Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, núm. 2-5, 2022, pp. 1-7.

Análisis de los modelos de gestión de Ciberseguridad en la elaboración de planes de concientización y capacitación para Contadores Públicos.

Diego Sebastian Escobar.

Documentos de Ciberseguridad

Análisis de los modelos de gestión de Ciberseguridad en la elaboración de planes de concientización y capacitación para Contadores Públicos

Diego Sebastián Escobar

Profesor Adjunto de Tecnología de la Información. Universidad del Salvador.

Introducción

El objetivo del presente artículo es identificar y sintetizar los modelos de gestión de ciberseguridad y su vinculación con los modelos de capacitación para profesionales en Ciencias Económicas en general y Contadores Públicos en particular.

Diciembre de 2022

Modelos de gestión generales

Considerando las normas vigentes y establecidas por el BCRA, la IGJ y la AAIP, cada una de ellas impactan en la planificación, gestión y control de los activos de información.

Para ello es recomendable la implementación de buenas prácticas y estándares para contribuir a una eficiente administración de los sistemas en las organizaciones; entre los que se destacan:

Estándares de análisis de Seguridad de la Información

Estándares y buenas prácticas	Activos de información en custodia de la entidad					
	N1 – Procesos	N2 – Documentación en papel	N3 – Repositorios de archivos y bases de datos	N4 – Plataforma de Software	N5 – Plataforma de Hardware	N6 – Sitios físicos
IRAM/ISO 9001	X	X				
COBIT 5	X			X	X	
Informe COSO	X	X				
IRAM/ISO/IEC 27001	X	X	X	X	X	X
PCI-DSS		X		X		
ITIL	X			X		

Fuente: Elaboración propia.

En el siguiente cuadro comparativo se analizan los modelos de gestión mencionados precedentemente.

Análisis de los Modelos de Gestión de la Seguridad de la información y capacitación de los usuarios.

Modelos de Gestión de la Seguridad de la información			
Nombre	**Difusión**	**¿Adapta a la gestión?**	**Características**
Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security"	Alta	SI	Toma como ejes fundamentales en la gestión de la seguridad a las personas, procesos, tecnologías y organización del ente.
Modelo IRAM/ISO/IEC 27.001	Alta	SI	Establece los lineamientos para implementar un Sistema de Gestión de la Seguridad de la Información.
COBIT	Alta	SI	Está dirigida a la gestión de tecnología de la información (TI).
Modelo Information Security Management Maturity Model (ISM3)	Baja	SI	Se orienta exclusivamente a los sistemas de gestión de calidad IRAM/ISO 9.001.
Modelo Information Security Forum's Standard of Good Practice (SOGP).	Baja	NO	Se basa en buenas prácticas y en las experiencias del ISF (El Foro de Seguridad de la Información).
Modelo ITIL	Media	SI	Se basa en la gestión de los procesos de TI.
Modelo Prince2	Baja	SI	Se orienta a la seguridad relacionada con la gestión de proyectos.

Modelo TLLJO	Baja	NO	Se basa en la implementación de un SGSI, pero permitiendo un mayor control sobre el sistema de costos.
Norma SP800-53 del NIST	Media	SI	Fue tomada como base para la confección de la citada Comunicación “A” 5374/6017 del BCRA.

Fuente: Elaboración propia.

Para el cumplimiento de todas las normas analizadas se establece la necesidad de adoptar procedimientos para administrar eficientemente la Seguridad de la Información en las organizaciones.

Relación de los modelos de gestión y los planes de capacitación y concientización

Para poder proteger a los activos de información en conocimiento de los empleados, proveedores y clientes de las organizaciones se plantea la necesidad de definir la gestión de la capacitación y concientización en Ciberseguridad.

En el desarrollo del plan se debe establecer el nivel de madurez que cuenta la entidad y utilizar un modelo de gestión de la capacidad adecuado a la misma. Basándose en la necesidad de resguardar los datos sensibles, las entidades deben analizar los riesgos si los usuarios no reciben la capacitación adecuada para un óptimo cuidado de la información.

A continuación, se analizan los modelos de madurez y los modelos difundidos para gestionar la capacitación y concientización en seguridad:

Modelos de madurez cultural de la Seguridad de la Información

Modelos de madurez cultural de la Seguridad de la Información			
Nombre	**Difusión**	**¿Se adapta a gestión?**	**Características**
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITII-SEM)	Alta	SI	Se centra en la concienciación y adaptación por parte de la organización en seguridad.
Modelo de madurez de COBIT	Alta	SI	Se centra en los procedimientos específicos de auditoría de COBIT
Modelo de Madurez de Seguridad en TI del NIST-CSEAT	Baja	SI	Se orienta a los niveles de documentación en la organización.
Modelo SSE-CMM	Media	SI	Se basa en la madurez en la ingeniería de seguridad y diseño de software.
Modelo de CERT/CSO	Baja	NO	Se centra en la medición de la calidad relativa a niveles de documentación.
Modelo de Madurez de la Gestión de la Seguridad Informática (MMAGSI)	Baja	SI	Se basa en “La quinta disciplina” de Senge P. (1992).

Fuente: Elaboración propia.

Luego de haber analizado los modelos de evaluación de la madurez y de gestión de la capacitación en la seguridad de la información, se puede destacar que el Modelo CITII-SEM es el único que se centra en concientización en la seguridad, y el modelo de COBIT se centra en los procedimientos específicos de auditoría, lo que permitiría complementarlo con otras normas y actividades de control, por lo tanto, el CITII-SEM es el que más se orienta en la implementación de programas de concientización.

En el análisis de la cultura organizacional se deben tener en cuenta a los usuarios internos y externos para el armado de los contenidos y los programas en concientización de la Seguridad de la Información. Asimismo, resulta necesario que los mismos se encuentren alineados a las estrategias del negocio, así como contar con la colaboración y apoyo de la alta dirección.

Bibliografía

National Institute of Standards and Technology. (10 de Octubre de 2019). *NIST SP 800-12 - An Introduction to Computer. Security: The NIST Handbook.* Obtenido de National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Tesoro, J. (1998). *Estado de la Cultura Informativa.* Bahía Blanca: Universidad Nacional del Sur.

Saroka, R. (17 de abril de 2020). *Sistema de Información.* Obtenido de Biblioteca de la Funcación OSDE: http://www.fundacionosde.com.ar/pdf/biblioteca/Sistemas_de_informacion_en_la_era_digital-Modulo_I.pdf

Escobar, D. S. (2010). Ley de Protección de Datos Personales. *Revista Imagen Profesional de La Federación Argentina de Consejos Profesionales en Ciencias Económicas*, 22-24.

Escobar, D. S. (2013). *SEGURIDAD INFORMÁTICA EN LOS SISTEMAS CONTABLES: Un análisis de los aspectos legales, normativos y tecnológicos de la Seguridad de la Información en el almacenamiento, procesamiento, control y resguardo de los Registros Contables.* Buenos Aires: Facultad de Ciencias Económicas. UBA.

Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. *XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL* (págs. 40-50). San Fernando del Valle de Catamarca: UNIVERSIDAD NACIONAL DE CATAMARCA.

CitiGroup. (2018). *Modelo de Evaluación de la Seguridad de la Información de Citigroup.* Buenos Aires: Grupo Citibank.

Information Systems Audit and Control Association. (06 de Septiembre de 2019). *Objetivos de Control para Información y Tecnologías Relacionadas.* Obtenido de (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association): www.itgi.org

The International Systems Security Engineering Association (ISSEA). (20 de octubre de 2019). *SSE-CMM - Systems Security Engineering Capability Maturity Model.* Obtenido de Carnegie Melon University: www.ssecmm.org

CXO Media Inc. (01 de Octubre de 2019). *CERT Security Capability Assessment Tool.* Obtenido de Carnegie Melon University: www.csoonline.com/surveys/securitycapability.html

Senge, P. (1992). *La Quinta Disciplina.* Barcelona: Granica.

Senge, P., Ross, R., Smith, B., Roberts, C., & Kleiner, A. (2004). *La Quinta Disciplina en la Práctica.* Buenos Aires: Granica.

Villegas, M. (2008). Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades. *Trabajo de Grado para optar a la Magíster en Ingeniería de Sistemas*. Caracas, Venezuela: Universidad Simón Bolívar.

Villegas, M., Orlando, V., & Walter, B. (2009). Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizacion es Inteligentes. *Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, Energy and Technology for the Americas: Education, Innovation, Technology and Practice.* Venezuela: LACCEI.

Tipton, H., & Krause, M. (2005). Information Security Management Handbook. En H. Tipton, & M. Krause, *Social Science, Psychology, and Security Awareness: Why?* Editorial AUERBACH.

Tipton, H., & Krause, M. (2005). Attitude Structure and Function: The ABC's of the Tripartite Model. En H. Tipton, & M. Krause, *Information Security Management Handbook.* Editorial AUERBACH.