Polo del Conocimiento

Pol. Con. (Edición núm. 20) Vol. 3, No 6
Junio 2018, pp. 478-491
ISSN: 2550 - 682X
DOI: 10.23857/pc.v3i6.641

Recepción: 23 / 02 / 2018
Aceptación: 19 / 04 / 2018
Publicación: 05 / 06 / 2018

Ciencias de la Computación

Artículo Descriptivo

ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo

ISO / IEC 27001 assurance of the quality of information: Timeline

ISO / IEC 27001 garantia da qualidade da informação: Timeline

Yolanda de la N. Cruz-Gavilánez [I]
nube5502@gmail.com

Carlos J. Martinez-Santander [II]
cmartinezs@ucacue.edu.ec

Correspondencia: nube5502@gmail.com

[I] Ingeniera en eletronica y telecomunicaciones Insucom Cia. Ltda.

[II] Universidad Católica de Cuenca, Azuay, Ecuador

Resumen

En la actualidad los datos son esenciales en la vida cotidiana de todas las personas, empresas, organizaciones, entre otras. Desafortunadamente el riesgo de fraude cada vez es mayor. Ciberataques, hacking de los datos digitales, perdida de información se ha convertido en algo común de esta década. La aparición de nuevos sistemas acoplados a la parte industrial, de salud, energía, servicios básicos. Los han convertido en infraestructuras críticas, si incurre un ataque, puede traer consigo la paralización de una ciudad, además de las pérdidas económicas. Por tanto, el riesgo es cada vez mayor. Una de las medidas efectivas para contrarrestar en un alto porcentaje estos problemas, sería la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Esto provee un detallado marco para el desarrollo, implementación y gestión de seguridad de la información ISO/IEC27001. Representa un propósito importante para proteger su TI (Tecnología Informática), infraestructura y aseguramiento de los datos para una empresa u organización ya sea pública o privada. EL objetivo de este artículo es discutir el origen y evolución de la ISO / IEC 27001, además se hace una comparación entre la ISO 27001: 2005 y 2013 que es el estándar actual e implementado en la mayoría de las organizaciones.

Palabras claves: ISO/IEC 27001; estándar.

Abstract

At present, data is essential in the daily life of all people, companies, organizations, among others. Unfortunately, the risk of fraud is increasing. Cyber-attacks, hacking of digital data, loss of information have become common in this decade. The appearance of new systems coupled to the industrial part, health, energy, basic services. They have turned them into critical infrastructures, if incurred an attack, it can bring with it the paralysis of a city, in addition to economic losses. Therefore, the risk is increasing. One of the effective measures to counteract these problems in a high percentage would be the implementation of an Information Security Management System (ISMS). This provides a detailed framework for the development, implementation and management of information security ISO / IEC27001. It represents an important purpose to protect your IT (Information Technology), infrastructure and data assurance for a company or organization, whether public or private. The objective of this article is to

discuss the origin and evolution of ISO / IEC 27001, in addition, a comparison is made between ISO 27001: 2005 and 2013, which is the current standard and implemented in most organizations.

Keywords: ISO / IEC 27001; standard.

Resumo

Atualmente, os dados são essenciais no dia a dia de todas as pessoas, empresas, organizações, entre outros. Infelizmente, o risco de fraude está aumentando. Ataques cibernéticos, pirataria de dados digitais, perda de informações tornaram-se comuns nesta década. O surgimento de novos sistemas acoplados à parte industrial, saúde, energia, serviços básicos. Eles os transformaram em infraestruturas críticas, se incorridos em um ataque, podem trazer consigo a paralisia de uma cidade, além de perdas econômicas. Portanto, o risco está aumentando. Uma das medidas eficazes para combater esses problemas em uma alta porcentagem seria a implementação de um Sistema de Gerenciamento de Segurança da Informação (SGSI). Isso fornece uma estrutura detalhada para o desenvolvimento, implementação e gerenciamento da segurança da informação ISO / IEC27001. Representa um propósito importante para proteger sua TI (Tecnologia da Informação), infraestrutura e garantia de dados para uma empresa ou organização, seja pública ou privada. O objetivo deste artigo é discutir a origem e evolução da ISO / IEC 27001, além de uma comparação entre a ISO 27001 é: 2005 e 2013, que é o padrão atual e implementado na maioria das organizações.

Palavras chave: ISO / IEC 27001; standard.

Introducción

La información es un activo vital para el éxito y la continuidad en el mercado de las empresas, si alguien logra cambiar o robar esta información, traería serios problemas para la misma. Si las empresas desean salvaguardar su valor, deben invertir en la protección. Una de estas soluciones seria la implementación de un SGSI basado en ISO / IEC 27001.

Un Sistema de Gestión de la Seguridad de la Información, contiene todo lo instrumentos y métodos que la administración debería usar para satisfacer la seguridad de la información en todas las actividades que se realizan. Este contiene políticas, procedimientos, directrices, recursos

relacionados y actividades para ser gestionados, al momento de su implementación, evaluación y control se toma en cuenta las necesidades, objetivos, actividades, procesos, el tamaño de la empresa u organización y los requisitos de seguridad. Es fundamental considerar el SGSI como parte importante de la organización. Las ventajas más importantes además de la seguridad son: la garantía de mercado y la gobernanza.

Los Estándares Internacionales han sido creados para proporcionar un modelo que permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. La adopción de un SGSI debe ser una decisión estratégica de cualquier organización. Todo esto da lugar al uso de la norma ISO / IEC 27001 que es una solución para la mejora continua en base a la cual podemos evaluar todo tipo de riesgo o amenaza que puede poner en peligro la información propia o de terceros de una empresa u organización.

El propósito de este artículo es realizar una evaluación de la evolución que ha tenido la Norma ISO / IEC 27001 a través del tiempo. El estándar nació en 1998 como BS 77779-2 y al momento tenemos a la ISO / IEC 27001:2013.

Background

En este apartado se expone la conceptualización de la ISO como estándar internacional, además se habla del funcionamiento de la ISO y su familia.

ISO/IEC por sus siglas en inglés (International Organization for Standardization- International Electrotechnical Commission), son estándares mundiales que desarrollan normas internacionales por medio de comités técnicos, que tratan de áreas particulares de actividades técnica.

ISO e IEC con el apoyo de organizaciones gubernamentales, no gubernamentales e internacionales colaboran en brindar ideas y experiencias propias para fortalecer estas normativas.

Los estándares internacionales se crearon con fines específicos como el buen manejo en la gestión de calidad de una empresa, es decir, para mejorar, mantener, operar, diseñar, implementar, establecer reglas para su organización.

En el campo de la informática la Organización internacional de estándares propone un sistema de gestión de seguridad de la información para que garantice que los riesgos de seguridad que sufren la información sean conocidos y adopten medidas para prevenirlos, formando un comité ISO / IEC JTC que cuenta con dos puntos importantes; 1. Código de prácticas que consiste en obtener una certificación; 2. Mejorar la práctica en seguridad de la información esto radica en recomendar el mejor nivel de gestión de seguridad TI.

En el mundo tecnológico a nivel mundial admite la necesidad de imponer normas para el aseguramiento de la información en organizaciones que manejan miles de datos con la ISO/IEC como lo es la 27001 que es la encargada de registrar los requisitos de control e imponer la guía de sistema de gestión de seguridad de la información (ISMS).

La normativa 27001 se lo define como el sistema de gestión de seguridad de la información, que se lo realiza mediante un proceso sistemático, documentado y difundido al personal de toda la organización. Es un estándar público encargado exclusivamente a la seguridad de la información y pertenece a la familia de las normas ISO 27000.

El establecimiento de políticas de gestión (ISMS) se centra en un enfoque de gestión de riesgos dela información, cuando se comienza definiendo políticas se necesita la comprensión del entorno la evolución de los recursos y los procesos con el fin de identificar los riesgos de seguridad de la información que se podrían dar a lugar.

Cuando se identifican los riesgos de seguridad la empresa lo que hace, es evaluar el proceso para reducir a un nivel aceptable e implementar mecanismos apropiados para que el nivel de riesgos se encuentre en un nivel admisible. La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos de la organización. Los resultados de la evaluación deben determinar el plan de tratamiento del riesgo.

Una evaluación de riesgos se sugiere que se lo debe realizar periódicamente debido a que existe un cambio frecuente en los dispositivos electrónicos y en los requisitos de seguridad.

La ISO/IEC para el tratamiento de riesgos

Análisis de Riesgos:

En este punto identifica y evalúa los activos de información, analizar las amenazas sobre esos activos de información, identifica vulnerabilidades, determina probabilidades de ocurrencia y el impacto, establece criterios de aceptación del riesgo, identifica los controles para mitigar y por último evalúa el costo beneficio de las contramedidas

Enfoque de análisis de Riesgos:

Se analiza de forma cualitativa, cuantitativa y sus vulnerabilidades

Selección e implementación de controles:

En este punto del tratamiento de riesgos se selecciona los controles se prioriza la implementación de los controles, además se planifica la implementación se asigna responsables y por último en este punto se implementa controles para determinar Riesgo Residual

Monitoreo y evaluación de los Controles Implementados:

La etapa como prioridad es Revisar, monitorear la efectividad de los controles.

Para aplicar estas etapas se debe tomar en consideración los criterios si se debe o no aceptar los riesgos, los riesgos se pueden aceptar si como resultado de la evolución es bajo por lo tanto la aceptación y el motivo deben quedar registrados.

Funcionamiento de la ISO 27001

El funcionamiento de este estándar tiene que ver con la gestión de seguridad de la información en entornos informáticos, que prueban la seguridad de la información y miden la efectividad de un Sistema de Gestión de seguridad de la información (SGSI).

Garantiza la seguridad de los activos relacionados con la información y la visión, misión y objetivos de la organización, sistema que es seguro en el momento de medir efectividad. Cuando evalúa efectividad el SGSI lo realiza con medidas esta medida hace referencia a la norma internacional ISO 27001 que incluye la medición de políticas, gestión de los riesgos de seguridad

de la información, los objetivos de control, los controles, los procesos y los procedimientos, y respaldará proceso de revisión.

Al mismo tiempo identifica, evalúa y determina si es necesario cambiar o reparar el Sistema de seguridad de la información o el control del proceso. También puede ayudar a las organizaciones a proporcionar evidencia adicional para las revisiones de gestión y el proceso de gestión de riesgos de seguridad de la información.

El funcionamiento de la norma 27001, se plasma en la aplicación de los cuatro ciclos que está construido el modelo SGSI y las tareas que se deben realizar en cada una de ellas.

1. **Planificar** este ciclo define la normativa del alcance y manual del SGSI, política de seguridad y la metodología de evaluación de riesgos. Se realiza el inventario de activos identificando amenazas, vulnerabilidades e impactos que se pueden presentar, elaborando un análisis y evaluación de riesgos y así seleccionar los controles y establecer la declaración de aplicabilidad.

2. **Hacer** es definir el plan e implantar el tratamiento de riesgos efectuando los controles para ejecutar el plan de capacitación y concientización y de esa manera operar el SGSI.

3. **Verificar** se revisar el SGSI midiendo la eficacia de los controles implementados, revisando los riesgos residuales para realizar auditorías internas del SGSI y de esa manera registrar acciones y eventos.

4. **Actuar** se implanta mejoras y se ejecuta acciones preventivas - acciones correctivas para comprobar la eficacia de las acciones

Los beneficios que se llegan a obtener con la aplicación de los cuatro ciclos son: reducción de costos, la optimización de recursos y las inversiones, mejora la imagen corporativa, es un facilitador para la organización de un negocio y aumenta la competitividad.

Algunas tareas del SGSI de la 27001 es la asignación del compromiso de la dirección, asignación de recursos, formación y concienciación y revisión del SGSI.

En el acompañamiento del SGSI, se debe incluir la documentación correspondiente para un ISMS como prueba de la implementación de los controles con la finalidad de que existan mejoras continuas, de acuerdo a una de las tareas dentro de las etapas establece que como punto central y

obligatorio se debe de cumplir. Como mejor perspectiva de mejorar las practicas recomendada por Alan Calder, dice que en la cláusula 4 de ISO 27001 se puede distinguir cuatro niveles jerárquicos diferentes nivel1, nivel2, nivel3 y nivel4.

Empezando con el nivel 1, que es el nivel superior cada uno de los niveles; es afectado por el nivel debajo del 2, hasta que alcanza al último que a su vez es el nivel 4. Por lo que se necesitan estándares (Set) y pautas (Gl), para las políticas definidas (Pol) asignadas al nivel. Los estándares y las pautas se definen en el nivel inferior. Además, los estándares y las pautas solicitan pasos, procedimientos para su aplicación. Los Procedimientos (Pr) requieren listados de verificación (Cl), e instrucciones de trabajo (Ws). Después, se observa que como prueba de implementación existen registros en el nivel 4 que el último nivel en forma de protocolos, archivos de registro y datos.

La Familia de las ISO 27001

La familia de las ISO 27001, fue evolucionando de acuerdo al pasar del tiempo y la evolución de la tecnología en donde los temas de seguridad iban tomando renombre, los hackers ya buscaban la manera de eliminar las seguridades de cada uno de los sistemas quedando vulnerables ante los ataques tantos los equipos como las normativas.

El objetivo principal de la normativa 27000, ha sido diseñar la medición del sistema de gestión de Seguridad de la información SGSI en sus distintas versiones que han adoptado una actualización en cada una de ellas.

Entre las estudiadas y utilizadas a nivel de organizaciones mundiales se tienen, las que se enumeran a continuación:

- ISO/IEC 27000:2014
- ISO/IEC 27001 preparo el comité técnico en conjunto con ISO/IEC JTC 1, Tecnologías de la información, subcomités SC27 y técnicas de seguridad TI.
- ISO/IEC 27001:2005
- ISO/IEC 27001:2013

- ISO/IEC 27002 esta normativa fue preparado por el comité técnico en conjunto con ISO/IEC JTC 1, Tecnologías de la información, subcomités SC27 y técnicas de seguridad TI [3].
- IEC 27002: 2013.

Los estándares son capaces de examinar la seguridad de la información y medir la efectividad y fiabilidad de un sistema de gestión de la información implementado (SGSI) que fue adoptada como SIN ISO/IEC 21004: 20013.

Línea De Tiempo De La Iso/Iec 27001

En esta sección, se describe una secuencia de eventos o hitos que dio lugar a la ISO 27001. Como se muestra en la Fig. 1. La presenta línea de tiempo tiene lugar en el año 1995 y finaliza en el 2013.

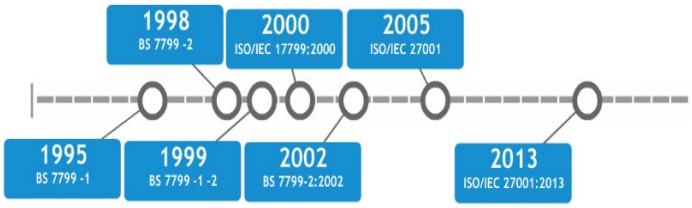

Fig. 1. Line de Tiempo de la ISO/IEC 27001.

Los pioneros en desarrollar un código de buenas prácticas para la seguridad de la información, fue British Standards Institution (BSI) y el Departamento de Comercio y Administración del Reino Unido en el año 1995 como BS -77799. Fue dividida en dos partes; la primera la (BS7799-1), contiene el código de prácticas y la (BS7799-2) 1999, contiene las especificaciones para la certificación. Esta normativa permite el desarrollo posterior de la gestión de seguridad de la información (ISO 17799) en el año 2000. Aquí se desarrolla un marco abierto para un sistema de gestión de seguridad para toda la empresa o denominada; Gestión de Seguridad de TI.

En el 2002 la versión BS 7799-2 introdujo (PDCA) Plan-Do-Check-Act (Fig. 2. Modelo PDCA según BS 7799-2), como se aprecia en la Fig. 2. Esta versión está diseñada para proteger los Sistemas de Información de las organizaciones.

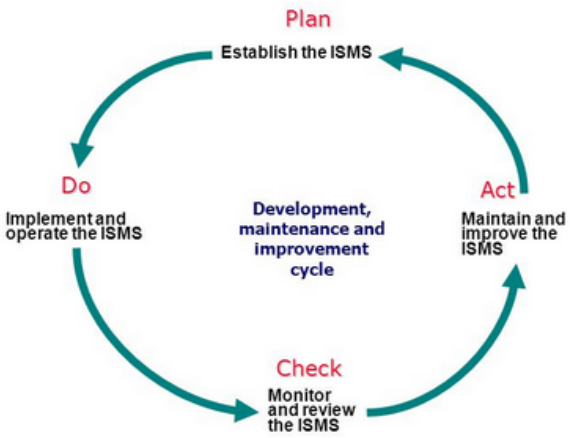

Fig. 2. Modelo PDCA según BS 7799-2.

Desde el año 2005, se adopta la serie 27000 esta norma es más importante de la familia, la 27001 especifica los requisitos para la implementación de un SGSI. Esta norma da una lista completa de los controles a aplicar para poder obtener la certificación ISO. Una característica importante de esta norma es que se define los roles y responsabilidades de cada persona, es decir, exige una estructura organizativa. Exige procesos y recursos para la consecución de los objetivos. También presenta un proceso de revisión, cuyos resultados sirven de retroalimentación para la mejora continua. Todo esto acompañado con una metodología de evaluación del SGSI.

Para el 2013 se hace una actualización de la ISO/IEC 27001 2005. Esta actualización está basada en el Anexo SL, este anexo es la razón principal que permite distinguir de la 2005. El Anexo SL es una guía que integra estándares de sistemas de gestión ISO. Todos estos estándares revisados del sistema de gestión deben integrarse y adaptarse a esta estructura de alto nivel. Otra característica importante es que esta norma es complementada con la ISO 22301: 2012 que hace referencia a la continuidad comercial y la ISO 9001 Sistema de Gestión de la Calidad.

Esta norma estipula que no pueden ser excluidos ninguno de los requisitos de las clausulas 4 a 10, esto no es aceptable. Los títulos y contenidos de las clausulas 4 a 10 en la actualización 2013 son distintos a los del 2005.

ISO/IEC 27001:2005 VS ISO/IEC 27001: 2013

La norma ISO/IEC 27001, surge en el 2005 con el fortalecimiento de sus antecesoras. Al momento la actualización liberada es la 2013. Por esta razón, surge la necesidad de hacer una comparación entre estas dos normas.

	ISO/IEC 27001 2005	ISO/IEC 27001 2013
Cicalo PDCA(Plan-Do-Check-Act)	✔	
Compatibilidad con otros estándares		✔
Obligatoriedad de cumplir con el Alcance		✔
Términos y Definiciones		✔
Establecer objetivos de Seguridad		✔
Criptografía		✔
Seguridad en Comunicaciones		✔
Relación con proveedores		✔
Políticas de Seguridad de la Información		✔
Gestión de comunicaciones y operaciones	✔	✔
Control de acceso	✔	✔
Adquisición, desarrollo y mantenimiento de sistemas de información	✔	✔
Organización de la Seguridad de la Información	✔	✔
Gestión de Activos	✔	✔
Gestión de Incidentes de la Seguridad de la Información	✔	✔
Gestión de Continuidad del	✔	✔

Pol. Con. (Edición núm. 20) Vol. 3, No 6, junio 2018, pp. 478-491, ISSN: 2550 - 682X

Negocio		
Seguridad de los Recursos Humanos		✔
Seguridad Física y Ambiental		✔
Cumplimiento	✔	✔

Tabla 1. Comparación de la ISO / IEC: 2005 con la ISO / IEC: 2013

Como se puede apreciar en la Tabla 1. La actualización de la ISO 27001 del año 2013 se acoplan nuevos términos y se abordan nuevos campos como son: Criptografía, Seguridad de Comunicación, Relación con los proveedores, Políticas de seguridad de la información. Un aspecto importante de esta actualización es el Ciclo PDCA el cual es eliminado, existe una camisa de fuerza al usar este ciclo, debido a que no había la posibilidad de acoplar a otros modelos.

El alcance, es decir las cláusulas de la 4 a la 10, son obligatorias en la versión 2013. Se fortalece la evaluación de la Seguridad Física y Ambiental. También se implementa la seguridad a nivel de usuarios a la que se denomina Seguridad de los Recursos Humanos.

	ISO/IEC 27001 2005	**ISO/IEC 27001 2013**
Dominios	11	14
Objetivos de Control	39	35
Controles	133	114

Tabla 2. Dominios, Objetivos de Control y Controles de la ISO /IEC: 2005 VS ISO /IEC: 2013

En cuanto a la Estructura la ISO / IEC 27001: 2005, esta diseminada en cinco cláusulas: 4. Gestión de la seguridad del Sistema de información, 5. Responsabilidad de gestión, 6. Auditorías internas del ISMS, 7. Revisión de la gestión del SGSI, 8. Mejora del ISMS. Mientras tanto la ISO / IEC 27001: 2013, especifica siete clausulas obligatorias: 4. Contexto de la organización, 5. Liderazgo, 6. Planificación, 7. Apoyo, 8. Operación, 9. Evaluación del desempeño, 10. Mejora.

Conclusiones

Los SGSI han traído ventajas notables en cuanto al aseguramiento de la información, sin embargo, es necesario fusionar con otras normativas para abarcar casi por completo la seguridad la de la información.

La actualización de cada norma según ISO, debe hacerse cada 5 años. Ese tiempo debería ser menor ya que se ha demostrado, la tecnología, aplicaciones, sistemas, entre otros, tiene avances en menor tiempo, por tanto, esto hace que la ISO se quede rezagada de algunos campos.

Referencias Bibliográficas

W. Boehmer, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001," in 2009 International Conference on Availability, Reliability and Security, 2009, pp. 392–399.

B. Shojaie, H. Federrath, and I. Saberi, "Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A," in 2014 Ninth International Conference on Availability, Reliability and Security, 2014, pp. 259–264.

I. STANDARD, "ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements." [Online]. Available: https://www.iso.org/standard/42103.html. [Accessed: 15-Nov-2017].

A. Aginsa, I. Y. Matheus Edward, and W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and zachman framework - A study case of XYZ company," in 2016 2nd International Conference on Wireless and Telematics (ICWT), 2016, pp. 62–66.

C. Hsu, T. Wang, and A. Lu, "The Impact of ISO 27001 Certification on Firm Performance," in 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 4842–4848.

I. STANDARD, "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements." [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: 15-Nov-2017].

K. Pecina, R. Estremera, A. Bilbao, and E. Bilbao, “Physical and Logical Security management organization model based on ISO 31000 and ISO 27001,” in 2011 Carnahan Conference on Security Technology, 2011, pp. 1–5.

M. Nancylia, E. K. Mudjtabar, S. Sutikno, and Y. Rosmansyah, “The measurement design of information security management system,” in 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), 2014, pp. 1–5.

B. Blakley, E. McDermott, and D. Geer, “Information security is information risk management,” in Proceedings of the 2001 workshop on New security paradigms - NSPW ’01, 2001, p. 97.

M. Siponen and Mikko, “Information security standards focus on the existence of process, not its content,” Commun. ACM, vol. 49, no. 8, p. 97, Aug. 2006.

H. Susanto, M. N. Almunawar, and Y. C. Tuan, “Information Security Management System Standards: A Comparative Study of the Big Five,” Int. J. Electr. Comput. Sci. IJECS-IJENS, vol. 11, no. 23, pp. 113505–6969.