Sinergias educativas
ISSN: 2661-6661
compasacademico@icloud.com
Grupo Compás
Ecuador

Implicancias de la NTP ISO/IEC 27001:2008 EDI, en la seguridad de la información en los ministerios del estado peruano, 2018

Implications of the NTP ISO / IEC 27001: 2008 EDI, on information security in the Peruvian state ministries

Fernando Rolyn Flores Solís
Maestro en Ingeniería de Sistemas por la Universidad Nacional del Callao, Callao, Perú;
pcelfflo@upc.edu.pe; rolynflores@gmail.com; https://orcid.org/0000-0002-6105-3371
https://scholar.google.com/citations?user=aQ8FMFUAAAAJ&hl=es

Giovana Edith Ruiz Villavicencio
Magister en Contabilidad; Universidad Particular San Martin De Porras, Perú;
gruizv@cientifica.edu.pe; gioruiz8@gmail.com; https://orcid.org/0000-0001-9216-4456;
https://scholar.google.es/citations?hl=es&pli=1&user=dmZY1XMAAAAJ

Ricardo Edmundo Ruiz Villavicencio
Doctor en Administración, Universidad Inca Garcilaso de la Vega. Lima, Perú;
reruizvi@ucvvirtual.edu.pe; catedra2020@gmail.com; http:// orcid.org: 0000-0002-1353-1463;
https://scholar.google.es/citations?user=K7nNqcIAAAAJ&hl=es

Godofredo Pastor Illa Sihuincha
Doctor en Educación por la Universidad Nacional de Educación Enrique Guzmán y Valle, Lima, Perú;
gillas@ucvvirtual.edu.pe; gilla@une.edu.pe; https://orcid.org/0000-0002-2532-3194;
https://scholar.google.es/citations?user=irsWSOQAAAAJ&hl=es

Resumen

En la actualidad, el uso de las tecnologías de la información y comunicaciones se han convertido en el principal soporte de los procesos de negocio tanto privados y públicos incluso de la vida diaria de los ciudadanos. En tal sentido, el Estado Peruano a través de la Oficina Nacional de Gobierno Electrónico (ONGEI) prioriza el fortalecimiento de la sociedad de la Información a través de un plan denominada Agenda Perú. Para comprobar si la implantación de la norma ha permitido mejorar la seguridad de la información en los Ministerios del Estado Peruano, se realizó una investigación cuantitativo correlacional de tipo no experimental y transversal, determinando el grado de implantación de la norma y el nivel de incidentes de seguridad de información en la población seleccionada, que para efecto del estudio fueron 18 ministerios y la Presidencia del Consejo de ministros. El resultado señalo un coeficiente de correlación positiva de .636 y una significancia de .003; determinándose el grado de implantación de la norma en los ministerios es de 2.83, encontrándose en el nivel de planificación respecto a cinco niveles de implantación incremental (organización, planificación, despliegue, revisión y consolidación) propuesto por la ONGEI.
Palabras clave. Norma técnica, confidencialidad, integridad, disponibilidad.

Abstract

At present, the use of information and communication technologies have become the main support for both private and public business processes, including the daily life of citizens. In this sense, the Peruvian State through the National Electronic Government Office (ONGEI) prioritizes the strengthening of the Information society through a plan called Agenda Peru. To verify whether the implementation of the standard has allowed the improvement of information security in the Ministries of the Peruvian State, a quantitative correlational investigation of a non-experimental and cross-sectional type was carried out, determining the degree of implementation of the standard and the level of incidents of Information security in the selected population, which for the purpose of the study were 18 ministries and the Presidency of the Council of Ministers. The result indicated a negative correlation coefficient of -.636 and a significance of .003; Determining the level of implementation of the standard in the ministries is 2.83, being at the planning level with respect to five levels of incremental implementation (organization, planning, deployment, review and consolidation) proposed by the ONGEI.
Keywords. Technical standard, confidentiality, integrity, availability.

Introducción

En el año 2003, se desarrolló en Ginebra la cumbre Mundial de la Información, auspiciada por la Organización de Naciones Unidas y la Unión Internacional de Telecomunicaciones donde se planteó como compromiso de los estados, la creación de la sociedad de la información. Es por ello, que la Oficina Nacional de Gobierno electrónico (ONGEI) creo en junio de 2003 la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI) la cual elaboró y publicó en el año 2006, el Plan de Desarrollo de la Sociedad de la Información en el Perú, también denominada Agenda Digital Peruana (CODESI, 2011); relacionado con el objetivo de Promover una administración Pública de Calidad Orientada a la Población, donde la estrategia es Implementar mecanismos para la mejora de la Seguridad de la información, la cual a su vez propone el desarrollo una estrategia de ciberseguridad con el objetivo de minimizar los riesgos de sufrir algún tipo de incidente en las infraestructuras críticas y la disuasión del crimen cibernético (Iriarte, 2019).

El modelo de ciberseguridad española, define como elementos esenciales de su política, conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta. En esta medida, se ha establecido como línea de acción para garantizar la implantación del Esquema Nacional de Seguridad (Departamento de Seguridad Nacional, 2013), constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Fue aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias (Presidencia del Estado Español, 2010; Esquema Nacional de Seguridad).

Otro modelo es el caso mexicano con el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de seguridad de la información (MAAGTICSI) que se fundamenta en la necesidad de homologar los procesos contenidos en la Estrategia Digital Nacional, para agilizar y optimizar su gestión al interior de las dependencias y entidades de la Administración Pública Federal y en la Procuraduría General de la República, para ello se emitió políticas y disposiciones para la estrategia digital nacional, así como establecer el manual administrativo de aplicación general en dichas materias (México, 2014).

Del mismo modo en nuestro país, la ONGEI por medio de su agenda digital prioriza el fortalecimiento de la sociedad de la información a través de un plan de desarrollo de la sociedad de la información, el cual incluye entre sus estrategias implementar mecanismos para la mejora de la seguridad de la información, por lo que ha venido recomendado la implantación de sistemas de gestión de seguridad de la información basados en las normas técnicas peruanas NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Esta resolución toma como acciones; la derogatoria de las resoluciones ministeriales anteriores referentes a la seguridad de la información, establecer un cronograma de implantación incremental de la NTP y establece una lista de instituciones prioritarias que deberán iniciar el proceso.

1.1. ISO/IEC 27001:2005 Sistema de Gestión de Seguridad de la Información

Esta norma internacional especifica los requisitos para el establecimiento, implantación, mantenimiento y mejora continua del sistema de seguridad de la información dentro del contexto de la organización. Esta norma internacional también incluye los requisitos para la evaluación y tratamiento de los riesgos de la información adaptados a las necesidades de la organización. Los requisitos establecidos son genéricos y son elaborados para ser aplicados

en toda organización, independientes del tipo, tamaño y naturaleza (ISO & IEC, 2005).

1.1.1. Evolución de la Norma

La norma ha evolucionado desde su aparición en Inglaterra, siendo tomada en el 2005 por la Organización Internacional para la estandarización (ISO) para oficializarla como el estándar en Seguridad de la Información (Alexander, 2007).

Tabla 1

Evolución de la norma

Norma	Base
7799-1:1995	ecesora del código para la gestión de la seguridad de la información.
7799-2:1999	ma creada para que las empresas se certificaran y es auditable.
/IEC 17799:2000	SO adopta y oficializa en base de la norma británica BS 7799-1:1999
7799-2:2002	isión de la BS 7799-2:1999
17799:2005	isión de la ISO 17799:2000
27001:2005	isión al BS 7799-2:2002
27001:2013	isión de la ISO/IEC 27001:2005

1.1.2. Familia de la ISO 27001

Es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño (López & Javier, 2015).

Tabla 2

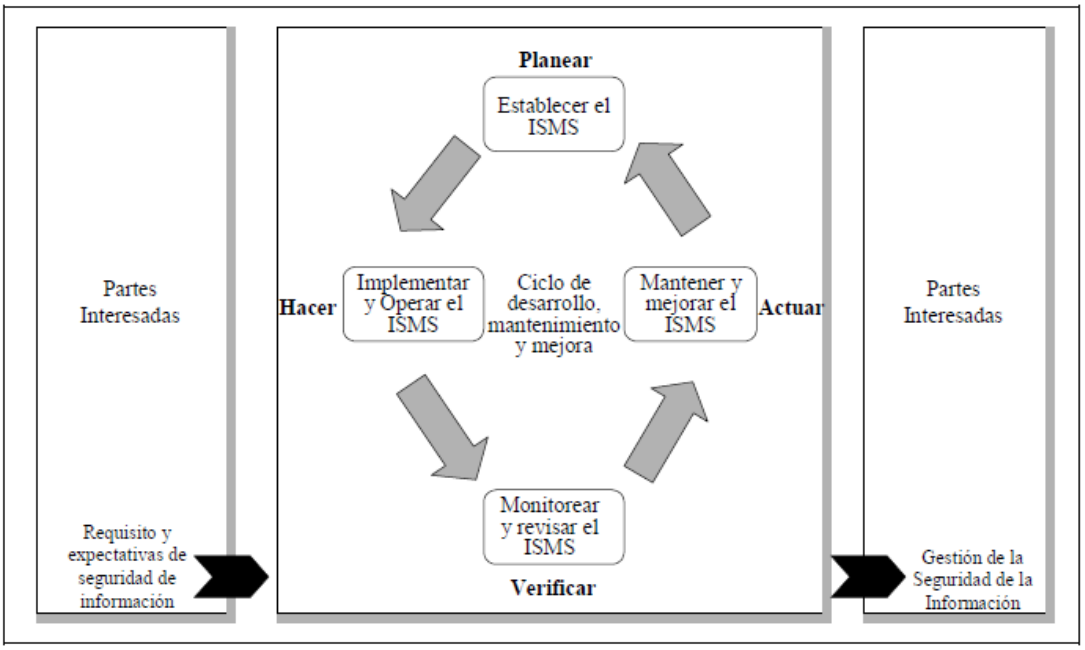
Clasificación de la norma

Norma	Descripción
ISO/IEC 27000	Contiene vocabulario del estándar para el Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27001	Norma que establece los requisitos para la implantación del SGSI. Esta norma es certificable.
ISO/IEC 27002	Código de buenas prácticas para el manejo del SGSI.
ISO/IEC 27003	Directrices para la implantación del SGSI
ISO/IEC 27004	Métricas para la gestión de la seguridad de la información.
ISO/IEC 27005	Contiene modelos de gestión de riesgo para el SGSI
ISO/IEC 27006:2007	Contiene los requisitos para la acreditación de las organizaciones que proporcionan la certificación de los SGSI
ISO/IEC 27007	Guía para la auditoria del SGSI
ISO/IEC 27799:2008	Guía para implementar el SGSI

1.1.3. Naturaleza de un SGSI

Nos exhorta a entender la ISO/IEC 27001 como un modelo para el establecimiento, implantación, operación, monitoreo, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información para cualquier clase de organización. Esta norma tiene como base el denominado ciclo de Deming que se refiere a Planear, Actuar, Revisar y Hacer (Plan, Act, check y Do) (Alexander, 2007).

Figura 1. Modelo PDCA aplicado al proceso SGSI. Tomado de NTP ISO/IEC 27001:2008



1.1.4. NTP/IEC 27001:2008 Sistema de Gestión de Seguridad de la Información

Esta Norma Técnica Peruana de Seguridad de la Información ha sido preparada en base a la ISO/IEC 27001:2005 con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener, y mejorar un efectivo Sistema de Gestión de Seguridad de la Información. Esta NTP puede usarse en el ámbito interno y externo de las organizaciones (Norma Técnica Peruana NTP-ISO/IEC 27001:2008).

1.1.5. NTP/IEC 27001:2014 Sistema de Gestión de Seguridad de la Información

Esta Norma Técnica Peruana de Seguridad de la Información está basada en la ISO/IEC 27001:2013, la cual, tiene cambios importantes en la implantación del SGSI, como por ejemplo la elección sobre cómo ponerla en práctica, no solamente mediante el enfoque de procesos. Además, la nueva estructura contiene 10 elementos sincronizados con las demás ISO's de gestión (Norma Técnica Peruana NTP-ISO/IEC 27001:2014, 2014).

1.1.6. Marco regulatorio Legal

De acuerdo al Decreto Supremo N° 063-2007-PCM la Oficina Nacional de Gobierno Electrónico e Informática, es el órgano especializado que depende jerárquicamente del Presidente del Consejo de Ministros, encargada de dirigir como ente rector, el Sistema Nacional de Informática, y de implementar la Política Nacional de Gobierno Electrónico e

Informática. La Oficina Nacional de Gobierno Electrónico e Informática coordina con la Secretaria de Gestión Pública y brinda asistencia técnica en la implantación de los procesos de innovación Tecnológica para la modernización de la Administración Pública, teniendo como funciones las siguientes:

a. Actuar como ente rector del Sistema Nacional de Informática, para lo cual emite las directivas o lineamientos que permitan la aplicación de dicho Sistema.
b. Proponer la Estrategia Nacional de Gobierno Electrónico, así como coordinar y supervisar su implantación.
c. Desarrollar acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática y supervisar el cumplimiento de la normativa correspondiente
d. Coordinar y supervisar la integración funcional de los sistemas informáticos del Estado y promover el desarrollo de sistemas y aplicaciones de uso común en las entidades de la Administración Pública.
e. Coordinar y supervisar el desarrollo de los portales de las entidades de la Administración Pública para facilitar la interrelación de las entidades entre sí y de éstas con el ciudadano, con el fin de establecer la ventanilla única de atención.
f. Administrar el Portal del Estado Peruano.
g. Proponer los lineamientos de política de contrataciones electrónicas del Sistema Electrónico de Adquisiciones y Contrataciones del Estado - SEACE.
h. Brindar asistencia técnica a las entidades de la Administración Pública para la implantación de proyectos tecnológicos en materia de su competencia.
i. Formular propuestas para impulsar el proceso de desarrollo e innovación tecnológica para la mejora de la gestión pública y modernización del Estado promoviendo la integración tecnológica.
j. Aprobar los estándares tecnológicos para asegurar las medidas de seguridad de la información en las entidades de la Administración Pública.
k. Fomentar una instancia de encuentro con representantes de la Administración Pública y del sector privado, con el fin de coordinar y potenciar los distintos esfuerzos tendientes a optimizar un mejor aprovechamiento de las tecnologías aplicadas a la modernización de la Gestión Pública.
l. Emitir opinión técnica respecto de las autógrafas, proyectos de Ley y proyectos normativos que las Alta Dirección somete a su consideración. Dicha opinión versará respecto de las competencias que le han sido asignadas.
m. Emitir opinión técnica en materia de su competencia.
n. Otras funciones que le sean encomendadas por el Presidente del Consejo de Ministros.

La función relacionada con la investigación, es la que permite aprobar los estándares tecnológicos para asegurar las medidas de seguridad de la información en las entidades de la Administración Pública (NTP/IEC 27001:2008).

Resolución Ministerial N° 224-2004-PCM.

El 23 de julio de 2004 se publicó la resolución ministerial para que, la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, en coordinación con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, ha recomendado la aplicación y uso obligatorio de la Norma Técnica Peruana antes mencionada en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar a la creación de la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente importante para dicho objetivo.

Se aprobó el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI, Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información, en todas las entidades integrantes del Sistema Nacional de Informática, documento que será publicado en el portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe). Además, la Norma Técnica Peruana señalada en el artículo precedente, se aplicará a partir del día siguiente de la publicación de la presente Resolución Ministerial, teniendo las Entidades antes mencionadas un plazo de dieciocho (18) meses para su implantación, por lo que deberán considerar en sus respectivos Planes Operativos Informáticos (POI) las actividades necesarias con esa finalidad.

Resolución Ministerial N° 246-2007-PCM.

Mediante esta resolución del 22 de agosto de 2007 se aprueba el uso obligatorio de la NTP-ISO/IEC 17799:2007, Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información, en todas las entidades públicas que pertenecen al Sistema Nacional de Informática. Esto significaba el reemplazo de la NTP-ISO/IEC 17799:2004. Esta resolución no establece ningún plazo para la implantación de la norma.

Resolución Ministerial N° 197-2011-PCM.

La resolución del 14 de julio de 2011 establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana NTP ISO/IEC 17799:2007 EDI. Código de buenas Prácticas para la gestión de la Seguridad de la Información. Se establece como fecha límite el 31 de diciembre de 2012, para que las entidades de la Administración Pública implementen el plan de la norma. Además, proporciona una lista de entidades del Estado que serán auditadas luego del plazo cumplido.

Resolución Ministerial N° 129-2012-PCM.

Esta resolución el 23 de mayo de 2012 aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/ IEC 27001:2008 EDI Tecnología de la Información, técnicas de seguridad y sistemas de gestión de seguridad de la Información, además de sus requisitos; las cuales deben ser implementadas en todas las entidades integrantes del Sistema Nacional de Informática. La implantación de los Sistemas de Seguridad de la Información en las entidades integrantes del Sistema Nacional de Informática deberá empezar con la aplicación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información, técnicas de seguridad, sistemas de gestión de seguridad de la Información y requisitos; cuyos controles deberán ser implementados de acuerdo a las recomendaciones de la Norma Técnica Peruana NTP-ISO/ IEC 17799: 2007 EDI Tecnología de la Información y código de buenas prácticas para la gestión de la seguridad de la información, dispuesto por la Resolución Ministerial N° 246-2007-PCM.

2. Materiales y métodos

El estudio es cuantitativo porque cumple con sus principales características como medir fenómenos, utiliza estadística, prueba de hipótesis y realiza un análisis causa-efecto y correlacional ya que permite conocer la relación entre dos variables, como son, la Implantación de la NTP 27001:2008 EDI y la Seguridad de la Información, en una determinada población, los Ministerios del Estado Peruano y de la Presidencia del Consejo de Ministros (Hernández, Fernández, & Baptista, 2014) (Aguirre et al., 2019); es de tipo no experimental – transversal, porque no se varia de forma intencional las variables

independientes para ver su efecto en otras variables, además nos permite recolectar datos en un único momento para determinar la relación entre la implantación de la NTP 27001:2008 EDI y la Seguridad de la Información en los ministerios del Estado Peruano y de la Presidencia del Consejo de Ministros.

La población para esta investigación serán todos los ministerios del Estado Peruano y la Presidencia de Consejo de Ministros que tienen la obligación de implementar la NTP-ISO/IEC 27001:2008 por resolución Ministerial N° 129-2012-PCM. Además, en salvaguarda de la información de las instituciones encuestadas se codificarán los nombres de cada una de ellas con la denominación *Ministerio NN*. Se utilizó un muestreo probabilístico de tipo aleatorio simple, el cual se caracteriza porque el investigador elige de manera aleatoria la población que estudia (Carrasco, 2005) (Barros & Turpo, 2018); se empleó como técnica las encuestas y como instrumento los cuestionarios para ser desarrollada por el oficial de seguridad, encargado de la Oficina de Tecnologías de la Información o especialista de cada Ministerio del Estado Peruano y de la Presidencia del Consejo de Ministros.

3. Resultados

En este punto se presentan los resultados del estudio. En primer lugar, se presentan los hallazgos en cuanto a la implantación por Ministerio y el nivel de incidentes de la Norma Técnica Peruana ISO/IEC 27001:2008; luego, se presenta los resultados inferenciales.

Tabla 3

Grado de implantación por ministerio

Ministerios	Grado	Nivel de incidencias
Ministerio 01	4.33	1.00
Ministerio 02	2.33	4.67
Ministerio 03	3.17	3.00
Ministerio 04	2.33	3.33
Ministerio 05	2.17	3.67
Ministerio 06	5.00	1.67
Ministerio 07	4.50	3.00
Ministerio 08	1.17	3.00
Ministerio 09	0.33	4.00
Ministerio 10	5.00	1.67
Ministerio 11	1.33	3.67
Ministerio 12	5.00	2.33
Ministerio 13	2.00	4.00
Ministerio 14	2.00	3.00
Ministerio 15	1.17	3.00
Ministerio 16	0.67	3.00
Ministerio 17	5.00	1.00
Ministerio 18	5.00	1.67
Ministerio 19	0.67	3.00
Promedio	**2.80**	**2.83**

Nota. El grado de implementación de la Norma Técnica Peruana ISO/IEC 27001:2008, alcanzó el 2.80 > 2.50; por lo tanto, se considera que está logrando implantarse de manera incremental. En cuanto al nivel de incidencias, el promedio alcanzado es el 2.83 > 2.50; por lo tanto, las incidencias han sido superadas y están en proceso de mejora continua en los Ministerios.

Tabla 4

Prueba de hipótesis

Factores	**CC**	***p***	1-β	f^2
(VX→DY1) Implantación → Confidencialidad de la información	.574**	.001	1	.748
(VX→DY2) Implantación → Integridad de la información	.518**	.023	1	.723
(VX→DY3) Implantación → Disponibilidad de la información	.574**	.010	1	.748
(VX→VY) Implantación → Seguridad de la información	.636**	.023	1	.823

* Sig. < .05 / ** Sig. < .01 / *f2= .10 bajo, .30 media, .50 alta.*

La hipótesis sobre la implantación de la norma y la confidencialidad de la información, quedo demostrada con un nivel de correlación de .574 y un Sig. (bilateral)= .001; con un tamaño de efecto (*f2)* grande (.748), y una potencia (1-β) = 1. La hipótesis sobre la implantación de la norma y la integridad de la información, quedo demostrada con un nivel de correlación de .518 y un Sig. (bilateral)= .023; con un tamaño de efecto (*f2)* grande (.723), y una potencia (1-β) = 1. La hipótesis sobre la implantación de la norma y la disponibilidad de la información, quedo demostrada con un nivel de correlación de .574 y un Sig. (bilateral)= .010; con un tamaño de efecto (*f2)* grande (.748), y una potencia (1-β) = 1. La hipótesis sobre la implantación de la norma y la seguridad de la información, quedo demostrada con un nivel de correlación de .636 y un Sig. (bilateral)= .023; con un tamaño de efecto (*f2)* grande (.823), y una potencia (1-β) = 1.

4. Discusión

Para comprobar si la implantación de la norma ha permitido mejorar la seguridad de la información en los Ministerios del Estado Peruano, mostrando avances significativos en su implantación; sin embargo, por la envergadura y complejidad de las instituciones, está en procesos de adaptación y mejora constante, considerado de necesidad en la era de la información; tal como lo afirma Calisaya (2012), quien propone la estructura metodológica para la seguridad de la información utilizando normativa gubernamental que garantice el cumplimiento de la normativa de la Superintendencia de Bancos y Seguros (SBS). Este documento revisa toda la normativa existente en el Estado que debe cumplir cualquier institución que este bajo la supervisión de la SBS, además propone la metodología que se debería implantar. Por otra parte, Chávez Bravo (2013), evalúa los modelos de seguridad en capas existentes que se vienen aplicando como buenas prácticas de seguridad de la información para aplicarlos específicamente en el Ministerio de Economía y Finanzas. Además, propone la alineación de los niveles de seguridad de la defensa en profundidad en computación con la norma internacional ISO 27001 Sistema de Gestión de Seguridad de la Información. En ese sentido, Aguirre (2014) muestra los procesos realizados en la implantación del Sistema de Gestión de Seguridad de la Información basado en la NTP ISO 27001:2008 en la empresa estatal Servicios Postales de Perú S.A. (SERPOST). Esta implantación es realizada en base a la resolución ministerial N° 129-2012-PCM. Finalmente,

Huamán (2014) establece un procedimiento de auditoría de cumplimiento para la NTP/IEC 17799/2007 en el marco de COBIT 5.0 para las instituciones del Estado, como parte del proceso de implantación del a NTP/IE 27001:2008. Este procedimiento permite realizar una auditoría de cumplimiento para determinar si las instituciones del Estado han logrado implantar satisfactoriamente la norma.

5. Conclusiones

La NTP 27001:2008 EDI exigida a implantarse por la Oficina Nacional de Gobierno Electrónico e Informática en el año 2012 en todas las instituciones del Estado Peruano, tiene relación directa en la Seguridad de la Información de los Ministerios del Estado Peruano. El grado de implantación en promedio de la NTP 27001:2008 EDI en los Ministerios del Estado Peruano es de 2.80, que los ubica en general en el nivel de Planificación, lo que significa que se han desarrollado actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del Sistema de Gestión de Seguridad de la Información. La Oficina Nacional de Gobierno Electrónico (ONGEI) ha intentado desde el 2004 implantar medidas de seguridad de la información en el Estado Peruano, a través de la publicación de resoluciones ministeriales que obliguen a las entidades adscritas a ella implantar Normas Técnicas. Esta normatividad define el *qué hacer*, pero no el "Como", que se ve reflejado en la baja cantidad de Ministerios que han terminado el proceso de implantación. Los Ministerios del Estado Peruano han sido afectados en su seguridad de la información la cual se reflejan en la cantidad de incidentes que han tenido del 2012 a la actualidad considerándose en un nivel medio - alto.

Referencias

Aguirre, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú*. Lima: Pontificia Universidad Católica del Perú.

Aguirre, L. A., López, J. E., & Villamizar, D. F. (2019). Revisiones y reflexiones en la educación física: un camino de lo conceptual a lo investigativo en la escuela.

Alexander, A. (2007). Diseño de un sistema de gestión de seguridad de información. Bogotá Colombia: Alfaomega colombiana.

Barros Bastidas, C., & Turpo Gebera, O. (2018). Factors influencing the scientific production of university professors: a systematic review. Factores Que Influyen En La Producción Científica de Los Docentes Universitarios: Una Revisión Sistemática., 11(22),225234.http://10.0.85.43/pensam.v11i211.276%0Ahttps://ezproxy.uniandes.edu.co:8443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=141223533&lang=es&site=ehost-live

Calizaya, N. (2012). Metodología de auditoria gubernamental para revisión del cumplimiento de la normativa peruana por la SBS relacionada a seguridad de la información. Lima: Universidad Tecnológica del Perú.

Carrasco, S. (2005). *Metodología de la investigación científica*. Lima: San Marcos.

Chávez, B. (2013). Aplicación del modelo de seguridad en capas basado en el esquema de defensa en profundidad en computación para Instituciones del Estado. Lima: Universidad Tecnológica del Perú.

CODESI (2011). *Plan de Desarrollo de la Sociedad de la Información en el Perú.* la Agenda Digital 2.0. Lima: PCM.

Departamento de Seguridad Nacional (2013). Estrategia de Ciberseguridad Nacional España. Madrid: Presidencia de Gobierno.

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación*. México D.F.: McGraw-Hill.

Huamán, F. (2014). Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la Norma Técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano. Lima: Pontificia Universidad Católica del Perú.

INDECOPI (2008). Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Lima: INDECOPI.

INDECOPI (2014). Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Lima: INDECOPI.

ISO, O. I., & IEC, C. E. (2005). Norma Internacional ISO/IEC 27001:2005. Geneva, Suiza:

ISO.

Iriarte, E. (2019). Definiendo la Cuarta Revolución Industrial desde la realidad peruana. Comex, 23(263), 1-36.

López, A., & Javier, R. (14 de junio de 2015). ISO 27000.es. Obtenido de http://iso27000.es/

México, s/a (2014). Manual administrativo de aplicación general en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información. México D.F.: Diario Oficial México.

Presidencia del Estado Español (2010). *Esquema Nacional de Seguridad*. Madrid: Boletín Oficial del Estado.

Standardization, T. I., & Commission, T. I. (15 de 01 de 2014). ISO / IEC 27000. *Information technology - Security techniques - Information security management systems - Overview and Vocabulary. Suiza: ISO copyright office*. Geneva, Suiza: ISO.