ESTANDARIZACIÓN COBIT PARA EL CONTROL DE TECNOLOGÍAS INFORMÁTICAS (TI) DEL GOBIERNO DE CATAMARCA

Maria A. Barrera[1] ,Carolina I. Chayle[1] [2] ,Claudia M. Herrera [1] , Andrea Rosatto (1)

[1] *Facultad de tecnología y Ciencias Aplicadas. Maximio Victoria 55. Catamarca*
[2] *Facultad de Ciencias de la Salud. Maestro Quiroga S/N 1ra. C. Catamarca*
maritabarrera@arnet.com.ar & cchayle@salud.unca.edu.ar

CONTEXTO

Las integrantes del proyecto se encuentran en la etapa de desarrollo de sus tesis de posgrado en el marco de la carrera de maestría en Ingeniería del Software en temas específicamente relacionados al área del proyecto: Standares de Auditoria en ámbitos gubernamentales, Proyectos de Risk Management y Gobierno electrónico, todos aplicados en el gobierno de la provincia de Catamarca.
Además, la Lic. María Alejandra Barrera y la Lic. Claudia Mabel Herrera son docentes de la cátedra de Auditoria de la carrera Ingeniería en Informática de la Facultad de Tecnología y La Lic. Carolina Irene Chayle es docente de la cátedra de Calidad de Software de la carrera Ingeniería en Informática de la Facultad de Tecnología, ambas cátedras están ligadas estrechamente al tema en cuestión. Andrea Rosatto es alumna de la carrera de Ingeniería en Informática y se encuentran en etapa de desarrollo de su tesina de grado investigando sobre Auditoria Web. Un modelo de implementación para la evaluación de calidad del sitio Web de la Municipalidad de San Fernando del Valle de Catamarca.
Así mismo es prioritario para el Departamento de Informática de la Facultad de Tecnología y Ciencias Aplicadas de la UNCa, transferir soluciones concretas a las problemáticas que se plantean a los profesionales y a los organismos provinciales, en relación con el aseguramiento de la calidad y evaluación de los riesgos de las TI, para garantizar la seguridad de la información y prevenir las posibles contingencias en el uso de TI.

RESUMEN

El vertiginoso avance tecnológico ha incrementado cada vez más la dependencia de las tecnologías de información (TI) en las organizaciones, el crecimiento de este fenómeno aumenta también los riesgos informáticos a los que se enfrentan. La adopción de estándares de control de TI son actualmente utilizados a nivel mundial y proporcionan a las organizaciones que los aplican un mejoramiento en el aseguramiento de la información y de los activos informáticos, mediante la actualización de sus procesos. Sin embargo, es confusa la implementación de buenos controles de TI por parte de entidades comerciales, sin fines de lucro o gubernamentales. En el caso de entidades públicas es menester comprender su enfoque global de funcionamiento para poder focalizar los aspectos sustantivos de una reforma aplicable a cualquier nivel de Estado. A nivel nacional, la información muestra que pocas provincias han establecido las bases para evaluar los riesgos de TI en ámbitos gubernamentales. En el presente proyecto se busca evidenciar esta necesidad, suministrando los lineamientos a seguir para la aplicación del Standard COBIT, como herramienta de control de TI en el ámbito del Gobierno de la Provincia de Catamarca.

Palabras clave: Tecnologías de Información; Riesgos informáticos; Auditoría Informática; Standard COBIT; Sistemas de Control de Información.

1. INTRODUCCION

Las empresas públicas y privadas están valorando cada día más la creciente importancia que representa mantener sistemas informáticos seguros, confiables y confidenciales, que eviten o prevengan la ocurrencia de errores u operaciones ilegales a partir de debilidades en los sistemas de control.
El aseguramiento de la información es la base sobre la que se construye la toma de decisiones de una organización. Sin aseguramiento, las empresas no tienen certidumbre de que la información sobre la que sustentan sus decisiones sea confiable, segura y esté disponible cuando se la necesita. Muchas organizaciones reconocen estos beneficios potenciales, y por eso, las organizaciones exitosas comprenden y administran los riesgos asociados con la implementación de esta tecnología. Por lo tanto, los administradores deben tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de TI para proporcionar la dirección efectiva y los controles adecuados a los fines de decidir la inversión

razonable en seguridad y control, tratando de lograr un balance entre riesgos e inversiones en ambientes de este tipo, frecuentemente impredecibles.

El sector público no queda aislado de esta problemática, por lo que necesita definir una estrategia general de desarrollo informático, fundamentalmente para obtener información oportuna y veraz, tanto en su faz operativa como gerencial.

Tal estrategia implica uniformar criterios y estandarizar las actividades del Estado bajo un mismo enfoque. Este hecho es fundamental para planificar racionalmente las acciones tendientes a cumplir con la agenda de gobierno, para tomar decisiones al más alto nivel y a su vez, mejorar la gestión de las organizaciones haciéndolas más eficaces y eficientes en el cumplimiento de sus metas.

Existe una creciente necesidad de las organizaciones en cuanto a la seguridad en los servicios de TI a través del control y la auditoría. Sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc., y en consecuencia, los usuarios necesitan una base general a ser establecida como primer paso.

En este sentido, CObIT (Control Objectives for Information and related Technology) complementa a los modelos más generales como COSO (EEUU), CoCo (Canadá) o Cadbury (Inglaterra) y ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona "prácticas sanas" a través de un marco referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica. Dichas prácticas aspiran a optimizar el uso de los recursos disponibles, es decir, personas, instalaciones, tecnologías, sistemas de aplicación y datos, definiendo el marco de trabajo y el entorno tecnológico adecuado. (1)

Es importante mencionar aquí lo que sostiene el CObIT para organismos gubernamentales (2). El mismo define cuatro dominios para agrupar procesos de TI, concebir responsabilidades en una estructura organizacional y encuadrar los mismos según su ciclo de vida aplicable o su ciclo de administración. Tales dominios incluyen:

- Planificación y Organización: Vincula la identificación de la forma en que la Tecnología de Información puede contribuir más adecuadamente con el logro de los objetivos del gobierno. Precisa, planifica, comunica y administra la realización de la visión estratégica de Tecnologías de Información. Define una correcta organización e infraestructura tecnológica.
- Adquisición e Implementación: Identifica, desarrolla o adquiere soluciones de Tecnologías de Información, y luego las implementa e integra a los procesos del gobierno. Incluye cambios y mantenimiento de sistemas existentes para garantizar su ciclo de vida.
- Entrega y Soporte: Cumple con la prestación efectiva de los servicios requeridos, que comprenden desde operaciones tradicionales, aspectos de seguridad y continuidad de servicios hasta la capacitación. Incluye el procesamiento real de los datos por los sistemas de aplicación.
- Monitoreo: Evalúa los procesos de Tecnologías de Información a medida que transcurre el tiempo para determinar su calidad y el cumplimiento de los requerimientos de control.

El monitoreo incluye la descripción de la regulación de las mejores prácticas de Auditoría en Informática, como así también, la definición de cómo administrar los riesgos de TI en el sector público en base a los estándares establecidos por organismos nacionales e internacionales.

En la República Argentina, puede señalarse que muy pocas provincias han intentado establecer las bases para evaluar los riesgos de TI en ámbitos gubernamentales. En la Provincia de Catamarca, el órgano rector de la seguridad y control de TI, es la recientemente creada Dirección Provincial de Gestión de la Información, que aún no ha establecido las normas necesarias para definir los estándares comunes a todas aquellas tareas que implican el uso de las mismas.

A los fines de garantizar la seguridad de la información y prevenir las posibles contingencias en el uso de TI, se propone asegurar la confidencialidad, confiabilidad y disponibilidad de los datos en el gobierno de la Provincia de Catamarca, a través de la aplicación del Standard CObIT. Para ello, se analizarán los distintos parámetros rectores y su mejor adaptación al manejo de TI en el ámbito específico del gobierno provincial, a los efectos de proporcionar los lineamientos a seguir para una aplicación exitosa de dicho estándar.

1) COBIT Marco, Comité de Dirección COBIT y la Information Systems Audit and Control Foundation, Buenos Aires, 1998.)

2) COBIT, Gobernabilidad, Control y Auditoría de Información y Tecnologías Relacionadas, Information Systems Audit and Control Foundation,

Edición Especial para Organismos Gubernamentales, Buenos Aires, 1998.

2. LINEAS DE INVESTIGACION Y DESARROLLO

Ingeniería del Software: Auditoria y Control de Tecnologías informáticas

3. RESULTADOS ESPERADOS y OBTENIDOS

En la Provincia de Catamarca, al igual que en la mayoría de las provincias argentinas, no se han establecido aún las bases para evaluar los riesgos de TI en ámbitos gubernamentales.
Sin información segura, confidencial, confiable y accesible, difícilmente el Gobierno Provincial pueda planificar racionalmente sus acciones. La aplicación de una adaptación adecuada del Standard CObIT para garantizar la seguridad de la información y prevenir las posibles contingencias en el uso de TI, permitirá mejorar la gestión de las organizaciones gubernamentales de Catamarca, haciéndolas más eficaces y eficientes en el cumplimiento de sus metas. La definición y aplicación de normas de Riesgos y Auditoria de TI en el ámbito del Gobierno de la Provincia de Catamarca, producirá un impacto positivo y tangible en los procesos de toma de decisión que requieren de información, tal como diversos antecedentes en el mundo y en la región lo demuestran.
El control de riesgos y seguridad en el manejo de TI, proporcionará al Gobierno de la Provincia de Catamarca la herramienta necesaria para planificar racionalmente sus acciones sobre bases más confiables. Dicho control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración pública provincial.
El control interno de calidad de información permitirá optimizar el empleo de los recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos.
La adaptación de tales estándares para el manejo de TI en el ámbito específico del gobierno provincial, no sólo permitirá minimizar los riesgos y aumentar la seguridad en el manejo de TI, sino además, contribuirá a fijar los lineamientos a seguir en distintas provincias argentinas para garantizar mejores prácticas de manejo de datos en las esferas gubernamentales.

Resultados obtenidos

- Definición del Proceso de Administración de los Riesgos y Auditoria de TI en el ámbito del Gobierno de la Provincia de Catamarca.
- Establecimiento de las pautas a seguir en la aplicación del Standard CObIT para garantizar la seguridad de la información y prevenir las posibles contingencias en el uso de TI por parte del Gobierno de la Provincia de Catamarca.
- Selección de criterios adecuados de evaluación de riesgos de TI.
- Definición de procedimientos a seguir en cada fase del proceso de administración de los riesgos de TI.
- Proporcionar normas de Riesgos y Auditoría de aplicación en el manejo de la información del Gobierno de la Provincia de Catamarca.
- Formación de recursos humanos en administración de riesgos y auditoria en TI.

4. FORMACION DE RECURSOS HUMANOS

El programa de capacitación y formación de recursos humanos, contempla las siguientes actividades:

- Incorporación de alumnos de los últimos años de la carrera de Ingeniería en Informática de la Facultad de Tecnología y Ciencias Aplicadas de la UNCa., en calidad de auxiliares de investigación.
- Dirección de tesinas de grado de la carrera de Ingeniería en Informática de la Facultad de Tecnología y Ciencias Aplicadas de la UNCa. En este sentido la alumna e integrante del equipo del proyecto: Andrea Rosatto, se encuentra en etapa de elaboración del Trabajo Final de la carrera de Ingeniería en Informática denominado: Auditoria de Artefactos Web. Caso de Estudio: Pagina Web de la Municipalidad de San Fernando del Valle de Catamarca
- Participación de los integrantes del proyecto en cursos de actualización y posgrado en el área de estudio.
- Participación en talleres o workshops de herramientas informáticas relacionadas con el control y auditoría de TI.
- Celebración de convenios con entes estatales, como la Dirección Provincial de Gestión de la Información de la Provincia de Catamarca, la Municipalidad de la Capital y otras universidades, para capacitación de los recursos humanos en las herramientas normalizadas.
- Dictado de cursos de capacitación diseñados según demanda de la propia

Administración, con el objeto de transmitir las mejores prácticas a los agentes públicos asistentes.

Para garantizar la capacitación y actualización del equipo de investigación, así como la difusión de los avances y resultados logrados, se propuso la participación en eventos nacionales e internacionales de la especialidad, como congresos, simposios, seminarios y cursos.

5. BIBLIOGRAFIA

- COBIT Marco, Comité de Dirección COBIT y la Information Systems Audit and Control Foundation, Buenos Aires, 1998.
- COBIT, Gobernabilidad, Control y Auditoría de Información y Tecnologías Relacionadas, Information Systems Audit and Control Foundation, Edición Especial para Organismos Gubernamentales, Buenos Aires, 1998.
- COSO [Committee of Sponsoring Organisations of the Treadway Commisssion Internal Control-Integrated Framework, 1992]
- Prince, A. *Gobierno Digital, Primer Foro Gobierno Digital en Argentina,* Buenos Aires, Julio 2000.
- Herrera Cognetta, A. & M. A., Castro, Las TIC en la Administración Pública de Jujuy, *Investigaciones Docentes en Ingeniería*, Vol II, 987-9170-60 1, 580-585, 2006.
- *http://www.isaca.org, 2007.*
- ISO/IEC TR 13335 - Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 8.1.6.
- Piattini, M & E. del Peso, *Auditoria Informática. Un enfoque práctico,* Ed Alfaomega, Mexico 2005.
- Echenique Garcia, J. A., *Auditoria en Informática,* Ed. McGraw-Hill, Mexico 2004.
- Alvarez, B. R. & A. R., Garnacho, *Avances en Criptología y Seguridad de la Información,* Ed. Diaz de Santos, España, 2004.
- Izquierdo Duarte, F., Administración de Riesgos de TI, IX Encuentro Nacional y IV Iinternacional de Control Interno 2003.
- Herrera Cognetta, A. & M. A., Castro, Las TIC en la Administración Pública de Jujuy, Investigaciones Docentes en Ingeniería, Vol II, 2006.
- http://www.isaca.org, 2007.
- The Australian/New Zealand Joint Standards Committee AS/NZS 4360 Risk Management