Revista de investigación de sistemas e informática
17(2): 45-49 (2024)
DOI: https://doi.org/10.15381/risi.v17i2.29916

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

La seguridad de la información y los beneficios de la Norma ISO/IEC 27002:2013

Information security and the benefits of ISO/IEC 27002:2013

Manuel Fernando Pumasunco Rivera
https://orcid.org/0000-0002-4394-8526
mpumasuncor@usmp.pe
Universidad San Martin de Porres, Lima, Perú

Candy Esther Seminario Sanchez
https://orcid.org/0000-0002-5918-7813
candy.seminario@unmsm.edu.pe
Universidad Nacional Mayor de San Marcos, Lima, Perú

Recibido: 30/10/2024 - Aceptado: 09/12/2024 - Publicado: 31/12/2024

RESUMEN

La justificación se debe a la creciente amenaza en temas de seguridad de la información y constantes caso de robo informático a empresas u organizaciones. El objetivo de la presente investigación es brindar los beneficios de un Sistema de Gestión de Seguridad de la Información (SGSI) basados la norma Iso 27002:2013 la cual comprende controles a implementar por la empresa u organización que ayudaran a proteger su información e involucrar aspectos de ciberseguridad. La investigación es exploratoria, porque el tema es poco investigado y también de diseño no experimental poque no se va a alterar, inducir o modificar las variables. Como resultado tenemos la confirmación y eficacia de los controles de la Norma Iso 27002 entendido de una manera transversal para cualquier sector empresarial, y que no es necesario lograr una certificación de la norma Iso 27001, para poder aplicar los controles que sugiere la norma y lograr el objetivo de la seguridad de la información.

Palabras claves: Seguridad de la información, ISO 27001, ISO 27002, Ciberseguridad, Sistema de Gestión de Seguridad de la Información.

ABSTRACT

The justification is due to the growing threat in information security issues and constant cases of computer theft from companies or organizations. The objective of this research is to provide the benefits of an Information Security Management System (ISMS) based on the ISO 27002:2013 standard, which includes controls to be implemented by the company or organization that will help protect its information and involve aspects cybersecurity. The research is exploratory, because the topic is little investigated and also non-experimental in design because the variables will not be altered, induced or modified. As a result we have the confirmation and effectiveness of the controls of the ISO 27002 Standard understood in a transversal way for any business sector, and that it is not necessary to achieve a certification of the ISO 27001 standard, in order to apply the controls suggested by the standard and achieve the objective of information security.

Keywords: Information security, ISO 27001, ISO 27002, Cybersecurity, Information Security Management System.

1. INTRODUCCIÓN

Después del efecto de la pandemia, toda la información va en camino a una mayor digitalización, este cambio ha traído una mayor ventaja competitiva a muchas organizaciones a nivel mundial. Pero también han aparecido amenazas al respecto.

Muchos temas relacionados con ciberseguridad e inteligencia artificial están abarcando muchos artículos e investigaciones.

En los últimos años se ha experimentado un crecimiento a la importación del uso de la información para la toma de decisiones en las empresas u organizaciones, siendo así, se convierte en un activo muy valioso el cual debe ser protegido.

Por otro lado, también ha creció los temas de robo de información, espionaje u otros aspectos que perjudican a las empresas u organizaciones, es por ello por lo que el tema de ciberseguridad es muy considerado y cada vez toma mas fuerza el implementar no solo antivirus, sino establecer procedimientos e incluso cuando la Alta dirección se involucra se establecen Políticas de Seguridad de la Información.

Frente a esta necesidad, la adopción de un SGSI es una decisión estratégica para una organización y también es necesario que esta decisión se integre, escale y actualice a la perfección de acuerdo con las necesidades de la organización.

1.1. Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI comprende un conjunto de políticas ,procesos, instructivos y controles elaborados para proteger la información de una empresa u organización. Con respecto a nuestro país, un Sistema de Gestión de Seguridad de la Información (SGSI) consta de políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información (Gobierno del Perú. 2024).

Para un SGSI uno de los principales objetivos es reducir el riesgo de que se produzcan pérdidas de información valiosa de la institución. (Pronabec, 2024)

ISO 2700.ES(2024) menciona que cualquier información que una organización recoge y emplea puede estar vulnerable a ataques, errores de personas, inconvenientes ambientales o malfuncionamientos en los sistemas.

Para el Programa Nacional de Becas y Crédito Educativo (PRONABEC) el SGSI permite gestionar de manera adecuada la seguridad de la información institucional, a fin de hacer frente a diversas amenazas.

Según Guerra et las (2021) los sistemas de gestión de la seguridad de la información (SGSI) con llevan a la implementación de “procesos específicos que establecen mecanismos como indicadores de gestión”.

1.2. Seguridad de la información

Según las normas ISO 27001:2022 se debe tener en cuenta tres aspectos principales: confidencialidad, disponibilidad e integridad. Para lograr esto, se implementa un conjunto específico de controles que deben ser permanentemente supervisados. Según la norma ISO/IEC 27000: 2014 es fundamental que estos controles de seguridad se integren sin problemas con los procesos de negocio de la organización. (ISO/IEC 27000: 2014 - 3.2.3)

IBM en sus comentarios indica que “la seguridad de los datos implica la implementación de herramientas y tecnologías que mejoran la visibilidad de la organización sobre dónde residen sus datos críticos y cómo se utilizan”.

Además, IBM cita que “El valor empresarial de los datos nunca ha sido tan grande como hoy”**.**

Desde el punto de vista de una Certificadora Internacional como Bureau Veritas Certificación, “la seguridad de la información es crucial para mantener a las empresas operativas, una afectación de ella puede generar un profundo impacto en el desarrollo de actividades.”

1.3. Interpretación de la norma Iso 27001:2022 Sistemas de Gestión de Seguridad de la Información

Es un proceso que se repite de manera constante y evoluciona con el tiempo, enfocado en gestionar de forma efectiva los riesgos asociados con la seguridad de la información dentro de la organización. Por eso, entender claramente lo que se necesita es clave para lograr una implementación exitosa y asegurar que los controles de seguridad se apliquen correctamente.

Esta Norma Internacional proporciona una descripción general de los sistemas de gestión de seguridad de la información, y define términos relacionados.

Integrated Assessment Services - IAS (2020) esta entidad acreditadora nos comenta que “esta norma internacional especifica los requisitos para proteger a su empresa de los riesgos e incidentes de seguridad”.

Rivera et al (2019) Actualmente la información se ha transformado en un activo impalpable que requiere de garantizar su integridad, su disponibilidad y confidencialidad. (p. 28)

1.4. Norma Iso 27002:2013

Esta norma pertenece a la familia de la serie ISO/ IEC 27000 que está direccionada a la Seguridad de la información. Puede considerarse como un código de buenas prácticas en gestión de la seguridad de la información.

Tal como menciona Puentes (2021) la norma involucra a la Alta Dirección principalmente en la asignación de recursos para la seguridad de la información. (p.23)

2. MATERIALES Y METODOS

El método de investigación es exploratorio, porque el tema es poco investigado y también de diseño no experimental poque no se va a alterar, inducir o modificar las variables.

La recolección de información se realizó con base a datos obtenidos de diversas fuentes, como libros, artículos y revistas, con el objetivo de obtener una comprensión general.

El análisis tiene un enfoque aplicativo, ya que implica la formulación de propuestas para controles de seguridad dentro de una empresa u organización.

3. DISCUSIÓN

Los beneficios se van a evaluar en base a la norma La ISO 27002:2013 que proporciona directrices y recomendaciones de las mejores prácticas en la gestión de la seguridad de la información, manteniendo los puntos principales como la Confidencialidad (quienes pueden acceder a la información), integridad (sin alteraciones no autorizadas) y disponibilidad (libre acceso cuando se necesite) requieran).

La versión de 2013 del estándar describe 14 dominios principales con 35 objetivos de control y 114 controles.

Si bien, el número total de controles suma 114 entre todas las secciones, cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

El determinar qué requisitos de la ISO 27002 son aplicables a la empresa, ayudará a determinar cuánto tiempo y esfuerzo tomará para implementar un SGSI que cumpla estos requisitos. Por ejemplo, si la empresa no es financiera, no se requiere revisar el punto 14 de “consideraciones criptográficas”.

Por otro lado, una organización pequeña con sistemas informáticos limitados probablemente no necesite incluir los requisitos relacionados con el punto 7 de “adquisición y desarrollo de sistemas”.

Como parte de la investigación se va a mencionar cada requisito y se propone algunas preguntas para su validación respectiva de cumplimiento, lo cual servirá de apoyo para las empresas.

3.1. Políticas de seguridad

Para su validación debemos responder si: ¿Existen políticas de seguridad de la información en la empresa u organización? ¿De qué manera la Alta Dirección participa de las Políticas de Seguridad?

3.2. Organización de la seguridad de la información

Para su validación debemos responder si ¿Se definieron los roles y las responsabilidades en la empresa u organización en cuanto a seguridad de la información? ¿Se tiene algún procedimiento al respecto?

3.3. Seguridad de los recursos humanos

Para su validación debemos responder si ¿Se definió una política para investigar a los empleados durante el proceso de selección, en la contratación y después de terminar el vínculo laboral? ¿se tiene considerado un acuerdo de confidencialidad de información con los empleados?

3.4. Gestión de los activos

Para su validación debemos responder si ¿Se definió una política para los activos corporativos?;¿Se definió una política para la administración de medios extraíbles (USB)?

3.5. Control de accesos

Para su validación debemos responder si:¿Se definió una matriz de accesos por jerarquías? ¿Se definió una política para la validación y autenticación de usuarios?¿Se tiene un procedimiento o normativa en base al control de acceso?

3.6. Cifrado

Para su validación debemos responder si: ¿Se definió una política para la gestión de usuario y contraseñas? ¿Solo el personal autorizado puede acceder a cierta información? ¿Se tiene establecido la periodicidad para cambio de clave? ¿Cuál es el máximo de intentos fallidos al ingresar una clave errónea?

3.7. Seguridad física y ambiental

Para su validación debemos responder si: ¿Se definió una política para la administración de la seguridad patrimonial?

3.8. Seguridad de las operaciones

Para su validación debemos responder si: ¿Se definió una política para la administración de la seguridad operativa? ¿Se definió política para proteger a organización de malware? ¿Las computadoras, teléfonos y tablets tienen instalados programas antivirus que se actualizan al menos a diario y están configurados para analizar automáticamente los archivos y sitios web que visita?

3.9. Seguridad de las comunicaciones

Para su validación debemos responder si: ¿Se definió una política para proteger las redes e instalaciones? ¿Se definió una política para proteger las transferencias de información? ¿Se tiene un procedimiento en caso de caídas de las líneas de comunicaciones?

3.10. Adquisición de sistemas, desarrollo y mantenimiento

Para su validación debemos responder si: ¿Se definió una política para el análisis y la especificación de los requisitos de seguridad de la información?

3.11. Relaciones con los proveedores

Para su validación debemos responder si: ¿Se definió una política de confidencialidad con los proveedores? ¿Se tiene un modelo de acuerdo de confidencialidad y seguridad?

3.12. Gestión de incidencias que afectan a la seguridad de la información

Para su validación debemos responder si: ¿Se definió una política para identificar y responder a los incidentes de seguridad de la información? ¿Se estableció un plan de contingencia ante una violación de la seguridad de información?

3.13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Para su validación debemos responder si: ¿Se definió una política para formar controles de continuidad de seguridad de la información? ¿Con que periodicidad se realizan copias de seguridad de los archivos? ¿Cuáles son las medidas de contingencia en caso se perdiera el acceso a Internet durante más de 24 horas?

3.14. Conformidad criptográfica

Para su validación debemos responder si: ¿Se definió una política para controlar el uso de las claves y los controles criptográficos? ¿Se realizan pruebas de penetración y auditorías para asegurar que procesos criptográficos cumplen con los estándares de seguridad?

4. CONCLUSIONES

Se concluye que el implementar el Sistema de Gestión de Seguridad de la información (SGSI), basado en la norma ISO 27001:2022 beneficia a las empresas u organizaciones, porque les brinda pautas y soporte de cómo mantener su información protegida y con un respaldo ante cualquier contingencia o ataque cibernético.

Se llega a la conclusión que no es necesario contar con una Certificación de Seguridad de la información, ISO 27001:2022 , pero es muy importante tener la información protegida y que a la vez cumpla con las tres dimensiones esenciales de confidencialidad, disponibilidad e integridad.

Se concluye además que adoptar un SGSI permite a la empresa u organización mantener una mejora continua en lo que corresponde a Seguridad de la información.

Se concluye que todos los controles de la Norma ISO 27002 sirven en la autoevaluación de cada empresa u organización para identificar su posición con respecto a la seguridad de su información y sobre todo estar prevenidos ante cualquier eventualidad.

REFERENCIAS

[1] AENOR (2023) Revista digital. https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

[2] Bureau Veritas Certificación (2023) https://capacitaciones.bureauveritas.com.pe/?s=sgsi

[3] Comisión económica para América Latina y el Caribe – CEPAL (2024) Desde el gobierno digital hacia un gobierno inteligente. *Ciberseguridad.* https://biblioguias.cepal.org/gobierno-digital/ciberseguridad.

[4] Diaz, L. Et las (2021) Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica. vol.32 nº. 5.* http://dx.doi.org/10.4067/S0718-07642021000500145

[5] Drucker, P. (2012). Retos de gestión para el siglo XXI. Rutledge.

[6] El Peruano (08/09/2023) Secretaría de Gobierno y Transformación Digital. https://busquedas.elperuano.pe/dispositivo/NL/2212869-1

[7] Integrated Assessment Services IAS (2020) Certificación ISO 27001 Perú. https://iasiso-latinamerica.com/pe/iso-27001-certification-in-peru/

[8] IBM (2024) ¿Que es la seguridad de datos? https://www.ibm.com/mx-es/topics/data-security

[9] Instituto Nacional de Ciberseguridad (2020). Glosario de términos de ciberseguridad. *Una guía de aproximación para el empresario.* Gobierno de España.https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[10] ISOTools Excellence (2023) ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber. https://www.isotools.us/2022/07/29/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesitas-saber/

[11] ISOTools Excellence (2023) Riesgos más importantes para las organizaciones en Latinoamérica*. Blog especializado en Seguridad de la Información y Ciberseguridad.* https://www.pmg-ssi.com/2023/04/riesgos-mas-importantes-para-las-organizaciones-en-latinoamerica/

[12] ISO 27000.ES (2024) https://www.iso27000.es/Acerca.html#Acercade

[13] Gavidia, J. (2023) Propuesta de modelo en seguridad informática en el control de un sistema informático aplicando ISO 27002 y CSF de NIST. *Ingeniería e innovación del futuro*. Período enero-junio 2023 Vol. 2 Nº. 1. DOI: https://doi.org/10.62465/riif.v2n1.2023.10

[14] Gobierno del Perú (2024) Presidencia del Consejo de ministros. Seguridad Digital. https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion

[15] LWP (2024) La web del programador. *Diccionario informático*. https://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=informacion

[16] Programa Nacional de Becas y Crédito Educativo-PRONABEC (2024). Sistema de Gestión de la Seguridad e la información. https://www.pronabec.gob.pe/sistema-de-gestion-de-seguridad-de-la-informacion/

[17] Puentes, Z (2021) Diseño de una guía de mejoramiento en los procesos del SGSI bajo la norma iso 27002:2015, ítem, 6.1 en el área de infraestructura de la empresa Corbeta S.A. Bogotá sede calle 31. (tesis licenciatura) *Universidad Cooperativa de Colombia.* https://repository.ucc.edu.co/server/api/core/bitstreams/ce95afde-2a97-463d-88e9-c5c60f07ed8c/content

[18] The International Organization for Standardization - ISO and The International Electrotechnical Commission- IEC (2022) . ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/es/search.html?PROD_isoorg_es%5Bquery%5D=iso%2027002

Fuentes de financiamiento:

Propia.

Conflictos de interés:

Los autores declaran no tener conflictos de interés.

Contribuciones de autoría:

Ambos autores participaron en el desarrollo del articulo.