COMPARACIÓN DE MODELOS TRADICIONALES DE SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE EDUCACIÓN

COMPARISON OF TRADITIONAL MODELS OF INFORMATION SECURITY FOR EDUCATION CENTERS.

Recibido: 09/06/2018 – Aceptado: 22/08/2018

Elva Gioconda Lara Guijarro
Docente - Instituto Tecnológico Superior Central Técnico
Quito – Ecuador
Magister en Tecnologías de la Información Mención en Seguridad de Redes y Comunicaciones
elglarag@gmail.com
https://orcid.org/0000-0003-3025-4792

Flavio Aníbal Corella Guerra
Docente - Instituto Tecnológico Superior Central Técnico
Quito – Ecuador

Magister en Educación
facorellag@gmail.com

Como citar este artículo:

Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

Resumen

En la actualidad existen diferentes modelos de seguridad informática, en los cuales se puede basar una empresa para aplicarlos en sus redes de datos. Al utilizar un estándar adecuado se consigue un esquema acorde a las necesidades empresariales y se puede forzar políticas de seguridad que beneficiarán a la institución el momento de enviar los datos por una red jerárquica. El estudio desarrollado se basó en un análisis del estado del arte sobre esta temática y a partir de ello se determinaron las características principales de cuatro modelos de seguridad informática que dominan el mercado en la actualidad, como son: OSSTMM3, ISO 27001, NIST y COBIT 5, para luego hacer un cuadro comparativo de dichas características, con la finalidad de encontrar la mejor opción que pueda ser utilizada en los centros de educación. El estudio demostró que un modelo de seguridad es la presentación formal de una estrategia de seguridad y que debe identificar el conjunto de reglas y prácticas que regulan como un sistema maneja, protege y distribuye la información delicada. Se recomienda la utilización de los mismos, de acuerdo con el tipo de datos con los que se esté trabajando. El objetivo del presente trabajo es determinar las mejores prácticas de seguridad que serán utilizadas de acuerdo a la necesidad de la empresa, tomando en cuenta que no todas tienen las mismas necesidades para el envío de la información.

Palabras Clave: *modelos de seguridad informática; OSSTMM; NIST; ISO 2701.*

Abstract

At present there are different models of computer security, on which the company can be based to apply them in their computer or data networks. By using an adequate standard, a scheme according to business needs is achieved and security policies can be forced, which would benefit the institution when sending data through a hierarchical network. The study developed was based on the realization of a state of the art on this subject and from it the main characteristics of four computer security models that dominate the market in our days are analyzed, such as: OSSTMM3, ISO 27001, NIST and COBIT 5, to then make a comparative table of these characteristics, in order to find the best option that can be used in education centers. The study showed that a security model is the formal presentation of a security strategy and that it must identify the set of rules and practices that regulate how a system manages, protects and distributes sensitive information. It is recommended to use them, according to the type of data you are working with. The objective of this paper is to determine the best security practices that will be used according to the company's need, taking into account that not all of them have the same needs for sending the information

Keywords: *computer security models; OSSTMM; NIST; ISO 2701.*

Introducción

Actualmente, las redes informáticas resultan ser indispensables al momento de compartir recursos, sean estos físicos (como impresoras, almacenamiento, etc.) o lógicos (archivos generados digitalmente, o documentos digitalizados). El avance de las tecnologías de internet prácticamente ha hecho desaparecer las distancias entre las ubicaciones físicas de los distintos departamentos y/o sucursales de una institución, por lo que, toda comunicación que utilice una red informática como medio, debe realizarse de manera segura. De esta manera se puede conseguir que la documentación sensible no llegue a manos de personas inescrupulosas que puedan hacer daño o conseguir beneficio de ello. En la actualidad, la información es a la vez insumo y producto terminado, lo que ha llevado a varios sociólogos afirmar que se vive en una "era de la información", ésta se ha convertido en el bien más preciado de las empresas, cualquiera que sea su actividad. Por todo lo detallado, se han desarrollado diversos modelos o estándares que proporcionan guías para garantizar la seguridad de la información.

Materiales y Métodos

La metodología empleada se basa en el análisis documental de los referentes teóricos de los modelos o estándares de seguridad con vistas a revelar su desarrollo histórico y contradicciones, así como los principales resultados obtenidos en el análisis comparativo de lasa diferentes publicaciones hechas por Internet. Se han analizado documentos relacionados con resultados de proyectos de investigación asociados al resultado principal, se realizó una revisión bibliográfica en la base de datos obtenida con software adicional y palabras claves, en el título de los artículos. La búsqueda correspondió al período 2005-2018, por lo que se encontró muchas referencias. Se revisaron más profundamente las siguientes:

- Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final.
- Aplicación de una metodología de seguridad avanzada en redes inalámbricas.
- A methodological approach for assessing amplified reflection distributed denial of service on the internet of things.
- Hacking ético basado en la metodología abierta de testeo de seguridad–OSSTMM, aplicado a la Rama Judicial, seccional Armenia.
- Hacia una arquitectura de buenas prácticas de seguridad.
- Modelo de gestión de los servicios de tecnología de información.
- Análisis y estudio de la Universidad Politécnica Salesiana en base a COBIT 5.
- Un proceso práctico de análisis de riesgos de activos de información.

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

Después de determinar cuáles son las prácticas principales de los diferentes modelos de seguridad de datos, se determinó algunos que lideran el mercado, para proceder luego a determinar las características esenciales de cada uno de ellos, encontrándose así semejanzas y diferencias que permitan la aplicación de cada uno de ellos en una solución particular, o desarrollar un modelo ad-hoc, mediante la combinación de algunos elementos procedentes de cada modelo estudiado.

Las características relevantes de cada modelo fueron estudiadas, para permitir una rápida comparación entre ellos, y determinar sus aspectos más relevantes. Tomando en cuenta, que las necesidades de las instituciones no son las mismas, sino que están determinadas de acuerdo a los recursos que ellas tienen.

Resultados y Discusión

En el contenido de las organizaciones o instituciones, la gestión de la información se puede identificar como el método que se encarga de todo lo relacionado con el proceso de obtener la información acorde a las necesidades, libre de errores, para la persona indicada, a un coste conveniente, en el tiempo determinado y articulando todas estas operaciones para el desarrollo de una tarea correcta.

Las vulnerabilidades son puntos débiles en la seguridad de un sistema informático, a través de estos se pueden presentar cierto tipo de amenazas que pueden poner en peligro la confidencialidad, integridad y autenticación de los datos.(Milagros and Steven 2017)

Se puede decir que la información es lo más valioso que tiene una empresa o institución y si llega a manos de personas inescrupulosas puede causar daño tanto material como económico, por ello, es de gran importancia la seguridad de la información y la utilización de un modelo adecuado que pueda precautelar todos los datos y la utilización de los mismos. Algunos de los puntos más vulnerables de la seguridad pueden ser: integridad, confiabilidad, confidencialidad y disponibilidad de los datos.

El término seguridad de la información se refiere a la confianza de que la misma no sea accedida por usuarios no autorizados; que siempre esté disponible; que los canales de transmisión no estén comprometidos. Es decir, la seguridad de la información implica que se requiere proporcionar protección a los recursos físicos, así como a los recursos abstractos. La seguridad es una forma de protección contra los riesgos, es un conjunto de pasos o procedimientos en el que se toma en cuenta elementos como aspectos tecnológicos, de gestión organizacionales, de negocios, de tipo legal, de cumplimiento, entre otros. (Bertolín 2008)

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

De manera general, un modelo de seguridad de información es el conjunto de políticas, procedimientos, procesos, y controles, que una empresa adopta para promover la implementación de un sistema de gestión de la información. En la actualidad la gran mayoría de las empresas usan tecnologías de la información para la gestión de sus operaciones, es por ello que se han creado diversos estándares o modelos y su implantación se ha convertido en los últimos años en una necesidad para aquellas instituciones que deseen tener sus datos e información segura.

De acuerdo con cada circunstancia que se presenta en una institución o empresa se puede acoplar los métodos o estándares que existen hoy en día. Se debe recalcar que para cada uno de los inconvenientes que se presenten, hay más de un modelo aplicable para gestionar dichas problemáticas.

Existen varios modelos y estándares para la seguridad de la información, entre ellos se tiene los siguientes:(Triana and Triana 2014)

- Gestión de proyectos con PMBOK (Project Management Institute PMI), es un modelo para la gestión de proyectos en general, se basa en un conjunto de buenas prácticas divididas en 9 áreas de conocimiento subdivididas en actividades (siendo 44 en total) que van desde la gestión del alcance hasta gestión de las adquisiciones. Las partes del marco de trabajo de PMBOK es aplicable de acuerdo con la necesidad de la empresa.

- ITIL (Information Technology and Infraestructure Library), es un estándar para la gestión de los servicios TI, centrado en brindar servicios de alta calidad para lograr la máximo satisfacción del cliente a un costo manejable. Para ello, parte de un enfoque estratégico basado en el triángulo procesos-personas-tecnología.

- El modelo CMMI (Capacity Madurity Model Integrated) es utilizado para medir el grado de madurez de las empresas o instituciones respecto a la aplicación de las mejores prácticas de desarrollo y gestión del software. Este modelo tiene cinco niveles de madurez: inicial, repetible, definido, administrado, optimizado. Por lo general las empresas llegan solo hasta el nivel 3.

- COBIT (Control Objectives for Information and related Technology), estándar utilizado para gestión y control de TI. Está conformado por cuatro dominios organizados en procesos que se subdividen en actividades y objetivos de control.

De todos los modelos o estándares de seguridad de la información disponibles se han elegido: OSSTMM3, NIST SP 800-30, COBIT 5 e ISO 27001, por su presencia y aceptación en el mundo de la informática, se consideran que marcan la pauta a seguir en los distintos aspectos que

conforman un sistema de gestión de la seguridad de la informática.

3.1 OSSTMM3

Es uno de los estándares profesionales más completos y utilizados en Auditorías para analizar la Seguridad de los Sistemas desde Internet, está compuesto de un marco de trabajo que detalla las fases a realizarse para la ejecución de la auditoria. Éste modelo fue creado en 2001 por Pete Herzog, Director Ejecutivo del Instituto para la Seguridad y Metodologías Abiertas, trabajando conjuntamente con 150 personas expertas en el tema, que contribuyeron con conocimiento, experiencia y horas de revisión de este proyecto. (Acosta and Isazaa) Tiene varias versiones que incluyen el desempeño de normas y mejores prácticas como las establecidas en el NIST, ISO 27001 - 27002 e ITIL, por todo lo expuesto, se dice que éste estándar es uno de los más completos en cuanto a la aplicación de pruebas a la seguridad y riesgo de la información en las instituciones. (Valdez Alvarado 2013)

El OSSTMM se concentra en los detalles técnicos de los elementos que deben ser comprobados antes, durante y después de una prueba de seguridad y en la forma de medir sus resultados. Se divide en las siguientes secciones:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las Comunicaciones.
- Seguridad Inalámbrica.
- Seguridad Física.

Más que un modelo de seguridad es una herramienta de análisis de seguridad en las redes. Se la toma en cuenta debido a que provee directrices de pruebas de seguridad, en todos los ámbitos que conciernen a una red de información, desde el nivel físico (incluyendo al elemento humano), hasta el nivel de aplicación. (Herzog 2017).

Su propósito es proveer una metodología científica para examinar la organización, realizando pruebas de seguridad desde adentro hacia afuera. (Vásquez Alvarado 2014)

Provee descripciones específicas para implementar pruebas de seguridad en cada uno de los componentes de una red de información. Un resumen de los ámbitos de injerencia de OSSTM3 en cuanto a las seguridades que puede proporcionar al ser humano o a una red de datos, se puede apreciar en la tabla 1.

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

Tabla 1 Ámbito del manual

Canal	Sección	Descripción
Seguridad física	Humano	Todos los comprometidos con la organización
	Físico	Objetos tangibles de la organización
Seguridad de las comunicaciones	Redes de datos	Sistemas electrónicos y redes de datos
	Telecomunicaciones	Comunicaciones digitales y analógicas
Seguridad el espectro electromagnético	Comunicaciones inalámbricas	Señales electromagnéticas empleadas

Fuente: Vázquez 2014

OSSTMM contempla seis tipos de pruebas, que van desde la intrusión hasta la auditoría guiada, estas son: Blindaje o Hacking ético; Doble blindaje, auditoría de caja negra o pruebas de penetración, de caja gris, de doble caja gris, test tándem o secuencial y prueba inversa. (Vásquez Alvarado 2014)

3.2 NIST SP 800-30

Es una metodología de gestión de riesgo, proporcionada en forma de guía, desarrollada por el departamento de comercio del gobierno de los Estados Unidos. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) implemento la guía: Seguridad de la información para pequeñas empresas, que tiene como objetivo proporcionar recomendaciones de seguridad cibernética básicas para empresas a través de un proceso de evaluación de riesgos. (Nist 2012).

Al proporcionar liderazgo técnico para la infraestructura nacional de medición y estándares, NIST SP 800-30 desarrolla técnicas de prueba, datos de referencia, pruebas de implementaciones conceptuales y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. NIST contiene el desarrollo de normas y directrices técnicas, físicas, administrativas y de gestión para la seguridad y privacidad adecuada de la información delicada no clasificada en sistemas informáticos federales. La publicación especial 800-series informa sobre los esfuerzos de investigación, orientación y divulgación de NIST en seguridad informática, y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas. La guía está conformada por cinco secciones que en conjunto son un proceso iterativo

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

de tareas que se ejecutan de manera secuencial. (Luna and Rosa 2009).

La metodología propuesta por NIST SP 800-30, incluye los siguientes subprocesos: (Sotelo Bedón, Torres Utrilla et al. 2012)

- Caracterización de sistemas.
- Identificación de amenazas y vulnerabilidades.
- Análisis de controles.
- Determinación de probabilidades.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de controles.
- Documentación de resultados.

3.3 COBIT 5

Es un framework de gestión de tecnologías de la información, desarrollado por ISACA (Asociación de Control y Auditoria de Sistemas de Información), que permite a una empresa balancear los beneficios de la realización con niveles aceptables de riesgos y uso de recursos.

Se enfoca en el desarrollo de políticas y buenas prácticas de seguridad en el manejo de la información de la empresa.

De acuerdo con el documento How to integrate ISO 27001, COBIT and NIST, de 27001 Academy, el framework de COBIT está dividido en cuatro dominios:

- Planear y organizar.
- Adquirir e implementar.
- Distribuir y dar soporte.
- Monitorear y evaluar.

3.4 ISO 27001

Es la norma para seguridad informática de la Organización Internacional de Normalización que describe la manera de gestionar la seguridad de la información de una empresa. Está basado en el ciclo de mejora continua propuesto por Deming (planificar, hacer, verificar, actuar), lo cual implica que un sistema de gestión de información basado en esta norma es dinámico, puesto que se está revisando continuamente. (Calder and Watkins 2008)

Para conseguir la mejora continua, la norma pone énfasis en buscar los potenciales problemas de seguridad que pueden comprometer la información, y proponer formas de evitarlos. Pone énfasis en la documentación adecuada de cada proceso, y en la revisión continua de todos ellos, para adaptar el sistema de gestión a los cambios que se producen al expandirse la empresa.

El estándar ISO/IEC 27001 determina los requisitos para analizar, establecer, implementar, monitorear, proteger y optimizar un SGSI, además especifica lo que se necesita para la implementación de controles de seguridad de acuerdo a las necesidades de la institución, frente a un proceso específico o un servicio. Esta normativa comprende dos secciones, en la primera se especifican cinco cláusulas enfocadas a características metodológicas del SGSI y en la segunda se definen los controles para la gestión de la seguridad de la información. (Calder and Watkins 2008).

La ISO 27001 se utiliza en la alineación, requerimientos de seguridad, conocimiento de la administración de los riesgos, la disposición de las políticas y procedimientos de seguridad, y los mecanismos para la medición de efectividad del programa de seguridad de la información, las políticas, los controles y planes para el tratamiento del riesgo. (Solarte, Rosero et al. 2015).

3.5 COMPARACIÓN ENTRE MODELOS

En la tabla 2, se recogen las características principales de las mejores prácticas de seguridad de cada modelo estudiado. Los parámetros de comparación se tomaron de varios documentos publicados.

Tabla 2 Comparación entre los diferentes modelos o estándares

Indicador	OSSTMM 3	NIST	COBIT 5	ISO 27001
Recursos y métodos para la implementación	No	Suministra documentación para desarrollar metodologías de implementación	Proporciona documentación para desarrollar metodologías de implementación	Provee metodologías de implementación
Está orientado a procesos	Se orienta en proveer procedimientos de pruebas para verificar la seguridad del sistema	Si	Si	Si

Ejecuta la seguridad que está basada en gestión de riesgos	No	El propósito principal de la norma es la seguridad	Adopta una gestión de riesgos que definen qué controles de seguridad deben aplicarse	El propósito principal de la norma es la seguridad
Se puede aplicar a diferentes empresas	Si	Está orientada a empresas de los Estados Unidos	No es un framework oficial de soluciones globales	Se emplea en cualquier tipo de empresa y de cualquier tamaño
Objetivos claramente definidos	Si	Requiere de información previa para definir los objetivos	Si	Requiere de información previa para definir los objetivos
Estructura de gestión claramente definida	No	No	Si	No
Cobertura de los controles	No	Se enfoca en la seguridad de los equipos de cómputo.	Enfoca el control en las tecnologías de la información	Tiene controles de seguridad para cada proceso de implementación
Utiliza certificados	No	Sólo en Estados Unidos	Si	Si

Fuente: Los Autores

En la tabla puede apreciarse que todos los modelos tienen semejanzas importantes en cuanto a la gestión de la información. Las diferencias principales están en el enfoque que cada modelo hace de los diferentes aspectos de dicha gestión. Además, NIST tiene un origen más localista, lo que de alguna manera limita su aplicación. COBIT, ISO 27001, y OSSTMM3 se originaron pensando en un entorno global.

Conclusiones

Los modelos de gestión de la información abarcan un conjunto amplio de aspectos, que deben considerarse al momento de decidir implementar un SGSI (Sistema de Gestión de la

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

Seguridad de la Información).

La elección de un modelo en particular o el desarrollo de un marco de referencia en base a ellos, debe realizarse de manera razonada, sopesando los beneficios y costos asociados con dicha elección.

Aunque ISO 27001 provee prácticas reconocidas globalmente, esto no significa que es la respuesta definitiva a la seguridad de la información. La implementación de un sistema de seguridad debe tener un enfoque holístico para ser efectiva. Para conseguir esta orientación es necesario el aporte de los otros modelos de gestión de la seguridad, con sus características esenciales, que los hacen adecuados para los diferentes aspectos a considerarse durante la planificación e implementación de un sistema de gestión de la seguridad de la información. Por ejemplo, se puede utilizar el framework de ciberseguridad de NIST para ayudar en el diseño de los controles de TI de ISO 27001.

Recomendaciones

El estudio de los modelos de gestión de la información que son más utilizados en la actualidad debería tomarse como base para el desarrollo de un marco de referencia de un Sistema de Gestión de la Seguridad de la Información.

La elección de un modelo específico de seguridad informática, debe realizarse tomando en cuenta la realidad del entorno donde se aplicará dicho sistema de seguridad.

El desarrollo de un modelo ad hoc de seguridad informática, debe tener en cuenta las principales recomendaciones que se recogen en los modelos estudiados.

Referencias Bibliográficas

Acosta, R. E. and G. A. Isazaa "*Hacia un arquitectura de buenas prácticas de seguridad para sistemas ERP*."

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*, Editorial Paraninfo.

Calder, A. and S. Watkins (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*, Kogan Page Ltd.

Herzog, P. (2017). OSSTMM3.

Luna, C. and C. D. Rosa (2009). "*Análisis formal del estándar NIST para modelos RBAC.*" Reportes Técnicos 09-09.

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742

Milagros, P. B. L. and Y. C. E. Steven (2017). *Análisis De Vulnerabilidades En La Infraestructura Tecnológica De Una Empresa, Utilizando Herramientas De Test De Intrusión, Universidad De Guayaquil.* Facultad De Ciencias Matemáticas Y Físicas. Carrera De Ingeniería En Networking Y Telecomunicaciones.

Nist, S. (2012). 800-145: *The NIST definition of cloud computing.*

Solarte, F. N. S., et al. (2015). "*Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001."* Revista Tecnológica-ESPOL **28**(5).

Sotelo Bedón, M., et al. (2012). "*Un proceso práctico de análisis de riesgos de activos de información."*

Triana, R. and R. E. Triana (2014). "*Modelos de seguridad.*" Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacional, Bogotá.

Valdez Alvarado, A. (2013). *"OSSTMM 3.*" Revista de Información, Tecnología y Sociedad: 29.

Vásquez Alvarado, A. (2014). "OSSTMM3." 20-3

Como citar este artículo:
Lara, E., & Corella, F. (Enero – Diciembre 2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. *Tierra Infinita* (4), 22-33. https://doi.org/10.32645/26028131.742