Estándares de Seguridad Informática

Por: Anagraciel García Soto, José Luis Sandoval Días.
01/11/2009

Conceptos de Estándares de Seguridad Informática.

1. Estándar: Especificación que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.; y que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad (Anónimo, 2009).
2. Estándar de Seguridad Informática: Son conjunto de buenas prácticas en seguridad de la información en base a otros modelos de gestión (Anónimo, 2005).
3. Estándar COSO-SOX: (Committee of Sponsoring Organizations of the Treadway Commission). El informe COSO, es el resultado de la investigación de un grupo de trabajo integrado por la Comisión Treadway con el objetivo de definir un nuevo marco conceptual de Control Interno capaz de integrar las diversas definiciones y conceptos que se utilizan sobre este tema (Federico Iturbide (2005).

   Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos.

   Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

   En sentido amplio, se define como un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

   - Eficacia y eficiencia de las operaciones.
   - Confiabilidad de la información financiera.
   - Cumplimiento de las leyes y normas aplicables.
4. Estándar COBIT: Control Objectives for Information and related Technology: ofrece un conjunto de mejores prácticas para la gestión de los Sistemas de Información de las organizaciones, con el objetivo principal de proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos (Marble, 2008).
5. Estándar ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable (Anónimo, 2005).
6. Estándar CMM: Es el estándar de modelo de madurez de capacidades, describe un continuo de cinco etapas basado en que tan bien la organización se apega a procesos comunes y repetibles para realizar el trabajo. El nivel más bajo de la escala describe a compañías sin procesos repetibles, en donde mucho del trabajo es caótico y ad-hoc. El nivel más alto, describe a organizaciones que usan procesos definidos y repetibles, obtienen métricas que contribuyen a la mejora continua de sus procesos y que están en búsqueda de hacer las cosas mejor de manera continua (Anónimo).

   El CMM fue desarrollado de 1984 a 1987 por Watts Humphrey y el Instituto de Ingeniería de Software (SEI). El SEI es parte de la Universidad Carnegie Mellon; CMM es fondeado por el Departamento de Defensa de los Estados Unidos (DoD).

El CMM contiene cinco etapas para evaluar que tan sofisticada es una organización en el establecimiento y apego a procesos estándares.

Certificaciones:

COSO-SOX:

Los requisitos más importantes que exige la nueva ley son los siguientes:

- Establecer un nuevo consejo de vigilancia, supervisado por la SEC (Security Exchange Commision - Comisión de Valores de Estados Unidos).
- Definir nuevas funciones y responsabilidades para el comité de auditoría, que debe tener miembros independientes a la administración.
- Nuevas reglas para la conformación de los Consejos de Administración, para que incluyan personas ajenas al grupo de control de la empresa.
- Que los directivos acompañen los reportes con una certificación personal, en general se incrementan las responsabilidades de los directores generales y de los directores de finanzas.
- Código de ética para los altos funcionarios de la organización.
- Definir un esquema de medición del control interno que se aplique constantemente.
- Que los directivos certifiquen el buen funcionamiento de sus sistemas de control interno.
- Establecer nuevos requerimientos de información, que abarcan cuestiones no financieras y financieras que no aparecen en los estados respectivos.
- El auditor externo tiene que verificar la certificación del control interno y emitir un dictamen al respecto.
- Rotación de los auditores cada cinco años.
- Especificar los servicios que no podrán ser realizados por los auditores externos.
- Reforzar penas por fraudes corporativos y de personal administrativo.
- Emitir reglas sobre conflictos de interés.

- Nuevos esquemas de administración de riesgos.
- Aumentar la autoridad y funciones de la SEC.

CMMI,COBIT Y ITIL:

Personal de soporte de TI, Consultores de TI, Usuarios clave de negocio, Gerentes y administradores de TI y auditores, Prácticantes, Firmas que proveen servicios de administración de TI. Cada estudiante recibirá un manual que comprenderá las diapositivas usadas en el curso, versión 2.0, un examen ejemplo y definiciones clave.

ISO 2700 Y 2000:

- Pequeñas y medianas empresas.
- Otras Entidades sin fines de lucro legalmente constituidas, que presten servicios de asesoramiento y apoyo a la innovación en las PYME.
- Agrupaciones o asociaciones empresariales en las que participen PYME.

Los proyectos deberán involucrar a un conjunto de PYME, en número igual o superior a seis e igual o menor a 20 PYME.
En caso de que un mismo solicitante tenga más PYME a certificar, deberá presentar una nueva solicitud respetando los máximos y mínimos anteriores.

Los proyectos presentados deberán incluir la realización, entre otras, de las siguientes tareas:

- Diagnóstico previo de la gestión del servicio TI o gestión de la seguridad de la información en cada una de las PYME interesadas.
- La definición de los programas de mejora a llevar a cabo a fin de obtener la certificación correspondiente.
- La implantación de los procesos de mejora previos a la obtención de la certificación y la propia obtención de esta.

Cada proyecto presentado, incluyendo a un número mínimo de seis PYME, deberá orientarse a sólo una de las tres acciones antes indicadas (calidad del software, gestión del servicio TI y gestión de la seguridad de la información), no pudiendo incluirse en la misma solicitud diferentes tipos de certificación para PYME.

Referencias.

1. Anónimo (2009). Glosario de Seguridad Informática parte II. Consultado en Julio, 2009 en http://www.taringa.net/posts/info/2054049/Recopilaci%C3%B3n---Glosario-de-Seguridad-Informatica-PARTE-II.html.
2. Anónimo (2005). Otros Estándares. Consultado en Julio, 2009 en http://www.iso27000.es/otros_estandar.html.
3. Marble (2008). Cobit, Estándar para el Buen Gobierno de los Sistemas de Información. Consultado en Julio, 2009 en http://www.marblestation.com/?p=645.
4. Anónimo (2005). El Portal de ISO 27000 en Español. Consultado en Julio, 2009 en http://www.iso27000.es/glosario.html#I.
5. Anónimo (). Modelo de Madurez de Capacidad. Consultado en Noviembre, 2009 en http://www.tenstep.com.mx/Paso0.0.1.1.asp.

6. Federico Iturbide (2005). Ley Sarbanes-Oxley Act. Consultado en Noviembre, 2009 en http://www.economiaynegocios.uahurtado.cl/peee/pdf/Ley%20Sarbanes%20Oxley%20Federico%20iturbide.pdf.
7. IT INSTITUTE Advanced Information Tecnology Center (). COBIT. Consultado en Noviembre, 2009 en http://it-institute.org/index.php?option=com_content&task=view&id=33&Itemid=41&gclid=CP3K27-Ao54CFSWjagodZQ8elA.
8. Víctor Manuel Tascón (2009). Subvenciones Certificación ISO 27001, ISO 20000, CMMI. Consultado en Noviembre, 2009 en http://derechodelastics.blogspot.com/2009/03/plan-avanza-2-subvenciones.html.