Revista Innovación y Software
Vol. 4, No. 1, Mes Marzo-Agosto, 2023
ISSN: 2708-0935
Pág. 96-106
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Redes y seguridad informática
Recibido: 15/11/2022 | Aceptado: 27/12/2022 | Publicado: 30/03/2023

Identificadores persistentes:
ARK: ark:/42411/s11/a57
PURL: 42411/s11/a57

Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001

IT policy and information security management based on ISO 27001

Roy Guiller Ramos Mamami [1][0000-0001-7208-4977], **Rogelio Cahuaya Ancco** [2][0000-0003-1350-688X], **Roberto René Llanqui Argollo** [3][0000-0003-1871-5066]

[1] Universidad Nacional Jorge Basadre Grohmann, Perú. roy.ramos@unjbg.edu.pe
[2] Universidad Nacional Jorge Basadre Grohmann, Perú. rogelio.cahuaya@unjbg.edu.pe
[3] Universidad Nacional Jorge Basadre Grohmann, Perú. roberto.llanqui@unjbg.edu.pe

Resumen

La tecnología en los últimos tiempos ha ido cambiando a pasos agigantados y es natural aclimatarse a estos cambios tecnológicos y más aún por la pandemia covid-19 en el mundo, provocando el cambio drástico en las estrategias de las empresas. El artículo que se presenta a continuación pretende describir las causas y efectos de la norma ISO 27000 enfocándose a la norma ISO 27001.

En este sentido para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad. La metodología empleada para explicar las diversas áreas de impacto es la seguida por la norma ISO 27001 en el dominio que hace referencia al cumplimiento y que comprende: La norma ISO 27001 auxilia a las empresas en el cumplimiento de los requisitos legales, los cuales, tienen la finalidad de eludir la vulneración de la legislación o el incumplimiento de toda obligación legal de las entidades de cualquier requisito de seguridad.

Palabras clave: TIC's (Política Informática), cumplimiento, protección de datos, seguridad, propiedad intelectual.

Abstract

Technology in recent times has been changing by leaps and bounds and it is natural to acclimatize to these technological changes and even more so due to the covid-19 pandemic in the world, causing drastic change in company strategies. The article presented below aims to describe the causes and effects of the ISO 27000 standard, focusing on the ISO 27001 standard.

In this sense, to ensure an adequate information security policy that, in the absence of national legislation on the subject, must be based on international standards, comparative law and autonomy of will. The methodology used to

explain the various areas of impact is followed by the ISO 27001 standard in the domain that refers to compliance and which includes: The ISO 27001 standard helps companies comply with legal requirements, which have the purpose of avoiding the violation of the legislation or the breach of any legal obligation of the entities of any security requirement.

Keywords: *TIC's (Computer Policy), compliance, data protection, security, intellectual property.*

Introducción

Antes de la pandemia COVID-19 las herramientas digitales en las empresas eran muy pocas, a diferencia de otras organizaciones con mayor proporción que, si tienen el uso de tecnologías adecuadas norma ISO, pero cabe señalar que la gran mayoría de empresas informales y formales se limitan a tan solo a contar con un correo electrónico y tener una línea de internet básica. Las organizaciones enfrentan un desafío que es la transformación digital, para hacer frente a este contexto así mismo es necesario el uso de las herramientas tecnológicas de conectividad, conocimientos y de gestión. Pero este reto de adopción tecnológica trae altos costos de hardware, software.

La política de información es relevante e importante en estrategias y tomas de decisiones, para una organización, abarcando el área de las tecnologías de la información con el fin de asegurar de la información y datos. Identificando las reglas y procedimientos que deberán cumplir los usuarios al utilizar los recursos informáticos en una organización o empresa, su cumplimiento es fundamental para lograr los objetivos trazados.

El impacto de las Tecnologías de la Información y las Comunicaciones TIC no es ajeno al Derecho, por el contrario, cada día los avances de la tecnología imponen mayores retos a los operadores jurídicos, a los cuales hay que responder desde la legislación nacional si ésta existe, la legislación internacional, el derecho comparado, la autonomía de la voluntad privada, las mejores prácticas existentes en la industria y las normas que permitan dar un tratamiento uniforme a problemáticas que experimentan las organizaciones, cualquiera que sea la latitud en que estén ubicadas.

El desarrollo en nuestro país de normas jurídicas que respondan a los problemas que surgen del fenómeno de las TIC´s es mínimo. La Ley 527 de 1999 constituye uno de los pocos desarrollos importantes en este sentido. Esta situación genera un grado importante de inseguridad e incertidumbre no sólo para las organizaciones, sino para también los ciudadanos, en su condición de usuarios, consumidores y titulares de datos personales.

La información se ha convertido no sólo en un activo valioso, sino también estratégico en las organizaciones. La información puede ser protegida de muchas maneras. Desde el Derecho pudiera pensarse que se logra contar con un adecuado nivel de protección, con la encriptación, teniendo en cuenta que la mayor de las veces la compresión del tema tecnológico es poca; sin embargo, la encriptación es un mecanismo para otorgar a la información atributos de

confidencialidad, integridad, autenticidad, y dependiendo del mecanismo de encriptación, podría reputarse el no repudio. En la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras.

Así pues, el punto de partida de este estudio será acudir a los conceptos de Información y Seguridad, para lo cual se tendrá en cuenta las definiciones otorgadas por el Diccionario de la Real Academia de la Lengua Española, ello con el fin de partir de conceptos básicos.

El objetivo de este artículo es analizar parte legal como en la gestión de la protección de la información, de esta manera se puede concluir el valor que tiene la información como resultado de un conocimiento especializado en un área determinada y su seguridad, que a su vez requiere de ciertos mecanismos para garantizar su buen funcionamiento, en aras de protegerlo y asegurar su permanencia frente a los actos violentos que se pueden perpetrar contra la información.

Anteriormente la seguridad de la información estaba entendida como la aplicación de un conjunto de medidas de orden físico y lógico a los sistemas de información, para evitar la pérdida de la misma, siendo ésta una tarea de responsabilidad exclusiva de los departamentos de informática de las organizaciones.

Análisis Teórico

Importancia de la seguridad de la información

La seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de software, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia un modelo de gestión de la seguridad de la información en el que prima lo dinámico sobre lo estacional.

Para lograr niveles adecuados de seguridad se requiere el concurso e iteración de las disciplinas que tengan un impacto en el logro de este cometido, teniendo siempre presente que un sistema de gestión no garantiza la desaparición de los riesgos que se ciernen con mayor intensidad sobre la información.

Entonces, el problema es determinar cómo desde una disciplina como el Derecho se contribuye a la gestión de la seguridad de la información. Los enfoques de intervención jurídica podrían ser muchos; de hecho, no existe limitación alguna, para que una organización adopte las medidas que considere pertinentes con el fin de neutralizar un riesgo. La ISO 27 001 es una herramienta de gestión estratégica que conduce a lograr la protección de la información, bien en un contexto en el cual la empresa pretenda alcanzar una certificación,

o bien que sólo pretenda incorporar buenas prácticas de seguridad de la información, no sólo en sus procesos internos, sino también en sus procesos externos.

Métodos y Metodología computacional

La norma consagra un conjunto significativo de dominios que pretenden establecer un ciclo de seguridad lo más completo posible, advirtiendo que no todos ellos tienen impacto jurídico. Desde ya es importante mencionar que el enfoque que se propone se alimenta tanto de normatividad nacional como internacional, así como de otras fuentes del Derecho, en razón de la escasa legislación que existe.

La norma ISO 27 001:2013, contempla 14 dominios:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad de los recursos humanos.
4. Gestión de activos.
5. Controles de acceso.
6. Criptografía – Cifrado y gestión de claves.
7. Seguridad física y ambiental.
8. Seguridad operacional.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento del sistema.
11. Gestión de incidentes de seguridad de la información.
12. Cumplimiento.

Cumplimiento

El último capítulo del anexo A de la norma ISO 27001 está dedicado a controles que nos permitan garantizar el cumplimiento con las políticas, normas y legislación aplicable enfocándose principalmente en lo que se refiere a seguridad de la información.

Objetivo

- Cumplimiento de los requisitos y contractuales.
- Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.
- Revisiones de seguridad de la información.
- Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales.

Identificación de la legislación aplicable y de los requisitos contractuales

El control establece la necesidad de identificar de forma documentada todos los requisitos legales y contractuales que afecten a la organización, además de mantenerlos actualizados. Las leyes y reglamentos que afectan a una actividad son algo que evidentemente cambia con el tiempo y pueden ser distintas en cuanto a:

- Leyes o reglamentos sectoriales que afectan a una actividad.
- Leyes del parlamento europeo o leyes locales.
- Requisitos legales aplicables a tipos de información por su clasificación.

En la actualidad dado el crecimiento de los incidentes relacionados con la seguridad y la magnitud de su impacto han hecho que los gobiernos de todo el mundo sean conscientes de la necesidad de proteger a las personas y las empresas contra la gestión inadecuada de la información confidencial.

Derechos de propiedad intelectual

Este control nos requiere que se establezcan procedimientos que garanticen el uso del software de acuerdo a los términos previstos en la Ley de Propiedad.

Para ello se establecen los siguientes puntos a tener en cuenta para cumplir con este control:

- Se dispone de una política de uso legal de productos de software.
- Se asegura la no violación de derechos de copia.
- Dónde se compra los productos de software.
- Se mantiene la política de licencias del software comprado.
- Controlar el número máximo de usuarios por licencia.
- Revisar periódicamente que se estén utilizando solamente productos software con licencia.
- Cumplir con los derechos de copia de material audiovisual, libres e informes.
- Comunicar al personal la política de uso legar de software aclarando que cosas están permitidas y cuáles no.
- Advertir al personal sobre las consecuencias de la violación de las políticas de uso legal de software estableciendo las medidas disciplinarias oportunas.
- Identificar (listado de activos) los activos de información que estén afectados por derechos de propiedad intelectual.
- Mantener la documentación que justifique o acredite la propiedad de las licencias (discos, manuales, etc.).

Protección de los registros

Este control nos pide mantener un análisis de los requisitos contractuales legales en cuanto a las obligaciones de debido control sobre la protección de los registros en cuanto a evitar su pérdida, falsificación o acceso no autorizado.

Se clasifican los registros de información y aplica los controles necesarios según los requisitos legales:

- Registros contables.
- Bases de datos.
- Bases de datos de transacciones.
- Registros de auditoría (propios del sistema de Gestión de la Seguridad de la Información).

- Procedimientos operativos.
- Registros documentales en papel, microfichas, archivos electrónicos.
- Archivos cifrados (contraseñas, firmas digitales).

Para cumplir con la protección de los registros se nos requiere revisar el cumplimiento con:

- La definición y publicación de las directrices sobre la retención, almacenamiento, tratamiento y eliminación de os registros y la información.
- Mantenimiento de un calendario de retenciones donde se identifique los registros y los períodos de tiempo que deberían retenerse.
- Mantenga un inventario de los registros de información clave o critica.

Protección de los datos y privacidad de la información personal

Este control nos requiere el establecimiento de controles para el cumplimiento de la legislación en materia de cumplimiento con la legislación vigente en materia de protección de datos personales.

Regulación de los controles criptográficos

En caso de utilizar mecanismos de cifrado deben tenerse en cuentas las normativas sobre uso de controles criptográficos vigentes. Deberemos tener en cuenta leyes como:

- La Ley General de Telecomunicaciones.
- Ley de Firma Electrónica.

Limitaciones en el uso de medios criptográficos

En muchos países existen limitaciones en el uso de medios criptográficos por lo que tendremos que tener en cuenta estas limitaciones o restricciones en las importaciones o exportaciones de Hardware y/o Software para funciones criptográficas. También deberemos considerar si existen métodos obligatorios de cifrado de

información y cumplir los requisitos legales del cifrado de información establecidos por los reglamentos de cada país.

Códigos de conducta

Determinadas organizaciones y organismos pueden elaborar códigos de conducta sobre el tratamiento de datos personales. En este caso si nos adherimos a dichos códigos deberemos cumplir con los requisitos en cuanto al uso y obligatoriedad de los sistemas de cifrado.

Evaluación de riesgos

La evaluación de riesgos, también obligatoria en el reglamento RGPD sobre el tratamiento de datos personales puede determinar la necesidad de utilizar cifrado de datos como resultado de un control necesario para mitigar o evitar un riesgo para la seguridad de la información.

Cifrado legal

En el caso que nos veamos obligados a cifrar datos según lo expuesto hasta ahora deberemos dedicar los recursos necesarios para cumplir con estos requisitos. Sin embargo, cualquier sistema de cifrado no es suficiente ya que los archivos PDF o archivos comprimidos ZIP con clave no son considerados válidos para garantizar que la información no sea inteligible ni manipulada por terceros.

Revisión independiente de la seguridad de la información

Las revisiones deben ser llevadas a cabo por personal independiente al personal que es auditado. Aunque pueden ser llevadas a cabo por personal interno siempre de áreas o departamentos independientes al auditado, conviene que de forma regular se realicen auditorias de cumplimiento de la seguridad de la información por personal externo. Las auditorías realizadas por personal externo siempre podrán aportar beneficios como:

- Garantizar la independencia de las revisiones o auditorias.
- Aportar un punto de vista imparcial.

- Aportar la experiencia de profesionales de la seguridad de la información que conocen otras organizaciones y pueden aportar mejoras.

Cumplimiento de la política y las normas de seguridad

Este control nos pone como requisito la necesidad de que los responsables de cada área deben revisar que los procedimientos de la organización sean aplicados de acuerdo a los requisitos definidos.

Para ello los responsables deberían:

- Determinar la forma de revisar cómo se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables.
- Tener en cuenta la implementación de sistemas de medición automática y herramientas de informes.

Cuando se identifican incumplimientos se deberá:

- Identificar las causas.
- Evaluar la necesidad de tomar medidas.
- Implementar las acciones correctivas apropiadas.
- Revisar la eficacia de las acciones correctivas.
- Identificar las deficiencias y debilidades del sistema.

Revisión del cumplimiento técnico

Para la evaluación de los sistemas de información debe revisarse periódicamente si están configurados correctamente de acuerdo a las reglas y políticas definidas:

- Identificar fallos en las actualizaciones de los sistemas.
- Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para el sistema.

Resultados y discusión

Cada cierto tiempo, la Seguridad de la Información basada en la ISO 27001 tiene que examinarse. Estas revisiones se realizan a través de diferentes políticas de seguridad y tiene que auditarse que las plataformas técnicas y los sistemas de información satisfagan la totalidad de normas de implementación de seguridad y controles de seguridad documentados que sean aplicables. El control de que se está llevando a cabo el cumplimiento técnico únicamente tiene que estar revisado por los sujetos cualificados y además, estas personas tienen que estar autorizadas por la entidad, aunque puede pasar que lo realice otra persona bajo la supervisión del responsable. Se considera un elemento de reconocida importancia, por lo que hablamos del examen que tienen que pasar las entidades de sus sistemas operativos con el fin de asegurar que los softwares y los hardware han sido implantados perfectamente.

Conclusiones

La norma ISO 27001 auxilia a las empresas en el cumplimiento de los requisitos legales, los cuales, tienen la finalidad de eludir la vulneración de la legislación o el incumplimiento de toda obligación legal de las entidades de cualquier requisito de seguridad. La política informática, como administrador de riesgos, se encarga de dotar de seguridad los diferentes activos de información de una organización; desde esa perspectiva se requiere una gestión jurídica permanente de los riesgos, amenazas y vulnerabilidades, como medio para adoptar las medidas y controles que disminuyan los mismos. Las Tecnologías de la Información reclaman de la política informática respuestas innovadoras y globales respecto de los retos que le son intrínsecos; por tanto, los operadores jurídicos deben estar capacitados y entrenados para apoyar a la sociedad en la solución de las problemáticas propias de la política informática.

Referencias

[1] Marlon A. Di Luca. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso*. Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso (redalyc.org)

[2] Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. http://dx.doi.org/10.20511/pyr2020.v8n3.786. [Accessed: Set, 2020].

[3] Diana L. Carvajal, A. Cardona, F. J. Valencia. (2020). *Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana*. Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana | Entre Ciencia e Ingeniería (ucp.edu.co)

[4] Erick G., Harold N., Jorge L. Díaz, J. Patiño. (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*. Development of an information security management system based on analysis methodology and risk identification in university libraries (scielo.cl)

[5] Navira G. Angulo Murillo, María F. Zambrano Vera, G. García Murillo, F. Bolaños-Burgos. (2018). *Propuesta metodológica de seguridad de información para proveedores de servicios de internet en ecuador.* Microsoft Word - 165-176 (core.ac.uk)

[6] David A. Aguirre Mollehuanca. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú S.A*. http://hdl.handle.net/20.500.12404/5677

[7] Juan D. Aguirre Cardona, C. Aristizábal Betancourt. (2013). *Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial La Ofrenda*. https://hdl.handle.net/11059/4117

[8] Alexander, A. G., & Buitrago, L. J. (2007). *Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001: 2005*.

[9] Flores, L. C. A. (2013). *Diseño de un sistema de gestión de seguridad de información para un instituto educativo (Doctoral dissertation, Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Mención: Ingeniería Informática).* http://hdl.handle.net/20.500.12404/4721

[10] Ampuero Chang, C. E. (2011). *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. http://hdl.handle.net/20.500.12404/933*

[11] Aráoz Severiche, I. (2020). *Implementación ISO/IEC 27001:2013: Un enfoque práctico (Spanish Edition) Edición Kindle.*

[12] Calder, A. (2017). *ISO27001/ISO27002: A Pocket Guide.*

[13] García, F. Albarrán, S. (2015). *Guía para Implantar un Sistema de Gestión de Seguridad de Información: Basada en la Norma ISO/IEC 27001 (Spanish Edition).*

[14] Fernández, C. Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*.

[15] Muñoz, C. (2002). *Auditoria en sistemas computacionales. Pearson Educación.*

Roles de Autoría

Roy Guiller Ramos Mamami: Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Rogelio Cahuaya Ancco:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Roberto René Llanqui Argollo:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original.