza en el sector público debe ser priorizada en un esfuerzo de concienciación de la Administración Pública y de la sociedad acerca de las mejores prácticas internacionalmente reconocidas, que auxilian en el logro de los principales objetivos buscados por las organizaciones públicas.

1.2. Los mecanismos involucrados posibilitan 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 establecidos, 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 un lugar especial debido a su relevancia natural y a la creciente dependencia de las organizaciones públicas de las nuevas tecnologías desarrolladas y puestas a la disposición.

1.4. Empezando por el uso de equipos de procesamiento de datos desde el inicio del siglo pasado la incorporación de la tecnología de la información ha experimentado una aceleración exponencial a partir de la década de 1970. Con el desarrollo de los microcomputadores y su popularización, el mercado y los usuarios de TI han visto pasar una verdadera revolución. La utilización exclusiva de computadores de gran dimensión, o *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 las TI alcanzó a todos los segmentos de la sociedad y surgieron 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 a los ciudadanos.

1.6. En la década actual, ocurre la tercera revolución con el uso intensivo de equipos móviles, de conexiones a la Internet de banda ancha y de procesamiento, junto con el almacenamiento en la nube. Con todo esto, los cambios originarios por las nuevas tecnologías conllevan a consecuencias cada vez más profundas y a la competencia en la gestión de TI, el cual es el factor clave para el éxito en cualquier sector.

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

1.8. Seguramente, los resultados de esta auditoría podrán contribuir en un avance del grado de madurez en la 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 EFS en los temas elegidos. La Auditoría Coordinada sobre Gobernanza de TI, se encuentra alineada con la meta estratégica 3, relativa a la Gestión del Conocimiento, del Plan Estratégico 2011-2015, de la Olacefs.

2.2. Las EFS involucradas en esta iniciativa pueden compartir los costes 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 tres otros trabajos que han utilizado la misma modalidad: 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 las instituciones más representativas de los diversos segmentos de la Administración Pública de cada país participante.

3.2. Este trabajo busca obtener informaciones que permitan la elaboración de una estrategia de perfeccionamiento de la madurez de la 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:

a) La inducción de mejorías 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 direccionadas a las instituciones evaluadas en las auditorías;
b) 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;
c) 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 los meses de 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. Durante los días 21 y 22 de julio de 2014, se realizó el Seminario Internacional de Auditoría de Gobernanza de TI en Brasilia, Brasil, con 10 ponencias sobre 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 de 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 la definición de la matriz de planificación para 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 para enfocar 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 cuestiones de auditoría:

Q1. ¿Los mecanismos y estructuras de gobernanza de TI han sido definidos e implementados adecuadamente en el ámbito de la institución?

Q2. ¿Hay un proceso de planificación de TI?

Q3. ¿Hay un proceso para adquisición de soluciones de TI?

Q4. ¿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 período 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 de 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 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 corporativa que busca asegurar que el uso de la TI agregue valor al negocio con riesgos aceptables. Con ese objetivo, la gobernanza de TI intenta evitar o mitigar deficiencias en la gestión de una institución 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 a establecerse 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 su 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 el 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 propiamente asignados y los riesgos inherentes mitigados. Así, es posible gestionar y controlar las iniciativas de TI en las organizaciones para garantizar el retorno de inversiones y la adopción de mejorías en los procesos organizacionales.

5.6. La gobernanza del área de tecnología de la información en el sector público promueve la protección a datos críticos y contribuye para que las organizaciones públicas logren sus objetivos institucionales. Además, garantiza la correcta aplicación de los recursos empleados en tecnología de la información, teniendo en cuenta la gran dependencia de la Administración Pública con relación a la TI.

6. Hallazgos Estándar

6.1. De la elaboración de la matriz de planificación se identificaron 35 posibles hallazgos para las cuatro cuestiones de auditoría propuestas. A continuación, se describirán los hallazgos verificados en las auditorías ejecutadas.

6.2. Se debe observar que todos los hallazgos serán tratados de forma agregada, sin contener informaciones específicas de cada entidad auditada. Las informaciones específicas están presentes en el informe de cada auditoría y estarán disponibles de acuerdo con las normas de cada EFS y el respectivo país.

Hallazgo 1.1 – Inexistencia de mecanismos de Gobernanza de TI

6.3. En un 34% de las organizaciones auditadas se observó que no había mecanismos que posibilitaran la gobernanza de TI. Fue verificado que no contaban con ninguna política para gobernanza, gestión y uso de los recursos de TI; no estaban definidas las responsabilidades de cada sector o función del área de TI; no había comité de TI, asunto que se encuentra detallado en el hallazgo 1.3; y no había otras estructuras que permitieran la gobernanza de TI.

6.4. No poseían gobernanza de TI sin el establecimiento de estructuras y de mecanismos esenciales tales como políticas, controles, definición de responsabilidades, procedimientos y estructuras organizacionales para el área de TI.

Criterios

a) Cobit 5 – *Framework*, Capítulo 7 – Guía de Implementación;

b) Cobit 5 – Implementación, Guía de Referencia, Capítulo 3 – Adoptando los primeros pasos hacia la gobernanza de TI;

c) Cobit 5, proceso EDM01 – Garantizar la Definición y Mantenimiento del Modelo de Gobernanza, práctica de gestión EDM01.02 – Dirigir el sistema de gobernanza, actividades 2 y 3;

d) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI.

Causas

6.5. Básicamente, en muchos países no hay normas legales o reglamentarias que hagan obligatoria la implementación de mecanismos y estructuras esenciales para la gobernanza de TI, o que establezcan metas que las organizaciones públicas deban cumplir.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) No siempre los objetivos de las áreas de TI se encuentran alineados a los objetivos institucionales;

b) No se hace un uso óptimo de los recursos de TI;

c) No hay condiciones para medir el rendimiento de las áreas de TI;

d) Aumento del riesgo de fracaso de los proyectos de TI;

e) Despilfarro de recursos públicos.

Conclusión

6.6. En un tercio de las organizaciones auditadas se detectó la ausencia de condiciones básicas para la implantación de gobernanza de TI. Este hecho demuestra la necesidad de sensibilización y de divulgación de la importancia de la gobernanza de TI por medio de acciones coordinadas juntos a los expertos del ámbito y, principalmente, junto a los dirigentes de las organizaciones públicas, en especial a los de niveles más altos de la administración. La concienciación de la alta administración y de la gerencia, sobre la necesidad de implantar los mecanismos es el primer paso para mejorar el escenario. En la secuencia, se deben realizar intercambios de experiencias exitosas y buenas prácticas. En este sentido, la actuación de las EFS también es de extrema importancia así como la proposición de aprobación de leyes y normas que regulen la gobernanza de TI en los diversos países.

Hallazgo 1.2 – Hay mecanismos, están implementados, pero no actúan adecuadamente

6.7. Además de aquellas cuyas estructuras de gobernanza de TI son inexistentes, se observó en prácticamente la mitad de las organizaciones auditadas, un 46%, la existencia de mecanismos y estructuras de gobernanza de TI, que no actuaban adecuadamente.

6.8. Muchas organizaciones no poseen 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.

6.9. Diversas entidades no disponen de 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, y tampoco la definición de metas de gobernanza para los próximos ejercicios. Otra deficiencia advertida, fue la ausencia de una estructura de personal formalmente asignado para la gobernanza de TI.

6.10. En otras organizaciones, 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, las 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.

Criterios

a) Cobit 5 – *Framework*, Capítulo 7 – Guía de Implementación;

b) Cobit 5 – Implementación, Guía de Referencia, Capítulo 3 – Adoptando los primeros pasos hacia la gobernanza de TI;

c) Cobit 5, proceso EDM01 – Garantizar la Definición y Mantenimiento del Modelo de Gobernanza, práctica de gestión EDM01.02 – Dirigir el sistema de gobernanza, actividades 2 y 3;

d) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI.

Causas

6.11. Las causas probables para la existencia de este hallazgo son la fragilidad de la cultura de la gobernanza de las TI y la falta de compromiso de la alta administración.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) Gestión ineficiente de los riesgos de las TI;

b) Falta de evaluación del rendimiento de la institución en relación con la gestión y el uso de lasTI;

c) Dificultad para cumplir con los objetivos de las TI;

d) Desalineación de las acciones de TI con los objetivos de las áreas de negocio;

e) Limitaciones para el logro de la máxima eficacia, eficiencia y efectividad de las TI para agregar valor al negocio con riesgos controlados;

f) Falta de mecanismos adecuados para que los gerentes se anticipen a los problemas y los solucionen antes que generen impactos negativos en las áreas de negocio del organismo;

g) Mayor posibilidad de pérdidas de inversiones resultantes de fallos, deficiencias o inadecuación de procesos internos;

h) Despilfarro de recursos públicos.

Conclusión

6.12. Gran parte de las organizaciones no se encuentra desarrollando acciones para perfeccionar su nivel de gobernanza en las TI. Tal situación, puede comprometer la evolución del nivel de madurez de la gobernanza de las TI, así como, en un último análisis, perjudicar el logro de los objetivos de las TI. De esta manera, se entiende como oportuna la recomendación que las organizaciones elaboren y aprueben formalmente del proceso de perfeccionamiento continuo de la gobernanza de las 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 mejora de la gobernanza de las TI; realización de diagnósticos o autoevaluaciones de gobernanza y de gestión de las TI; y definición y seguimiento de metas de gobernanza de las TI y de las acciones necesarias para lograrlas, con base en los parámetros de la gobernanza, necesidades de negocio y riesgos relevantes.

Hallazgo 1.3 – Inexistencia de Comité de TI

6.13. 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 las TI, 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 que este comité se encuentre compuesto por representantes del área de TI y de otras de la organización, posibilita que las decisiones de inversiones se obtengan a partir de una visión organizacional más acabada, lo que reduce los riesgos de gastos innecesarios o no beneficiosos para la organización.

6.14. Se verificó que en un 44% de las organizaciones auditadas no había comité de TI constituido con las atribuciones precisadas en el Cobit 5. Cabe hacer presente que, en Brasil, donde la existencia de comité es obligatoria debido a normativas infralegales, había un comité en la totalidad de las ocho organizaciones auditadas.

Criterios

a) Cobit 5, proceso APO01 – Gestionar la Estructura para Gestión de TI, práctica de gestión APO01.01 – Definir la Estructura Organizacional, actividad 8.

Causas

6.15. En muchas organizaciones las estructuras que permiten una buena gobernanza de las TI, no están implementadas y, en diversos países, no hay legislación o norma que haga obligatoria la existencia de un comité de TI.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) La estrategia de TI de la organización no se encuentra alineada con la de negocio;
b) Apoyo inexistente o insuficiente de los proyectos basados en TI, a los objetivos institucionales;
c) Apoyo y compromiso insuficientes de la administración en las decisiones esenciales del área de TI;
d) Aumento del riesgo de fracaso de proyectos de TI;
e) Aumento del riesgo de gastos innecesarios en TI.

Conclusión

6.16. El hecho que en más de la mitad de las organizaciones auditadas haya un comité de TI funcionando, hace necesario notar que todavía no está consolidada la importancia de la participación de todos los sectores de la organización en las decisiones estratégicas de las TI. La existencia del comité de TI, aliada a las planificaciones estratégicas institucionales, constituye un instrumento valioso en la orientación de las inversiones de las TI, en el aumento del éxito de los proyectos de TI y en la disminución del riesgo de gastos innecesarios de los recursos.

6.17. Se puede hacer notar también que, la existencia de norma que obligue la constitución de comité de TI en el ámbito de las organizaciones favorece su adhesión a las buenas prácticas internacionales de gobernanza de TI.

Hallazgo 1.4 – La composición del comité de TI no es adecuada

6.18. El simple hecho que exista un comité de TI no garantiza que este cumplirá con su misión y efectivamente contribuirá a una buena gobernanza de las TI. El comité debe

actuar en todas las situaciones requeridas según el rol y las atribuciones definidas. Además, es esencial que el comité sea formado por los integrantes con perfiles adecuados y que representen el área de TI y todas las áreas relevantes de la organización: áreas ejecutivas y áreas de negocio.

6.19. En tres organizaciones auditadas, alrededor de un 7%, se constató que, a pesar de la existencia del comité de TI, sus integrantes no representaban todas las áreas relevantes de la organización. En otro caso, el comité se designó formalmente, pero no realizó ninguna reunión.

Criterios

a) Cobit 5, proceso APO01 – Gestionar la Estructura para Gestión de TI, práctica de gestión APO01.01 – Definir la Estructura Organizacional, actividad 8.

Causas

6.20. Las principales causas identificadas fueron la baja madurez en planificación y la falta de preocupación de la organización en la priorización de las inversiones de TI.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) La ausencia de representantes de todas las áreas relevantes en el comité para el negocio puede resultar en deliberaciones no alineadas con los objetivos de las áreas prioritarias para la organización;

b) La inactividad del comité lleva a no seguir políticas y planes relacionados a la gobernanza de TI, como por ejemplo, la preparación y seguimiento del PDTI, establecimiento de las normas de seguridad de TI, priorización de los proyectos y la definición de las prioridades de inversiones en TI.

Conclusión

6.21. El comité de TI debe contar con representantes de todas las áreas relevantes de la organización. Para ello, se debe recomendar a las organizaciones que perfeccionen la implementación de un comité de TI, en el sentido de asegurar su funcionamiento permanente, así como la efectiva asignación de representantes de áreas relevantes para el negocio de la organización, de forma similar a las orientaciones indicadas en el Cobit 5, práctica de gestión APO01.01 – Definir la Estructura Organizacional, actividad 8.

Hallazgo 1.5 – La alta administración no aprueba las políticas de Gobernanza de TI

6.22. En un 10% de las organizaciones auditadas se verificó la ausencia de la aprobación de las políticas de gobernanza de TI por la alta administración. Se observó casos en que, incluso existiendo las políticas de gobernanza de TI, la alta administración no las aprobó. En otras situaciones, hubo una actuación deficiente de la alta administración en el establecimiento y monitoreo de políticas corporativas, no formalizando su política de gobernanza de TI.

6.23. Se verificaron hechos en que no se establecieron mecanismos para dirigir y evaluar la gestión y el uso corporativo de las TI, por ejemplo los objetivos de gestión y de uso de las TI; indicadores de rendimiento para cada objetivo de gestión y de uso de TI; mecanismos de control del cumplimiento de las metas de gestión y de uso de TI; planes de auditoría aprobados para evaluar los riesgos considerados críticos para el negocio y la eficacia de los controles respectivos; y normas que demuestren que la alta administración

utiliza los indicadores de resultados estratégicos de los principales sistemas de información y la toma decisiones relacionadas cuando no se logran las metas.

Criterios

a) Cobit 5, proceso EDM01 – Garantizar la Definición y Mantenimiento del Modelo de Gobernanza, práctica de gestión EDM01.01 – Evaluar el sistema de gobernanza;

b) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI, práctica de gestión APO01.03 – Mantener los habilitadores para la gestión de TI;

c) Norma ISO/IEC 38500:2008, ítem 3.3.

Causas

6.24. Las posibles causas identificadas fueron la inexistencia de legislación o norma reglamentaria que establezca la obligatoriedad de aprobación de las políticas de gobernanza de TI por la alta administración y la baja madurez de la organización en gobernanza de TI.

Efectos y riesgos derivados de la mantención de la situación detectada

a) Mayor exposición del negocio a los riesgos;

b) Falta de efectividad de las políticas corporativas de TI existentes;

c) Dificultad para lograr los objetivos institucionales.

Conclusión

6.25. El liderazgo y la supervisión de la alta administración sobre la elaboración y la conducción de las políticas de TI son esenciales para obtener los resultados esperados del área de TI. En un 10% de las organizaciones auditadas, la dirección y la evaluación de la gestión y del uso corporativos de TI se presentan deficitarias, siendo necesario el establecimiento de los mecanismos de gobernanza de TI inexistentes, la aprobación formal de las políticas de gobernanza de TI y la ejecución de auditorías internas periódicas con el objetivo de proporcionar una evaluación objetiva a la alta administración en relación con la eficacia de la gestión de riesgos y el logro de las metas establecidas.

Hallazgo 2.1 – Inexistencia de proceso de planificación de TI

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

6.27. La incorporación del proceso de planificación de las 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 funcionar adecuadamente.

Criterios

a) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.03 – Definir la Capacidad de TI Deseada;

b) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.04 – Conducir Análisis de Deficiencias;

c) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.05 – Definir el Plan Estratégico y Guion de Implementación.

Causas

6.28. En general la falta de normativa específica que exija la existencia de proceso de trabajo para la planificación de TI, combinado con la falta de cultura de planificación y la carencia de recursos humanos capacitados.

Efectos y riesgos derivados de la mantención de la situación observada

a) Ausencia de planificación estratégica de TI;
b) Inexistencia de planes de acción y operacionales para el área de TI;
c) La elaboración de los planes de TI no cuenta con la participación de las demás áreas de negocio de la organización;
d) Planes de TI no alineados con los planes de negocio;
e) Planes de TI desactualizados;
f) La ejecución de las actividades de TI no es tutelada por la alta administración;
g) No se logran los resultados esperados por el área de TI;
h) Despilfarro de recursos públicos.

Conclusión

6.29. Solamente la implantación del proceso de planificación de TI permitirá a las organizaciones públicas el uso más eficiente de los recursos de TI. La inexistencia de ese proceso en una parte significativa de las organizaciones públicas, requiere la incoporación de las EFS en el sentido de concientizar a la alta administración y a los gerentes de TI en la importancia de la planificación de las TI.

Hallazgo 2.2 – No se producen documentos de planificación estratégica de TI

6.30. Casi dos tercios, un 63% de las organizaciones auditadas no realizan planificación estratégica de TI. Se debe destacar, una vez más, la importancia de la planificación estratégica para la gobernanza de las TI. Dado que para que la planificación estratégica de TI sea efectiva y proporcione los resultados esperados, 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.

6.31. Evidentemente, no se debe confundir el hecho de no haber planificación estratégica con el 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 reseñar los caminos y estrategias, solo prevén cómo se asignarán los recursos disponibles en aquel año. Además, esos planes no son instrumentos para seguir y apoyar los proyectos de mediana y larga duración, comunes en el área de TI. Otro problema normalmente observado, se produce cuando por ausencia de planificación estratégica se discontinúan esos proyectos y conlleva a la utilización innecesaria de recursos.

6.32. 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.

Criterios

a) Cobit 5, proceso APO02 – Gestionar la Estrategia.

Causas

6.33. Ausencia de normas y controles que aseguren la implantación y ejecución del proceso de planificación estratégica de TI, asociada a la inexistencia de recursos humanos capacitados.

Efectos y riesgos derivados de la mantención de la situación advertida

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;
b) Planes de TI no alineados con las necesidades del negocio;
c) Inexistencia de consultas regulares entre gerente de TI y demás gerentes acerca de los proyectos y servicios de TI;
d) Disminución de las acciones de TI;
e) Discontinuidad de los proyectos de TI;
f) Insatisfacción de los usuarios;
g) Visión negativa del área de TI;
h) Resultados del área de TI por debajo del esperado;
i) Dificultad de obtención de recursos para el área de TI;
j) Inversiones innecesarias en TI;
k) Despilfarro de recursos.

Conclusión

6.34. La planificación estratégica de TI debe posibilitar la definición, en cooperación con los principales interesados, sobre la forma por 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, los activos de TI y la forma en la cual el área de TI 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 ser suficientemente detallado para permitir su despliegue en planes tácticos de TI.

6.35. Se hace fundamental la diseminación de la cultura de la planificación estratégica en las organizaciones públicas; las EFS deben obtener sus resultados.

Hallazgo 2.3 – La alta administración no aprueba los planes de TI

6.36. Se constató que un 24% de las organizaciones auditadas a pesar de contar con planes estratégicos y tácticos de TI, estos no se encontraban aprobados por la alta administración. Se observan en esos casos que existe gran posibilidad que no se sigan esos documentos, no logrando los resultados planificados. Es fundamental la dirección y la supervisión de la alta administración de las acciones y proyectos de TI. Su inexistencia termina por desincentivar la ejecución de los planes y, en gran medida, hace que esos documentos sean buenas intenciones.

Criterios

a) Cobit 5, proceso EDM04 – Garantizar la Optimización de los Recursos;

b) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.05 – Definir el Plan Estratégico y Guion de Implementación.

Causas

6.37. La causa más evidente es la ausencia de iniciativa por parte de la alta administración de las organizaciones para la elaboración, aprobación y publicación de los planes estratégicos y tácticos de las TI.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;

b) Planes de TI no alineados con las necesidades del negocio;

c) Inexistencia de consultas regulares entre gerente de TI y demás gerentes acerca de los proyectos y servicios de TI;

d) Disminución de las acciones de TI;

e) Discontinuidad de los proyectos de TI;

f) Insatisfacción de los usuarios;

g) Visión negativa del área de TI;

h) Resultados del área de TI por debajo del esperado;

i) Dificultad de obtención de recursos para el área de TI;

j) Inversiones innecesarias en TI;

k) Despilfarro de recursos.

Conclusión

6.38. La existencia de proceso de trabajo, de documentos y de planes de TI no es suficiente para garantizar su efectividad. Tan importante dado que la elaboración y la ejecución de planificación de TI es su dirección y supervisión. Así, la alta administración debe aprobar los documentos más relevantes y definidores de la planificación de TI, siendo ello un control básico para la gobernanza de TI.

Hallazgo 2.4 – La elaboración de los planes de TI no cuenta con la participación de las áreas de negocio

6.39. La participación de todas las áreas relevantes de la organización en la elaboración de los planes de TI posibilita definir las decisiones más eficaces y eficientes, además, de la reducción de los riesgos asociados. Como ya se ha mencionado en la introducción de este informe, existe hoy una alta dependencia de las TI en todos los sectores de la administración pública y su uso optimizado de los recursos permite que se logren los objetivos de cada área de la organización de modo eficiente. Pero, en un 20% de las organizaciones auditadas se encontraron deficiencias en la comunicación y discusión de las necesidades de TI entre el área de TI y las demás áreas de la organización.

Criterios

a) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI, práctica de gestión APO01.04 – Comunicar Objetivos y Dirección de Gestión;

b) Cobit 5, proceso APO02 – Gestionar la Estrategia.

Causas

6.40. La alta administración no exige ni estimula la participación de las áreas relevantes de la organización en la discusión, elaboración y definición de los planes de TI.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;
b) Planes de TI no alineados a las necesidades del negocio;
c) Discontinuidad de los proyectos de TI;
d) Insatisfacción de los usuarios;
e) Visión negativa del área de TI;
f) Resultados del área de TI por debajo del esperado.

Conclusión

6.41. La alta administración debe definir estrategias y procedimientos que estimulen la participación de todas las áreas relevantes de la organización en la elaboración de los planes de TI. A partir de la definición de responsabilidades de cada área, no se deben aprobar los planes de TI que no cuenten con la previa discusión de las áreas involucradas.

Hallazgo 2.5 – Los planes de TI no están alineados con los planes de negocio

6.42. Se verificó que en un 24% de las instituciones auditadas los planes de TI no están alineados con los planes de negocio. En algunos casos, las acciones previstas en el plan táctico de TI, (PDTI) no están explícitamente relacionadas con las directrices establecidas en el Plan Estratégico Institucional (PEI) o en el Plan Estratégico de TI (PETI). Así, las acciones no pueden ser consideradas como directrices presentes en los planes estratégicos de la organización. En otros casos, la organización disponía del PEI, pero no disponía de un PETI, donde las acciones previstas en el PDTI no están explícitamente relacionadas con las directrices de negocio establecidas.

Criterios

a) Cobit 5, proceso EDM02 – Asegurar Entrega de Beneficios;
b) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.01 – Entender Dirección del Negocio.

Causas

6.43. La principal causa es la ausencia de comunicación entre las diversas áreas de negocio de la organización (hallazgo 2.4), pero en uno de los casos analizados se verificó que la elaboración de los planes estratégicos de la organización estaba a cargo de una empresa subcontratada. En ese caso específico, se atribuye la desalineación entre los planes a fallas de la organización en el seguimiento y supervisión de los trabajos realizados por la empresa contratada.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;
b) Discontinuidad de los proyectos de TI;
c) Insatisfacción de los usuarios;
d) Visión negativa del área de TI;
e) Resultados del área de TI por debajo del esperado.

Conclusión

6.44. Para lograr los resultados esperados en los planes de TI, es esencial que haya alineación entre los planes de TI y los planes de negocio. Fundamental, también, la permanente comunicación entre las áreas relevantes de la organización y el área de TI.

6.45. La alta administración tiene que establecer una estrategia y controles adecuados que aseguren la alineación necesaria entre los planes de TI y planes de negocio.

Hallazgo 2.6 – Los planes operacionales de TI no están alineados con el PETI o con el PDTI

6.46. En lo que se refiere a los planes de TI, otra situación observada en un 10% de las organizaciones auditadas fue la desalineación entre sí. Se constató que las acciones previstas en el PDTI no están directamente vinculadas a las metas e indicadores de negocio previstos en el PETI.

6.47. Importante observar que, en esos casos, además de no haber la alineación entre sí, los planes de TI tampoco están alineados con los planes de negocio como en el hallazgo 2.5.

Criterios

a) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.01 – Entender Dirección del Negocio;

b) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.05 – Definir el Plan Estratégico y Guion de Implementación.

Causas

6.48. La causa principal es la ausencia de proceso de planificación de TI, o sea, no se elaboran los planes de TI a partir de la ejecución del plan que está en un nivel superior para el otro plan que está en un nivel inferior de la planificación. Por ejemplo, el PDTI es la ejecución del PETI (estratégico), ya que un plan de acción (operacional) es el desarrollo del PDTI (táctico). Los planes de TI se elaboran eventualmente y no de forma regular, siguiendo un proceso definido.

Efectos y riesgos derivados de la mantención de la situación observada

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;

b) Discontinuidad de los proyectos de TI;

c) Insatisfacción de los usuarios;

d) Visión negativa del área de TI;

e) Resultados del área de TI por debajo del esperado.

Conclusión

6.49. Las EFS deben recomendar la implantación de un proceso de planificación de TI y que el PDTI contenga al menos los siguientes elementos:

- ejecución de las directrices establecidas en planes estratégicos, a ejemplo del plan estratégico institucional (PEI) y del plan estratégico de TI (PETI);
- vinculación de las acciones de TI (actividades y proyectos) a los indicadores y las metas de negocio;
- vinculación de las acciones de TI a los indicadores y las metas de servicios al ciudadano;
- vinculación entre las acciones de TI priorizadas al presupuesto de TI;

- cantidad necesario (ideal) para la fuerza de trabajo en TI.

Hallazgo 2.7 – La alta administración no sigue los planes de TI

6.50. En casi un tercio de las organizaciones auditadas, un 29%, se constató que la alta administración no sigue 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 del PETI contener la definición de metas, no constan informaciones acerca de cómo se miden y se controlan esas metas.

6.51. En otras situaciones, no se establecieron formalmente objetivos de gestión y de uso corporativo de las 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.

Criterios

a) Cobit 5, proceso EDM02 – Asegurar Entrega de Beneficios;

b) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI, práctica de gestión APO01.03 – Mantener los habilitadores para la gestión de TI;

c) Norma ISO/IEC 38500:2008, ítem 3.3.

Causas

6.52. Se identificaron como causas la escasa importancia entregada por la alta administración a los planes de TI o la concentración de la alta administración solo en las actividades que juzgó más relevantes, sin orientarse a las actividades y los resultados del área de TI como un todo.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Soporte ineficaz del área de TI en la consecución de la misión de la organización;

b) Disminución de las acciones de TI;

c) Discontinuidad de los proyectos de TI;

d) Insatisfacción de los usuarios;

e) Visión negativa del área de TI;

f) Resultados del área de TI por debajo del esperado;

g) Inversiones innecesarias en TI;

h) Despilfarro de recursos.

Conclusión

6.53. Las EFS deben recomendar a las organizaciones 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.

6.54. 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.

Hallazgo 2.8 – Los planes de TI no están actualizados

6.55. Solamente en un 7% de las organizaciones auditadas se encontraron planes de TI en ejecución que estaban desactualizados. El área de TI, debido a su dinámica está sujeta a cambios constantes. Esos cambios muchas veces hacen que los planes de TI existentes se encuentran desactualizados. Así que, es un factor crítico de éxito la gestión de los cambios y la actualización junto a la adaptación de los planes de TI.

Criterios

a) Cobit 5, proceso APO02 – Gestionar la Estrategia.

Causas

6.56. Fallos en el proceso de planificación de TI.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Soporte ineficaz del área de TI en la obtención de la misión de la organización;
b) Resultados del área de TI por debajo del esperado;
c) Inversiones innecesarias en TI;
d) Despilfarro de recursos.

Conclusión

6.57. El proceso de planificación de TI debe contener acciones que aseguren el mantenimiento de los planes de TI actualizados.

Hallazgo 2.9 – No se divulgan los planes de TI

6.58. Teniendo en consideración el principio del *accountability*, que se relaciona con el deber de rendir cuentas, las organizaciones públicas deben divulgar todas las informaciones que no sean consideradas reservadas. En los planes de TI, no debe ser diferente la situación expuesta, todas las informaciones cuya divulgación no comprometa la seguridad de la organización o que no estén clasificadas como reservadas deben ser comunicadas tanto a nivel interno como externo.

6.59. En algunos países, incluso, existe legislación vigente que obliga la divulgación de las informaciones. Se verificó que un 15% de las organizaciones auditadas no difunden sus planes de TI.

Criterios

a) Cobit 5, proceso EDM05 – Garantizar Transparencia para las Partes Interesadas.

Causas

6.60. Falta de mecanismos para la divulgación de las informaciones de los planes de TI a nivel interno y externo.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Dificultad en el control de los gastos públicos;
b) Dificultad en el seguimiento de las acciones de TI, por parte de las otras áreas de la organización.

Conclusión

6.61. Las EFS deben estimular las organizaciones auditadas a divulgar todas las informaciones de los planes de TI cuya comunicación no comprometa la seguridad de la organización o que no estén clasificadas como reservadas.

Hallazgo 3.1 – No se elabora el Plan de Gastos en TI

6.62. Entre las organizaciones auditadas, solamente un 12% no elabora un plan de gastos de TI. Para realizar todas las acciones de TI planificadas se necesitan diversos tipos de recursos, entre ellos recursos financieros. Con el objetivo de obtener los recursos financieros necesarios, el área de TI tiene que presentar un presupuesto para el próximo período, un plan de gastos en TI, en el que deben constar aquellos gastos habituales para el mantenimiento de las actividades de TI, así como la estimación de los gastos necesarios para la ejecución de los nuevos proyectos y de las nuevas actividades de TI.

Criterios

a) Cobit 5, proceso APO06 – Gestionar Presupuesto y Costes.

Causas

6.63. La causa principal de esta situación es la ausencia de la obligación explícita para el área de TI de presentar un plan de gastos separado, de modo que los gastos de TI terminan siendo incorporados a otros presupuestos no específicos.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) Dificultad de controlar los gastos específicos del área de TI;

b) Dificultad de evaluar el retorno del área de TI para la organización;

c) Posible despilfarro de recursos públicos.

Conclusión

6.64. Para que los recursos financieros no sean un obstáculo a la ejecución de los planes de TI, la organización tiene que establecer e implementar prácticas para elaborar un presupuesto que refleje las prioridades establecidas en la lista de proyectos de TI e incluya los costos actuales de operación y mantenimiento de la infraestructura existente. Las prácticas deben soportar el desarrollo de un presupuesto general para TI, así como la ejecución de presupuestos específicos para los proyectos con énfasis específico en los componentes de TI. Las prácticas deben permitir revisión del curso, refinamiento de las informaciones y aprobación del presupuesto general para TI y de los presupuestos específicos de los proyectos.

Hallazgo 3.2 – Inexistencia de Proceso para Adquisición de Soluciones de TI

6.65. Poco más de un tercio de las organizaciones auditadas, un 34%, no posee un proceso de planificación de las contrataciones de tecnología de la información. En la contratación de soluciones de TI, es esencial la adopción de un proceso de trabajo formalizado y estandarizado, el cual debe ser capaz de posibilitar la contratación por un valor adecuado que pueda traer beneficios a la organización. Este proceso mejora la relación con los proveedores y prestadores de servicios, maximiza la utilización de los recursos financieros asignados al área de TI y contribuye decisivamente para que los

servicios de TI entreguen el necesario soporte a las acciones de la organización en el logro de sus objetivos y metas.

6.66. Se debe observar que eso no significa dejar de cumplir la legislación específica. Sin embargo, la ausencia de un proceso de trabajo definido, estandarizado, documentado y aprobado para realizar las contrataciones de TI puede implicar consecuencias perjudiciales en la organización. Como no hay procedimientos formales y comunicados en la organización, cada área puede adquirir los recursos que necesita de una forma diferente. De esa manera, la organización se expone a riesgos innecesarios y que se podrían evitar con la adopción de un proceso de trabajo formalizado.

Criterios

a) Cobit 5, proceso APO06 – Gestionar Presupuesto y Costos;

b) Cobit 5, proceso BAI03 – Gestionar Identificación y Desarrollo de Soluciones, práctica de gestión BAI03.04 – Adquirir Componentes de la Solución.

Causas

6.67. La ausencia de normas que obliguen la organización a establecer un proceso estándar para la contratación de soluciones de TI y falta de cultura de planificación son identificadas como las principales causas de esta situación.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Incumplimiento de todas las disposiciones legales y normativas;

b) Fallas en el proceso de adquisición puede generar repercusiones en la gestión de los contratos;

c) Litigios judiciales debido a contrataciones mal efectuadas;

d) Contrataciones más costosas que el precio de mercado por falta de controles;

e) Realización de adquisiciones innecesarias, con baja calidad o que no estén alineadas con las necesidades del negocio;

f) Despilfarro de recursos.

Conclusión

6.68. Las EFS deben recomendar a las organizaciones el desarrollo e implantación de un conjunto de procedimientos y modelos consistentes con el proceso de licitación y la estrategia de adquisición generales de la organización para adquirir infraestructura, instalaciones, hardware, software y servicios de TI necesarios al negocio.

Hallazgo 3.3 – El proceso para adquisición de soluciones de TI no contiene las etapas necesarias para minimizar los riesgos que las contrataciones no logren los resultados esperados

6.69. En complemento al hallazgo 3.2, se debe asegurar que el proceso de adquisición de soluciones de TI implantado contemple todas las etapas necesarias para minimizar los riesgos inherentes a las contrataciones. Se observó en un 12% de las organizaciones auditadas deficiencias en el proceso de adquisiciones de soluciones de TI.

6.70. Para minimizar los riesgos que las contrataciones no logren los resultados esperados, el proceso de contratación debe contar, como mínimo, con las siguientes etapas: análisis de la viabilidad de la contratación (definición de los requisitos de la solución, investigación de las soluciones disponibles en el mercado y análisis y comparación del costo-beneficio de las soluciones encontradas), análisis de los riesgos de cada solución y

definición de la solución adoptada que contenga todos los componentes necesarios para generar los resultados esperados.

Criterios

a) Cobit 5, proceso BAI03 – Gestionar Identificación y Desarrollo de Soluciones, práctica de gestión BAI03.04 – Adquirir Componentes de la Solución.

Causas

6.71. Establecimiento de proceso falló en la contratación de soluciones de TI o actualización del proceso en función de cambios legales o regulatorios.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Incumplimiento de todas las disposiciones legales y normativas;
b) Fallos en el proceso de adquisición genera repercusiones en el proceso de gestión de los contratos;
c) Litigios judiciales debido a contrataciones mal efectuadas;
d) Contrataciones más costosas que el precio de mercado por falta de controles;
e) Realización de adquisiciones innecesarias, con baja calidad o que no estén alineadas a las necesidades del negocio;
f) Despilfarro de recursos.

Conclusión

6.72. Las organizaciones tienen que evaluar su proceso de contratación de soluciones de TI y revisarlo siempre que se encuentren fallos o imperfecciones.

Hallazgo 3.4 – No se elabora el presupuesto de TI a partir de las acciones planificadas

6.73. En un 17% de las organizaciones auditadas se verificó que en la elaboración del presupuesto de TI no se utilizaron los insumos necesarios a la confección de un documento fidedigno. Cuando no se utilizan las informaciones de las actividades de TI planificadas para elaboración del presupuesto de TI existe una gran probabilidad que la estimación de los gastos quede muy lejos de la real necesidad de la organización.

Criterios

a) Cobit 5, proceso APO02 – Gestionar la Estrategia, práctica de gestión APO02.05 – Definir el Plan Estratégico y Guion de Implementación;
b) Cobit 5, proceso APO06 – Gestionar Presupuesto y Costes;
c) Cobit 5, proceso BAI03 – Gestionar Identificación y Desarrollo de Soluciones, práctica de gestión BAI03.04 – Adquirir Componentes de la Solución.

Causas

6.74. La ausencia de planificación y de normas que regulen la correcta elaboración del presupuesto de TI son las principales causas para esta situación.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) No ejecución de las acciones de TI planificadas por falta de recursos presupuestarios;
b) Retraso en la ejecución de proyectos de TI;

c) No utilización de recursos presupuestarios reservados debido a la sobre-estimación de gastos.

Conclusión

6.75. La organización siempre debe perfeccionar la elaboración de presupuestos de TI, haciéndolos lo más preciso posible para evitar los retrasos en la ejecución de proyectos o impedir la realización de otros por retener recursos innecesarios.

Hallazgo 3.5 – Ausencia de monitoreo del proceso para adquisición de soluciones de TI

6.76. Además de la implantación de proceso de contratación de TI, se hace 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 organizaciones auditadas no se realiza dicho monitoreo.

6.77. 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.

Criterios

a) Cobit 5, proceso EDM04 – Garantizar la Optimización de los Recursos;

b) Cobit 5, proceso BAI03 – Gestionar Identificación y Desarrollo de Soluciones, práctica de gestión BAI03.04 – Adquirir Componentes de la Solución.

Causas

6.78. La ausencia de normas internas que establezcan el monitoreo del proceso como una de las etapas del propio proceso y la falta de métricas para gestión de las contrataciones.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Realización de adquisiciones innecesarias, con baja calidad o que no estén alineadas a las necesidades del negocio;

b) Despilfarro de recursos.

Conclusión

6.79. Los objetivos del monitoreo 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.

Hallazgo 3.6 – Ausencia de monitoreo del proceso de gestión de los contratos de TI

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

6.81. 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.

Criterios

a) Cobit 5, proceso EDM04 – Garantizar la Optimización de los Recursos;

b) Cobit 5, proceso BAI03 – Gestionar Identificación y Desarrollo de Soluciones, práctica de gestión BAI03.04 – Adquirir Componentes de la Solución.

Causas

6.82. La ausencia de normas internas que establezcan el monitoreo del proceso como una de las etapas del propio proceso y la falta de métricas para gestión de los contratos de TI.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Rendimiento de los recursos de TI contratados por debajo de la necesidad de la organización;

b) No atención de las necesidades del negocio;

c) Despilfarro de recursos.

Conclusión

6.83. 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.

Hallazgo 4.1 – No se aprobó ni publicó la Política de Seguridad de la Información (PSI)

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

6.85. 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.

Criterios

a) Norma ISO/IEC 27002:2013, sección 5.1.1;

Causas

6.86. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Aumento del riesgo de incidentes de seguridad de la información;

b) Disminución de las acciones de seguridad, por no tener el respaldo de una política institucional;

c) Desacuerdo entre la gestión de la seguridad de la información y los objetivos de negocio;

d) Percepción por los usuarios y clientes de falta de compromiso de la alta administración de la organización con la seguridad de la información.

Conclusión

6.87. 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 Política de Seguridad de la Información para toda la organización.

Hallazgo 4.2 – Ausencia de aprobación y publicación del proceso de gestión de la seguridad de la información

6.88. En un 12% de las organizaciones auditadas no se verificó la existencia de proceso de gestión de la seguridad de la información aprobado y publicado. Ese proceso busca proteger el procesamiento de la información, ya que organizaciones, procesos, tecnología y personas están en constante cambio.

Criterios

a) Norma ISO/IEC 27002:2013, sección 6;

b) Cobit 5, proceso APO13 – Gestionar Seguridad.

Causas

6.89. La causa principal observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) No garantiza la ejecución plena de las directrices, políticas y procedimientos definidos para la seguridad de la información;

b) Aumento del riesgo de incidentes de seguridad de la información;

c) Dificultad en garantizar la confidencialidad, integridad y disponibilidad de las informaciones;

d) Desacuerdo entre la gestión de la seguridad de la información y los objetivos de negocio.

Conclusión

6.90. La organización debe disponer de proceso para gestión de seguridad de la información que permita la evaluación, la corrección y el registro de las acciones de seguridad de la información. La evaluación busca determinar si la seguridad de la información está actualizada. Ya la corrección busca perfeccionar las deficiencias y mantener siempre los procesos con el nivel de calidad adecuado. Por fin, el proceso de registro tiene por objetivo aprender del pasado y ejecutar un análisis de tendencias para prever el futuro, además de evidenciar los resultados de la seguridad de la información.

Hallazgo 4.3 – Ausencia de designación formal de unidades o personas para gestionar la seguridad de la información

6.91. En un 51% de las organizaciones auditadas no había responsables, unidades o personas, designados para ejecutar la gestión de la seguridad de la información. 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.

Criterios

a) Norma ISO/IEC 27002:2013, sección 6.1.1;

b) Cobit 5, proceso APO13 – Gestionar Seguridad.

Causas

6.92. La causa principal observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Falta de garantía de la ejecución plena de las directrices, políticas y procedimientos definidos para la seguridad de la información;

b) Aumento del riesgo de incidentes de seguridad de la información;

c) Dificultad de garantizar la confidencialidad, integridad y disponibilidad de las informaciones;

d) Desacuerdo entre la gestión de la seguridad de la información y los objetivos de negocio.

Conclusión

6.93. Cada organización debe designar formalmente un responsable como 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.

Hallazgo 4.4 – Ausencia de designación formal del comité de seguridad de la información

6.94. Se constató que en un 46% de las organizaciones auditadas, no había comité de seguridad de la información formalmente instituido. La principal función de ese comité es coordinar las actividades de seguridad de la información contando con la participación de representantes de todas las áreas relevantes de la organización. Como el comité no desempeña funciones ejecutivas, su papel no se confunde con el área responsable de la gestión de la seguridad de la información.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 6;

b) Cobit 5, proceso APO01 – Gestionar la Estructura de Gestión de TI;

c) Cobit 5, proceso APO13 – Gestionar Seguridad.

Causas

6.95. La causa principal observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Falta de garantía de la ejecución plena de las directrices, políticas y procedimientos definidos para la seguridad de la información;

b) Aumento del riesgo de incidentes de seguridad de la información;

c) Dificultad de garantizar la confidencialidad, integridad y disponibilidad de las informaciones;

d) Desacuerdo entre la gestión de la seguridad de la información y los objetivos de negocio.

Conclusión

6.96. La existencia de un comité gestor de seguridad de la información formalmente instituido contribuye significativamente para el perfeccionamiento y la efectividad de la seguridad de la información de la organización.

Hallazgo 4.5 – No se aprobó ni publicó un proceso para inventariar activos de TI de la organización

6.97. Se observó que en un 46% de las organizaciones auditadas no se realizaba inventario de los activos de TI. Para alcanzar y mantener la protección adecuada de los activos de TI de la organización, se deben inventariar todos estos. Para cada activo de TI debe ser designado un propietario responsable que tendrá la obligación de la protección y del mantenimiento apropiado de los controles sobre éste.

6.98. Hay varios tipos de activos: de información (base de datos, documentos, etc.); de software (sistemas, aplicativos, utilitarios, etc.); físicos (equipos computacionales, de comunicación y medios extraíbles); servicios (electricidad, refrigeración, comunicación, etc.); personas y sus calificaciones; e intangibles (reputación e imagen de la organización).

Criterios

a) Norma ISO/IEC 27002:2013, Sección 8.1.1;

b) Cobit 5, proceso BAI09 – Gestionar Activos;

c) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.99. La causa principal advertida es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Aumento del riesgo de incidentes de seguridad de la información.

Conclusión

6.100. Las EFS deben orientar a las organizaciones que auditan en la implementación del proceso de gestión de activos de TI de la organización, de forma similar a lo manifestado en la sección 8.1.1 de la norma ISO/IEC 27002:2013 y en el Cobit 5, proceso BAI09 – Gestionar Activos.

Hallazgo 4.6 – Ausencia de aprobación y publicación del proceso de clasificación de las informaciones

6.101. Se observó que en un 24% de las organizaciones auditadas no se aprobó ni publicó un proceso de clasificación de las informaciones, que busca asegurar que la información reciba un nivel adecuado de protección, de acuerdo con su importancia para la organización. La información debe ser clasificada en términos del valor, de requisitos legales, de la sensibilidad y de la criticidad para evitar alteración o divulgación no autorizada. La clasificación da a las personas que trabajan con informaciones una indicación concisa de cómo tratar y proteger la información.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 8.2;

b) Cobit 5, proceso BAI09 – Gestionar Activos;

c) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.102. La principal causa observada consiste en la falta de comprensión por parte de las organizaciones, de la importancia del tema seguridad de la información para el logro de los objetivos de negocio.

Efectos y riesgos derivados del mantenimiento de la situación encontrada

a) Aumento del riesgo de incidentes de seguridad de la información.

Conclusión

6.103. Las EFS deben orientar a las organizaciones que auditan en la implementación del proceso de clasificación de informaciones de la organización, de forma similar a las orientaciones presentes en la sección 8.2 de la norma ISO/IEC 27002:2013.

Hallazgo 4.7 – Ausencia de aprobación y publicación de la Política de Control de Acceso (PCA)

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

6.105. 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.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 9.1.1;

b) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.106. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Aumento del riesgo de incidentes de seguridad de la información.

Conclusión

6.107. Las EFS deben recomendar a las organizaciones que audita 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.

Hallazgo 4.8 – Ausencia de aprobación y publicación de proceso de gestión de los riesgos a los que la información crítica del negocio está sometida

6.108. Se constató que un 49% de las instituciones auditadas no poseen 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 del riesgo, la aceptación de éste, la comunicación del riesgo junto al monitoreo y al análisis crítico de los riesgos de seguridad de la información.

Criterios

a) Norma ISO/IEC 27005:2008;

b) Cobit 5, proceso APO12 – Gestionar Riesgos;

c) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.109. La causa principal observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) La ausencia de proceso de gestión de riesgos de seguridad de la información hace inviable la identificación, prevención, eliminación o mitigación de los riesgos de seguridad de la información a que la organización está sujeta.

Conclusión

6.110. Las EFS deben recomendar a las organizaciones 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.

Hallazgo 4.9 – Ausencia de aprobación y publicación del proceso de gestión de incidentes

6.111. Se detectó que un 22% de las organizaciones auditadas no poseen proceso de gestión de incidentes de seguridad de la información formalmente aprobado y publicado. El proceso de gestión de incidentes de seguridad de la información tiene por objetivo asegurar un enfoque consistente y efectivo para gestionar los incidentes de seguridad de la

información, incluyendo la comunicación sobre fragilidades y eventos de seguridad de la información.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 16;

b) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.112. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Las organizaciones no podrán dar tratamiento oportuno y adecuado a los incidentes de seguridad de la información, además de hacerse cargo de las pérdidas derivadas.

Conclusión

6.113. Las EFS deben recomendar a las organizaciones que auditan, que instituyan y ejecuten un proceso de gestión de incidentes de seguridad de la información, de forma similar a las orientaciones presentes en la sección 16 de la norma ISO/IEC 27002:2013.

Hallazgo 4.10 – Ausencia de designación formal del equipo de tratamiento y respuesta a incidentes en redes computacionales

6.114. Se verificó que un 29% de las instituciones evaluadas no designaron formalmente a un equipo de tratamiento y respuesta a incidentes en redes computacionales, ETIR. Éste consiste en un grupo de personas con la responsabilidad de recibir, analizar y responder a las notificaciones y actividades relacionadas a incidentes de seguridad en redes de computadoras, la que es coordinada por el área de gestión de seguridad de la información y debe ser designada formalmente.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 16.1.5;

b) Cobit 5, proceso DSS05 – Gestionar Servicios de Seguridad.

Causas

6.115. La causa principal observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

b) Las organizaciones no podrán dar tratamiento oportuno y adecuado a los incidentes en redes computacionales, además de hacerse cargo de las pérdidas derivadas.

Conclusión

6.116. Las EFS deben recomendar a las organizaciones que auditan, que designen formalmente equipo de tratamiento y respuesta a incidentes en redes computacionales de forma similar a las orientaciones presentes en la sección 16.1.5 de la norma ISO/IEC 27002:2013.

Hallazgo 4.11 – Ausencia de aprobación y publicación del proceso de gestión de la continuidad de los servicios de TI

6.117. Se constató que más de la mitad (un 54%) de las organizaciones auditadas no implementó 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 posibilitando que las informaciones más críticas estén disponibles de acuerdo con el nivel de servicio requerido.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 17;

b) Cobit 5, proceso DSS04 – Gestionar Continuidad.

Causas

6.118. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Falta de garantía de la oferta perenne de servicios a los clientes internos, de forma adecuada a las necesidades de la organización;

b) Ausencia de preparación para planificar medidas de seguridad necesarias, de forma a minimizar los impactos derivados de fallos, desastres o indisponibilidades significativas en los recursos que soportan los procesos de información de la organización;

c) Aumento del riesgo de incidentes de seguridad de la información;

d) Dificultad en garantizar la confidencialidad, integridad y disponibilidad de las informaciones.

Conclusión

6.119. Las EFS deben recomendar a las organizaciones 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.

Hallazgo 4.12 – Ausencia de aprobación y publicación del Plan de Continuidad de Negocios (PCN)

6.120. Se detectó que la mayoría (un 59%) de las organizaciones auditadas no posee 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, asegurando su retorno en un tiempo definido.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 17;

b) Cobit 5, proceso DSS04 – Gestionar Continuidad.

Causas

6.121. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Falta de garantía de la oferta perenne de servicios a los clientes internos, de forma adecuada a las necesidades de la organización;

b) Ausencia de preparación para planificar medidas de seguridad necesarias, de forma a minimizar los impactos derivados de fallos, desastres o indisponibilidades significativas en los recursos que soportan los procesos de información de la organización;

c) Aumento del riesgo de incidentes de seguridad de la información;

d) Dificultad en garantizar la confidencialidad, integridad y disponibilidad de las informaciones.

Conclusión

6.122. Las EFS deben recomendar a las organizaciones 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.

Hallazgo 4.13 – Ausencia de concienciación de los colaboradores en seguridad de la información

6.123. Se observó que en un 34% de las organizaciones auditadas no se hace la concienciación de los colaboradores en seguridad de la información. Cabe señalar, que todos los funcionarios y colaboradores de la organización reciban capacitación, educación y concienciación acorde a la seguridad de la información.

Criterios

a) Norma ISO/IEC 27002:2013, Sección 7.2.2;

b) Cobit 5, proceso APO07 – Gestionar Recursos Humanos, práctica de gestión APO07.03 – Mantener las Habilidades y Competencias del Personal, actividad 5 – Desarrollar y aplicar un programa de capacitación, basado en los requisitos organizacionales y de los procesos, incluyendo requisitos para el entendimiento del negocio, control interno, conducta ética y seguridad.

Causas

6.124. La principal causa observada es que las organizaciones no comprenden satisfactoriamente la seguridad de la información como tema importante para el logro de los objetivos de negocio.

Efectos y riesgos derivados de la mantención de la situación encontrada

a) Sin programas de concientización y capacitación en seguridad de la información la organización correrá riesgos de no adopción de los usuarios a la política de seguridad de información implantada y a otras políticas y prácticas derivadas.

Conclusión

6.125. Las EFS deben orientar a las organizaciones que auditan, en la implantación de los programas de concientización y capacitación en seguridad de la información en el ámbito de la organización de forma similar a las orientaciones presentes en la sección 7.2.2 de la norma ISO/IEC 27002:2013 y proceso APO07 – Gestionar Recursos Humanos 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 organizaciones 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 enfocarse 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 existir los mecanismos y las estructuras implementados en casi dos tercios, un 66%, de las organizaciones auditadas, todavía existen muchas deficiencias. De las instituciones auditadas, en un 46% los mecanismos presentaban fallas, en un 44% no existía comité de TI y en un 7% los participantes del comité no poseían el perfil adecuado al rendimiento de las actividades. Del análisis de estas tendencias se concluye que existen problemas en la mayoría de las organizaciones, 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 organizaciones no poseían un proceso implantado de planificación de TI, y que en casi los dos tercios de las instituciones no se producen documentos de planificación estratégica de TI. Se debe destacar que, la ausencia de planes estratégicos deja a las organizaciones sin instrumentos para efectuar seguimiento y apoyo de los proyectos de mediana y larga duración, que comúnmente se generan en el área de TI, lo que provoca la discontinuidad de estos y consecuentemente el gasto innecesario 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 organizaciones. 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 el peor puntuación de las cuatro áreas enfocadas en el 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%; de proceso de continuidad de servicios de TI, con un 54%; y de la designación de responsables del 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 organizaciones auditadas. Además, documentos y procesos esenciales tampoco han sido implantados o elaborados en casi mitad de las organizaciones auditadas, lo que refuerza la necesidad de atentarse 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 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 instituciones evaluadas.

7.7. Ante el escenario presentado, se advirtió que la situación de la gobernanza de TI en las organizaciones públicas de los países miembros de la Olacefs es bastante heterogénea en diversos aspectos. Además, de las diferencias naturales entre los diversos países participantes de la auditoría, el tema contratación de TI 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. 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 organizaciones 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 de los hallazgos más significativos encontrados en este trabajo, presentados en la tabla abajo.

Hallazgos	%
Ausencia del comité de TI	44
Inexistencia del proceso de planificación de TI	39
Ausencia de documentos de planificación estratégica de TI	63
Ausencia de monitoreo sobre el proceso de contratación de TI	39
Ausencia de aprobación y publicación del PCN	59
Ausencia de aprobación y publicación del proceso de continuidad de servicios de TI	54
Ausencia de la designación de responsables de la gestión de seguridad de la información	51
Ausencia del proceso de gestión de riesgos	49
Ausencia del proceso de inventario de activos	46
Ausencia del Comité de Seguridad de la Información	46
Ausencia de aprobación y publicación de la Política de Seguridad de la Información	46
Ausencia de aprobación y publicación de la Política de Control de Acceso	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 para los países y para 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 labores han sido coordinadas por André Luiz Furtado Pacheco, con la colaboración de Carlos Alberto Mamede Hernandes y Clayton Ferreira da Silva. La revisión de este informe y supervisión de los trabajos ha estado a cargo de Antônio Daud Júnior. El seguimiento y soporte administrativo ha estado a cargo de José Roberto Valentin y Luciana Rodrigues Tolentino.

9.2. Las 41 auditorías han sido realizadas por 52 auditores de 11 diferentes Entidades de Fiscalización Superior:

Bolivia	Erick Quintanilla Martínez
	Fernando Oropeza Núñez
	Renato Ampuero Beltrán
	Zulma Heredia Poma
Brasil	Alessandro de Araújo Fontenele
	Antônio Carlos Merlim
	Carlos Alberto Tanaka
	Erick Muzart Fonseca dos Santos
	Eules Leonardo Santos Lima
	Geraldo Marcio Rocha de Abreu
	Helder Wanderley Sasaki Ikeda
	Jorge Tawaraya
	Klaus Felinto de Oliveira
	Luiz Geraldo Santos Wolmer
	Marcio Rodrigo Braz
	Marcos Roberto Medeiros
	Rafael Albuquerque da Silva
	Robinson Araujo da Frota
	Rodrigo Machado Benevides
	Rosa Virgínia da Silva Rêgo

	Tibério Cesar Jocundo Loureiro
Chile	Jean Paul Thibaut Verdugo
	Ricardo Muñoz Ortega
	Víctor Garcés Almonacid
Costa Rica	Gino Ramírez Solís
	Grettel Camacho Aguilar
	Manolo Córdoba Pérez
Ecuador	Adrian Arturo Castillo Granda
	Darwin Xavier Paillacho Corredores
	Jairo René Navarro Bustos
	Mariuxi Geovanna Tituaña Dávila
	Wilfrido Rigoberto Rosero Álvarez
El Salvador	Cecília Isabel Escobar Flamenco
	Conchamarina Rivas Magaña
	Mario Rafael Alberto Fuentes
	Ricardo Ernesto Flores Ramos
Guatemala	Guillermo Baldomero de León Sosa
	Richard Granja Guzmán
	Rosalina Francisca Arreaga Santizo
Honduras	Carlos Roberto Silva Sánchez
	Everth Raúl Gutiérrez Soriano
	Karla Janeth Escobar Gómez
Panamá	Doris del C. Tello Rodríguez
	Itsmaosgama Alvendas Velásquez
Paraguay	José Arzamendia Alarcón
	Mabel Elizabeth Arriola de Granada
Perú	Carlos Martín Verástegui Pereira
	Enrique Miguel Bardón Matos
	Leoncio José Rodríguez Manyari
	Luis Ángel Espinal Redondez
	Miguel Ángel Solano Baldeón
	Raúl Alberto Valle Ruiz

10. Agradecimientos

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

10.2. Al Banco Interamericano de Desarrollo (BID) por el apoyo financiero para la realización de la auditoría.

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

10.4. A las Áreas Internacionales de las demás Entidades de Fiscalización Superior que han apoyado en la realización de las actividades de esta auditoría coordinada de TI.