Factores que afectan la implementación del sistema de gestión de seguridad de la información en las Entidades Públicas Peruanas

Javier Alfonso Seclén Arana

javier.seclen@unmsm.edu.pe, jaseclen@gmail.com

Facultad de Ingeniería de Sistemas e Informática - FISI
Universidad Nacional Mayor de San Marcos (UNMSM)
Lima, Perú

Resumen: *En este artículo, se presenta una investigación que identifica las causas que restringen la implementación del Sistema de Gestión de Seguridad de la Información -SGSI- en las Entidades Públicas Peruanas. El problema fundamental que da origen a este estudio es que, en la actualidad, a pesar de que el Gobierno Peruano -a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)- ha venido impulsando todo un conjunto de normativas respecto de la obligatoriedad de su implementación, aún no se ha logrado el nivel de desarrollo definido en dichas normas. En la presente investigación cualitativa, se han realizado 07 entrevistas a profundidad con Oficiales de Seguridad de la Información, encargados de la implementación del SGSI en sus respectivas instituciones públicas.*

Palabras clave: Sistema de Gestión de Seguridad de la Información (SGSI). Oficial de Seguridad de Información, Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Entidades Públicas Peruanas.

Abstract: *In this research, It has been identified the causes that restrict the "Information Security Management System" -ISMS- in the Peruvian Public Entities. The main focus of this research stems from the lack of a mandatory implementation of defined norms that have been promoted by the Government through the National Office of Information and Electronics "Oficina Nacional de Gobierno Electronico e Informatica"-ONGEI, however, have not achieved a proper level of development in its standards. Therefore, in this research, seven in-depth interviews have taken place in public institutions with Chief Information Security Officers in charge of the ISMS.*

Keywords: Management System Information Security (ISMS). Information Security Officer, National Office of Electronic Government and Information Technology (ONGEI), Peruvian Public Entities.

1 Introducción

En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que ha aumentado los riesgos para las empresas que se exponen a nuevas amenazas. Por tanto, para proteger a las organizaciones de todas estas amenazas es necesario conocerlas y afrontarlas de una manera adecuada.

La seguridad de la información protege a las organizaciones de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar sus daños y maximizar el retorno de las inversiones y las oportunidades de negocio. Dicha seguridad se consigue implementando un conjunto adecuado de controles, los que necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

Un Sistema de Gestión de Seguridad de la Información -**SGSI**- es un conjunto de políticas y procedimientos cuyo objetivo es administrar la seguridad de la información de cualquier organización, proporcionando una metodología sistemática, documentada y fuertemente enfocada en los riesgos que pueda enfrentar una organización.

La norma estándar internacional ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información en una organización. Dicha norma, establece los procedimientos adecuados, así como la implementación de controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia.

El problema fundamental que da origen a este trabajo de investigación es que, al presente, a pesar de que el Gobierno Peruano ha venido impulsando todo un conjunto de normativas respecto de la obligatoriedad de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las Entidades Públicas Peruanas, aún no se ha logrado el nivel de desarrollo definido en dichas normas.

El Gobierno Peruano, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) órgano adscrito a la Presidencia del Consejo de Ministros, es el ente rector de la implementación de la Política Nacional de Gobierno Electrónico (D.S. N° 081-2013-PCM), el cual, desde su creación ha venido emitiendo normas —en forma orgánica y sistematizada— con el fin de desarrollar la seguridad de la información en el Sector Público, de acuerdo con estándares internacionales. Es precisamente este órgano el encargado de coordinar, con las entidades públicas integrantes del Sistema Nacional de Informática, la aplicación de la normatividad del SGSI vigente. (NTP-ISO/IEC 27001:2014).

El propósito de este estudio es realizar una investigación de tipo cualitativa que permita utilizar una estrategia de recopilación de información de una manera organizada y estructurada, a través de la realización de entrevistas, para identificar las restricciones y facilidades que encuentran las entidades públicas, donde se establecerá un conjunto de variables de estudio que permitan obtener información de apoyo a la mejora en la implementación de las políticas

de seguridad de información de las entidades integrantes del Sistema Nacional de Informática.

Los objetivos que se buscan en esta investigación son los siguientes:

1° Analizar las principales limitaciones y problemas *que vienen enfrentando actualmente* las entidades del sector público en la implementación del SGSI.
2° Investigar las estrategias y metodologías que vienen aplicando las entidades públicas *que ya han completado su ejecución* y los beneficios obtenidos de haberlo realizado en sus instituciones.

2 Teoría del dominio y trabajos previos

Esta investigación es llevada a cabo debido a la necesidad y obligatoriedad (R.M. N° 004-2016-PCM) que tienen las entidades públicas peruanas de implementar una estrategia efectiva de seguridad de la información, orientadas a dotar de una estructura organizacional de gestión de la información que permita el alineamiento de TI con la estrategia de negocios de las organizaciones, el logro de beneficios, la reducción de costes, el control de riesgos y, en general, la mejora de las operaciones de TI en el Estado Peruano.

En una investigación respecto de los *Factores inhibidores en la implementación de los Sistemas de Gestión de Seguridad de Información bajo la NTP-ISO/IEC 17799* [MARIÑO, 2010], se concluye que en el proceso de implementación de la norma no hay un mecanismo de control del organismo rector (ONGEI) para supervisar el desarrollo del mismo y sistematizar las lecciones aprendidas enmarcadas en un plan maestro de seguridad de la información de las entidades públicas, y que la seguridad de la información no está comprendida dentro del proceso de planificación estratégico que realizan las instituciones públicas.

En un reciente estudio, respecto de un *Modelo de Gestión de Seguridad de la Información para el E-Gobierno* [MERCADO, 2016], se señala que no se cuenta con un modelo de gestión de seguridad de la información que oriente la implementación y supervisión de la seguridad de la información en los servicios de gobiernos electrónicos brindado por las entidades del sector público, por lo cual pese a la obligatoriedad de la implementación de la norma de seguridad de la información y a la inversión realizada en tecnologías de información, continúa siendo mínima la implementación de seguridad de la información, observándose lo siguiente:

- No se ha definido un estructura organizacional con roles y responsabilidades que permita orientar la gestión de seguridad de la información.
- Se desconoce el nivel o la necesidad de seguridad con la que debe contar la información para el tratamiento que se realiza de acuerdo con las relaciones y fase del gobierno electrónico.
- Inexistencia de controles de seguridad o con vulnerabilidades para el almacenamiento, procesamiento y transferencia de la información requerida en los procesos de la organización.

Finalmente, podemos agregar que este estudio está encuadrado en dos Políticas Estratégicas de Estado, como son:

a) ***El Plan de Desarrollo de la Sociedad de la Información en el Perú - Agenda Digital 2.0*** (D.S. N° 066-2011-PCM), el cual tiene como objetivo general permitir que la sociedad peruana acceda a los beneficios que brinda el desarrollo de las Tecnologías de la Información en todos sus aspectos.

   Dicha estrategia tiene entre sus lineamientos el objetivo N° 7: "Promover una administración pública de calidad orientada a la población", teniendo como Estrategia N° 4: "Implementar mecanismos para mejorar la seguridad de la información, así como la necesidad de contar con una estrategia nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado".

b) ***La Política Nacional de Gobierno Electrónico*** (D.S. N° 081-2013-PCM), el cual tiene como fin, el uso de las Tecnologías de Información por parte del Estado para mejorar los servicios e información ofrecidos al ciudadano, así como aumentar la eficiencia y eficacia de la gestión pública.

   Dicha Política ha trazado 05 objetivos estratégicos, entre los cuales se encuentra el objetivo N° 3: "Garantizar la Confidencialidad, Integridad y Disponibilidad de la Información en la Administración Pública mediante mecanismos de Seguridad de la Información gestionada"

2.1. Análisis Normativo de la Seguridad de la Información en Perú

En Perú, ONGEI ha venido emitiendo, en el tiempo, normatividades para desarrollar la implementación de la Seguridad de la Información en el Estado Peruano, de acuerdo con estándares internacionales. (Figura 1)

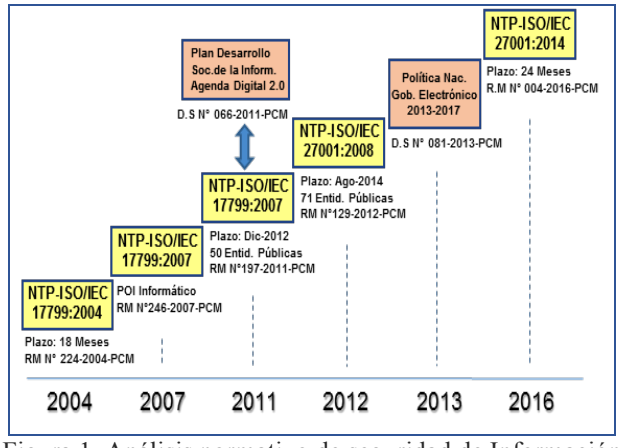

Figura 1. Análisis normativo de seguridad de Información en Perú. Fuente: ONGEI (2010) - Consejo Nacional de la Competitividad - CNC (2015). Elaboración propia

En el año 2011, se aprueba el Plan de Desarrollo de la Sociedad de la Información - Agenda Digital 2.0 mediante D.S. N° 066-2011-PCM. Más adelante, en el

año 2013, se aprueba la Política Nacional de Gobierno Electrónico en Perú, mediante D.S. N° 081-2013-PCM. Finalmente, a comienzos del año 2016, se publica la R.M. N° 004-2016-PCM donde se aprueba el uso obligatorio de la NTP-ISO/IEC 27001:2014 para todas las entidades integrantes del Sistema Nacional de Informática.

2.2. Indicadores de implementación de Seguridad de Información en Perú y el planeta

Según la VI Encuesta Nacional de Recursos Informáticos en la Administración (ENRIAP) realizada en el año 2007 (p.34), de 576 entidades públicas, 124 (21%) habían iniciado la implementación del SGSI, mientras que no implementaron 452 (79%). Mientras que en la VIII ENRIAP del año 2010 (p.75), de 552 entidades públicas, 182 (33%) habían iniciado la implementación del SGSI, mientras que las que no implementaron fueron 370 entidades públicas (67%) [ENRIAP, 2010]. Podemos apreciar, por tanto, que existe un incremento de aproximadamente del 10% entre el 2007 y el 2010, lo cual es un avance muy lento respecto de la implementación del SGSI en las instituciones públicas basado en la NTP 27001.

Por otro lado, de acuerdo con un estudio realizado por JackSecurity en el año 2008 (p.12) respecto de los niveles de maduración de la Seguridad de Información en Perú, se concluye que el Gobierno de Seguridad de la Información se encuentra en un nivel de maduración "informal" de Nivel 2 según el modelo de maduración ITGI de 0 a 5 (Nivel de maduración ITGI). Se puede afirmar también que muchas de las regulaciones pasadas y las aún vigentes no fuerzan directamente la relación de la "madurez" de los procesos de la seguridad de la información con una presencia supervisora de los agentes principales que componen el Gobierno, el comité de directorio y la alta gerencia de las organizaciones reguladas y normadas en Perú. [JACKSECURITY, 2008]

A nivel latinoamericano, según la IV Encuesta Latinoamericana de Seguridad de la Información [ACIS, 2012], dentro de los estándares más utilizados en los últimos años está la ISO 27001, que del 27% en el año 2010, pasó a un 56% en el 2012. (Tabla 1).

Tabla 1 - Estándares y Buenas Prácticas de TI

Tabla 19 ESTÁNDARES Y BUENAS PRÁCTICAS	2009	2010	2011	2012
ISO 27001	45.80%	27.37%	28.88%	55.83%
Common Criteria	5.20%	1.21%	3.65%	3.33%
Cobit 4.1	23.40%	14.88%	14.62%	31.11%
Magerit	5.20%	3.23%	2.74%	7.22%
Octave	2.30%	1.29%	2.19%	2.22%
Guías del NIST (National Institute of Standards and Technology) USA	12.30%	8.09%	7.49%	12.50%
Guías de la ENISA (European Network of Information Security Agency)	2.30%	9.70%	1.46%	1.94%
OSSTM - Open Standard Security Testing Model	7.50%	3.23%	4.38%	6.38%
ISM3 - Information Security Management Maturiy Model	3.90%	9.70%	1.46%	3.01%
ITIL	26.90%	17.47%	18.28%	40.27%
No se consideran	37.70%	10.19%	14.80%	21.38%
Otra;Top 20 de fallas de seguridad del SANS, ISO 17799. BS 259999, Cobit 5.0, NTC 5254, OWASP, ISSAF, PCI-DSS, MCIIEF, SOX, N4360, SARO, Comunicación A4609, Propias, Circular 052	7.10%	2.91%	-	6.94%

Fuente: IV Encuesta Latinoamericana de Seguridad de la Información [ACIS, 2012]

Esta encuesta se realizó a un total de 515 entrevistados, y entre los países participantes se encuentran: Argentina, Chile, Colombia, Costa Rica, México, Uruguay, Paraguay y Perú.

A nivel mundial, tenemos algunos modelos de implementación de la seguridad de la información a nivel gubernamental. Entre estos tenemos por ejemplo:

El Gobierno de Canadá, ha creado el Centro Canadiense de Respuestas a Incidentes Cibernéticos (CCIRC) que es el órgano responsable de supervisar las amenazas y coordinar la respuesta nacional a cualquier incidente de seguridad cibernética cuyo objetivo es la protección de la infraestructura crítica nacional contra incidentes cibernéticos. Además, es parte de FIRST (Organización Internacional de Respuestas a Incidentes de Seguridad). Por otro lado, se ha realizado una agrupación de especialistas de operaciones de TI en un solo grupo de trabajo nacional. Además, se ha creado el Área de Servicios Compartidos, que es un nuevo departamento creado en el 2011 con más de 6000 funcionarios que realizan los siguientes servicios: 1) Consolidación de 485 Data Centers en solamente 07. 2) Migración de todos los sistemas de correo electrónico a una sola plataforma. 3) Creación de una única infraestructura de red de telecomunicaciones compartida. [BOYLI, 2013].

El Gobierno de Uruguay, viene instrumentando políticas concretas para la administración pública en materia de Seguridad de la Información. Así, se ha creado por decreto gubernamental el Comité Nacional para la Sociedad de la Información (CNSI) que tiene la dirección ejecutiva de los planes para el desarrollo de la sociedad de la información [PEREYRO, 2011].

El Gobierno de Taiwán, viene impulsando fuertemente la política de seguridad nacional, cuya principal misión es promover y mejorar la implementación y certificación del SGSI [KU, 2009]. Además, el Gobierno también apoya la investigación académica, imparte cursos educativos y promueve la certificación profesional. Además, se ha unido a muchas organizaciones de seguridad global. Así, en el 2001, se unieron al Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST), que es el mayor foro internacional de Seguridad de la Información. En 2002, Taiwán se convirtió también en un miembro del equipo de Asia-Pacific Computer Emergency Response Team (APCERT).

Por otro lado, las principales entidades gubernamentales, incluyendo 37 departamentos públicos y 25 gobiernos locales, han establecido sus equipos de respuesta y designado a sus principales funcionarios de seguridad de la información para impulsar el plan de mecanismo. El rango de clasificación de seguridad se ha ampliado a casi 6800 sectores públicos después de incluir las unidades educativas. Finalmente, más de 170 sectores públicos han acreditado la autenticación SGSI. El Centro Nacional de Operaciones de Seguridad (NSOC) también mejoró sus habilidades y proporciona protección de seguridad para las instituciones críticas durante todo el día.

La tasa de penetración de los sectores públicos se ha reducido de 1,2% a 0,84% en el 2005 y seguía disminuyendo gradualmente. Por supuesto, el Gobierno

de Taiwán continuará mejorando la eficiencia de este plan y propagará sus esfuerzos de las unidades gubernamentales a las industrias y de las unidades básicas al sector público para asegurar la mejor utilización del SGSI.

Finalmente, se presenta la ***Encuesta Mundial de Certificaciones ISO 27001*** de los años 2013 y 2014, elaborada por la International Organization for Standardization (ISO), y donde se puede notar que la gestión de seguridad de la información (ISO/IEC 27001) respecto de la tendencia del año anterior, presenta un crecimiento constante contando con un 14% de aumento en la certificación a nivel mundial.

En la Figura 2, se ha hecho una comparación de la distribución mundial de la norma ISO/IEC 27001 certificados en el 2013 y 2014 donde se puede apreciar la marcada diferencia existente en países de Europa y Asia respecto de los países de Sudamérica. Los tres principales países con el mayor número de certificaciones en el mundo son Japón, Reino Unido e India; mientras que, en Sudamérica, los tres primeros países que han crecido en el número de certificaciones fueron Brasil, Colombia y Chile (que desplazó a Argentina en el año 2014)

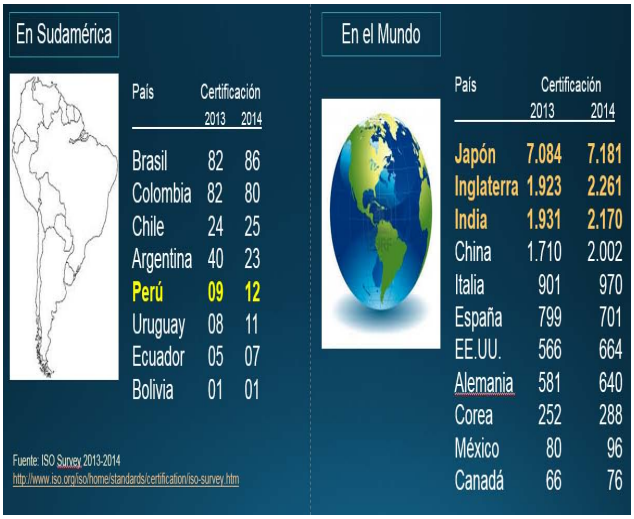

Figura 2. Certificación mundial ISO 27001 en los años 2013-2014. *Fuente*: ISO Survey. Elaboración propia.

3 Metodología de la investigación

El presente estudio de investigación es del tipo cualitativo, ya que tiene como fin la indagación descriptiva de los factores que afectan el problema en estudio. Además, esta investigación es inductiva, ya que pretende obtener conclusiones generales a partir de los resultados obtenidos en el levantamiento de información al marco muestral definido.

El procedimiento utilizado ha sido una estrategia basada en la ***Metodología de la Teoría Fundamentada*** [CUÑAT, 2005], el cual nos permite construir teorías a partir de un conjunto de datos recolectados y no de otras investigaciones, y que tienen como finalidad explicar la realidad basada en la recolección de datos e interpretación de la misma. Estos datos fueron recogidos a través de entrevistas, estableciéndose un conjunto de variables que han permitido el análisis de los datos y la obtención de resultados que responden al problema de investigación.

La *Población Objetivo* para esta investigación abarca a los Organismos Públicos Descentralizados que conforman el Sistema Nacional de Informática1 adscritos a la Presidencia del Consejo de Ministros (PCM) del Gobierno Central.

La *Unidad de Análisis* para la presente investigación está compuesta por las entidades responsables de la implementación del Sistema de Gestión de Seguridad de la Información que son de cumplimiento obligatorio según la NTP-ISO/IEC 27001:2014. [ONGEI, 2016]

Para el *Marco Muestral* de esta investigación se ha optado por elegir muestras homogéneas que comprende a los Directores/Gerentes del área de Informática o de los Oficiales de Seguridad de la Información de las instituciones representativas del Estado que, según la R.M. N° 004-2016-PCM, deben cumplir obligatoriamente con la implementación del SGSI de acuerdo a la NTP-ISO/IEC 27001 vigente. (Figura 3)

Para el tamaño de la muestra elegido en esta investigación, se ha tomado como referencia el tamaño mínimo de muestra sugerido en los "casos de estudio en profundidad", de acuerdo con la tabla referencial de los tamaños de muestra comunes en los estudios cualitativos citado por Hernández Sampieri, Fernández y Baptista [HERNANDEZ, 2010; p.395]. En la selección de las mismas, se tomó en cuenta una mixtura de situaciones entre entidades públicas donde aún su implementación es inicial y otras que ya han desarrollado y culminado dicha implementación.

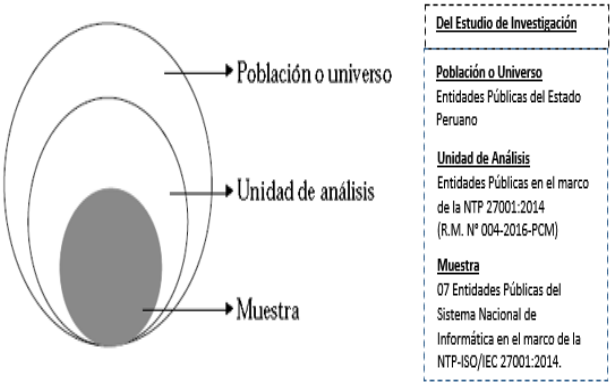

Figura 3. Diagrama de Población, Unidad de Análisis y Muestra. Fuente: Preparación de un proyecto de investigación -2003 (http://www.scielo.cl/pdf/cienf/v9n2/art03.pdf)

4 Análisis de datos y resultados

4.1. Análisis de datos de la investigación

Considerando que la investigación fue cualitativa, el análisis de datos se realizó paralelamente con la recolección de datos aplicando la *Metodología de la Teoría Fundamentada*, donde a través del método comparativo constante el investigador simultáneamente codifica y analiza datos para desarrollar conceptos.

Con este fin, se realizó un análisis inicial de la implementación de la Norma Técnica Peruana con el objetivo de identificar su nivel de importancia, las relaciones de dependencia entre ellos, el impacto

individual y en conjunto para el desarrollo del gobierno electrónico.

Para esta investigación, se concretaron siete (07) entrevistas semiestructuradas con las siguientes instituciones públicas:

1) Ministerio de Relaciones Exteriores - RR.EE.
2) Registro Nacional de Identificación y Estado Civil - RENIEC.
3) Instituto del Mar del Perú - IMARPE.
4) Oficina Nacional de Procesos Electorales - ONPE.
5) Ministerio Público - Fiscalía de la Nación - MPFN.
6) Ministerio de Economía y Finanzas - MEF y
7) Ministerio de Cultura - CULTURA.

Luego de las entrevistas realizadas, la recolección de datos, su transcripción, análisis y tratamiento de los mismos, se han categorizado las unidades de análisis identificadas, encontrándose los factores principales junto con un conjunto de variables o indicadores por cada uno de estos factores, así como en el número de incidencias presentadas en las entrevistas.

4.2. Resultados de la investigación

Los resultados obtenidos de esta investigación, luego de completadas las 03 fases de categorización de la metodología de la teoría fundamentada, ha sido la identificación de ocho (08) factores principales, los cuales fueron clasificados de la siguiente manera: Políticas de Estado, Desarrollo de la NTP, Presupuesto, Especialización, Apoyo Institucional, Gestión del SGSI, Normatividad del SGSI y Organización del SGSI.

Por cada factor propuesto, se han identificado una serie de indicadores, que para esta investigación, representan un conjunto de variables relacionadas que permiten describir y comprender dicho factor. Estos indicadores pueden afectar positiva o negativamente a cada uno de ellos.

Finalmente, y con el objetivo de establecer un parámetro de medición de los indicadores encontrados, se ha establecido un parámetro de valoración basado en las incidencias presentadas en cada uno de los indicadores durante las entrevistas. Este procedimiento se le denominó "matriz de evaluación de incidencias", que ha permitido asignar un grado de importancia a los indicadores, y que han derivado en las conclusiones finales del estudio de investigación.

4.3. Matriz de evaluación de incidencias de los factores encontrados

A continuación, se presenta la matriz de evaluación de incidencias de cada indicador encontrado en los factores propuestos. Estas variables han sido definidas durante el proceso de categorización realizada con la metodología definida en esta investigación. Esta evaluación permitió encontrar los principales problemas encontrados por cada factor propuesto. En algunos factores (3, 5 y 7) se especifica un único indicador debido a que éste abarca en su totalidad a dicho factor. Los factores encontrados fueron las siguientes:

A) Evaluación del Factor 1: Políticas de Gobierno

Tabla 2. Relación entre los indicadores del factor 1 y el número de incidencias presentadas en las entrevistas

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
1. Políticas de Gobierno	**1.1. Insuficiente desempeño de la ONGEI**	1	1	2	1	4	3	2	14
	1.2. Constantes cambios en las Políticas de Estado	1	1	2	-	-	-	-	4
	1.3. Metas de Estado para el SGSI más integrales	-	3	4	-	-	2	-	9
	1.4. Estructura organizacional y funcional del Oficial de Seguridad en las Entidades Públicas	1	1	2	1	2	-	2	9
	1.5. No existe suficiente apoyo del Gobierno en implementar el SGSI	-	-	-	1	2	2	-	5
	1.6. ONGEI funciona como ente normativo pero no implementador	-	-	-	3	-	1	1	4

En las Políticas de Gobierno, se ha determinado que las principales causas que se presentan en este factor son:

- Insuficiente desempeño de la ONGEI.
- Metas de Estado para el SGSI más integrales
- La estructura organizacional y funcional del Oficial de Seguridad

B) Evaluación del Factor 2: Desarrollo de la NTP

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
2. Desarrollo de la NTP	2.1. Los objetivos del SGSI están claramente definidos	1	-	2	1	1	1	2	8
	2.2. La evolución técnica es progresiva	1	-	-	-	-	3	4	8
	2.3. Falta de adecuación operativa a la norma estándar ISO	1	2	1	1	1	2	1	9

Tabla 3. Relación entre los indicadores del factor 2 y el número de incidencias presentadas en las entrevistas

En el Desarrollo de la NTP, se ha determinado que la principal causa que se presenta en este factor es:

- Falta de una adecuación operativa a la norma ISO

C) Evaluación del Factor 3: Presupuesto del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
3. Presupuesto	**3.1. Falta de un plan presupuestal para el SGSI**	1	3	2	1	6	5	2	20

Tabla 4. Relación entre los indicadores del factor 3 y el número de incidencias presentadas en las entrevistas

En el Presupuesto del SGSI, se ha determinado que la principal causa que se presenta en este factor es:

- Falta de un plan presupuestal integral para el SGSI

D) Evaluación del Factor 4: Especialización en SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
4. Especialización	4.1. Escasa capacitación del SGSI para el personal de las entidades públicas	1	-	-	1	-	3	2	7
	4.2. La experiencia profesional del SGSI aún está en desarrollo	1	3	1	1	-	-	2	8
	4.3. La capacitación profesional de especialistas en SGSI está avanzando	-	-	1	-	-	2	2	5
	4.4. Formación de equipos profesionales interinstitucionales en seguridad de información	-	-	-	1	-	-	-	1

Tabla 5. Relación entre los indicadores del factor 4 y el número de incidencias presentadas en las entrevistas

En la Especialización en SGSI, se ha determinado que la principal causa que se presenta en este factor es:

- La experiencia profesional en SGSI aún está en desarrollo.

E) Evaluación del Factor 5: Apoyo Institucional SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo	4	5	2	2	10	4	2	29

Tabla 6. Relación entre los indicadores del factor 5 y el número de incidencias presentadas en las entrevistas

En el Apoyo Institucional del SGSI, se ha determinado que la principal causa que se presenta en este factor es:

- El respaldo de la Alta Dirección es exiguo

(Generalmente por desconocimiento).

F) Evaluación del Factor 6: Gestión del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
5. Gestión del SGSI	5.1. Existe desconocimiento respecto de su operatividad	2	-	2	-	-	1	-	5
	5.2. Los conceptos y definiciones del SGSI están claros	-	2	-	-	2	2	-	6
	5.3. Estrategias operativas diversas en las entidades públicas	2	3	2	3	7	1	2	20
	5.4. El SGSI proporciona una mejor imagen institucional	1	-	-	-	-	-	1	1
	5.5. El mapa de procesos en las instituciones públicas está desactualizado	-	4	2	-	-	-	-	6
	5.6. La estructura orgánica en las entidades públicas es funcional y no por procesos	-	-	-	-	4	-	-	4
	5.7. Se asocia mucho la implementación del SGSI con el área de Tecnologías de Información (TI)	1	2	1	3	2	2	2	13
	5.8. No existe mucho conocimientos de la gestión por procesos	1	-	-	2	-	3	3	6
	5.9. Existen mayores riesgos en las entidades públicas debido al incremento del uso de las TIC	1	-	-	1	-	-	-	2
	5.10. Utilización del ISO 9001 como soporte de la gestión por procesos	3	-	-	3	-	2	-	8

Tabla 7. Relación entre los indicadores del factor 6 y el número de incidencias presentadas en las entrevistas

En la Gestión del SGSI, se ha determinado que las principales causas que se presentan en este factor son:

- Estrategias operativas diversas en las Entidades Públicas.
- Se asocia mucho la implementación del SGSI con el área de TI.
- Utilización del ISO 9001 como soporte de la gestión por procesos.

G) Evaluación del Factor 7: Normatividad del SGSI

Tabla 8. Relación entre los indicadores del factor 7 y el número de incidencias presentadas en las entrevistas

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
7. Normatividad del SGSI	7.1. No existe un entendimiento normativo claro del SGSI	-	1	1	-	-	3	2	7

En la Normatividad del SGSI, se ha determinado que la principal causa que se presenta en este factor es:

- No existe un entendimiento normativo claro del SGSI.

H) Evaluación del Factor 8: Organización del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
8. Organización del SGSI	**8.1. No se define un alcance estándar en las entidades públicas**	3	3	2	1	1	2	2	14
	8.2. Existen comités de seguridad de la información conformados en las entidades públicas	-	2	1	4	2	2	2	13
	8.3. No existe un nivel de avance del SGSI muy desarrollado en las entidades públicas	-	4	-	-	-	-	2	6
	8.4. La cultura organizacional del SGSI es poca o inexistente	1	1	1	1	4	3	4	15

Tabla 9. Relación entre los indicadores del factor 8 y el número de incidencias presentadas en las entrevistas

En la Organización del SGSI, se ha determinado que las principales causas que se presentan en este factor son:

- No se define un alcance estándar en las entidades.
- La cultura organizacional del SGSI es poca o nula.

5 Conclusiones

El presente estudio de investigación ha permitido identificar los factores que restringen o impiden el avance y ejecución del proceso de implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas, basada en la NTP-ISO/IEC 27001.

Teniendo en cuenta los fundamentos de la dirección estratégica de las organizaciones (estratégica, técnica y operativa), se ha establecido una categorización de estos factores en 03 niveles de gestión con una visión holística e integral del gobierno de seguridad de la información, los cuales son:

I) Nivel Estratégico

1 Una Política Estratégica de Estado en Seguridad de la Información

II) Nivel Operativo (compuesta de 04 pilares operativos)

2 Una gestión eficiente de la seguridad de información,

3 Apoyo institucional de la Alta Dirección

4 Una adecuada organización del SGSI

5 Aplicación efectiva de la normatividad en seguridad de información

III) Nivel Técnico (compuesta de 03 estratos técnicos)

6 Desarrollo integral institucional de la NTP

7 Contar con un presupuesto nacional para la seguridad de la información

8 La especialización técnica de profesionales en SGSI como prioridad nacional

El desarrollo de estas conclusiones son las siguientes:

5.1 A Nivel Estratégico

- Es necesaria la formalización del cargo de Oficial de Seguridad de Información en la estructura funcional de las entidades públicas, a través de los instrumentos de gestión institucional, como son el Reglamento de Organización y Funciones (ROF) y el Manual de Organización y Funciones (MOF), documentos que establecen las funciones a nivel de áreas y cargos.

- El desempeño de la ONGEI, si bien es aceptable en términos normativos, aún es insuficiente como ente implementador.
- Esto conlleva a la necesidad de fortalecer la organización actual de la ONGEI, ente encargado del monitoreo y avance de la NTP 27001 vigente en las entidades públicas.

5.2 A Nivel Operativo (Ámbito Institucional)

- Las estrategias operativas de implementación del SGSI en las entidades públicas son diversas. Algunas están más desarrolladas que otras y no hay una estrategia de transmisión del conocimiento.
- Normalmente, el SGSI se encarga al área de informática. Esto hace que muchas veces se limite únicamente a la tecnología.
- No existe un desarrollo de gestión por procesos en las entidades públicas, las cuales son organizaciones funcionales. Sin embargo, la NTP 27001 recomienda la implementación por procesos.
- No se define un alcance estándar en las entidades públicas. Estas podrían organizarse por tamaño o complejidad.
- Normalmente, en los Comités de Seguridad de Información se suele poner al Oficial de Seguridad a liderar el mismo.
- La cultura en seguridad de información en el personal de las entidades públicas es casi nulo. Se necesita definir que la NTP va más allá de lo tecnológico.

5.3 A Nivel Técnico (Ámbito Interinstitucional)

- Es necesario contar con recursos propios para implementar el SGSI. Actualmente, las actividades del SGSI se cubren con presupuesto de otras áreas (generalmente TI). No hay una asociación importancia vs coste.
- Las entidades públicas no tiene experiencia en el desarrollo de las fases de la NTP.
- Las entidades públicas que ya certificaron han desarrollado una gestión por procesos de su organización basado en la ISO 9001.38600.
- La profesionalización en SGSI aún es escasa. Es necesario darle un mayor recurso técnico para una eficiente ejecución operativa.

5.4 Diagrama de implementación del SGSI en el Estado Peruano

En base a todo lo referido anteriormente, se ha elaborado un diagrama que permite visualizar gráficamente las conclusiones obtenidas. (Figura 4)

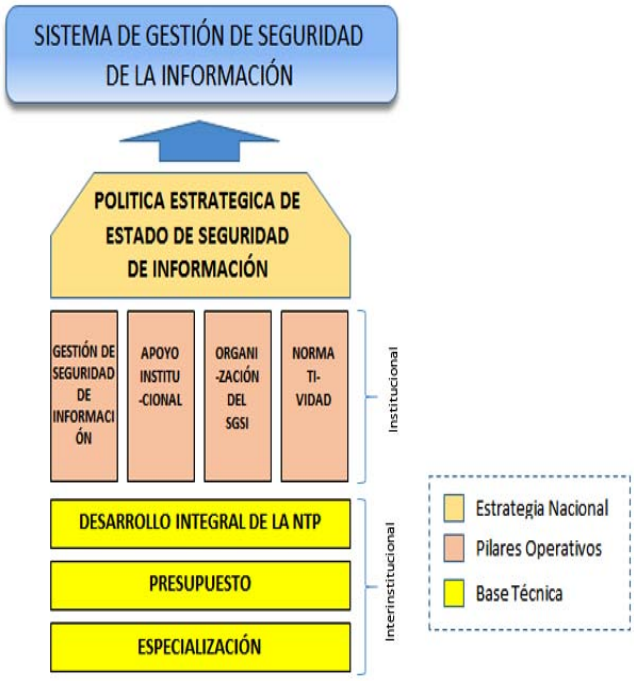

Figura 4. Diagrama de implementación del SGSI en las entidades públicas. Elaboración propia.

6. Recomendaciones

De acuerdo con las conclusiones referidas, se establecen un conjunto de recomendaciones para las instituciones públicas, que están enmarcadas en la NTP-ISO/IEC 27001, y que permitirán cumplir exitosamente con todas las fases de implementación del SGSI. Estas recomendaciones son las siguientes:

1° Creación de un Departamento de Gobierno de Seguridad de la Información

Se requerirá el establecimiento de una norma para la creación de un Departamento de Gobierno de SGSI. Esta oficina deberá estar adscrita a la PCM, y deberá contar con capacidad funcional especializada para operar a nivel de todo el Estado.

Deberá tener como objetivos principales:

a. Establecer políticas estandarizadas de Seguridad de la Información.
b. Diseñar y armonizar normativas institucionales en materia de Seguridad de la Información.
c. Facilitar la incorporación de todos los entes gubernamentales a la Seguridad de la Información.
d. Brindar instrumentos (concientización) a las autoridades de las instituciones gubernamentales para la implementación del SGSI.

2° Incorporar la Gestión por Procesos

Debería existir un área de procesos en las entidades públicas que coordine con el Oficial de Seguridad a determinar el más óptimo proceso de la organización para iniciar el SGSI.

3° Presupuesto centralizado

Es necesario asignar un presupuesto central para una gestión adecuada de los recursos de seguridad de la información en la implementación del SGSI en las entidades del Estado Peruano, según lo dispuesto en la NTP-ISO/IEC 27001.

4° Contar con un staff de especialistas

Es necesario contar con un equipo de especialistas en seguridad de la información nacionales y extranjeros que monitoreen y auditen el proceso de implementación del SGSI en las entidades públicas y además formen profesionales.

5° Potenciar la especialización

Apoyarse en las certificaciones como mecanismo para asegurar el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información.

7. Trabajos Futuros

Se plantean los siguientes estudios futuros que complementarían la presente investigación, como son:

- Investigación respecto de la *implementación integral de la NTP de Seguridad de la Información en el Estado Peruano, aplicando la metodología de Gobierno de Seguridad de la Información* (ISO 27014), que permita identificar las características principales de los factores estratégicos, técnicos y operativos que influyen en la gestión integral del SGSI.
- Investigación sobre un *modelo de implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas integrando la Gestión por Procesos* bajo la norma ISO 9001, que permita comprender la estructura operativa y los principales actores de las organizaciones relacionadas con la seguridad de la información.

Referencias bibliográficas

[ACIS, 2012] Asociación Colombiana de Ingenieros de Sistemas-ACIS. (2012). IV Encuesta Latinoamericana de Seguridad de la Información 2012. Recuperado el 15 de enero de 2014 desde

http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no-123/item/101-iv-encuesta-latinoamericana-de-seguridad-de-la-información

[BOYLI, 2013] Boyli, B. La Seguridad de la Información en el Gobierno de Canadá. En Colegio de Ingenieros del Perú. 54. Lima, Perú. Recuperado el 09 de diciembre de 2013 desde

http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada.html

[CNC, 2015] Consejo Nacional de la Competitividad. Análisis de la normatividad en TIC y recomendaciones de mejora. Iriarte y Asociados S.CIVL de R.L. desde

http://www.cnc.gob.pe/images/upload/paginaweb/archivo/25/An%C3%A1lisis%20de%20la%20Normatividad%20TIC.pdf

[CUÑAT, 2005] Cuñat, R.J. Aplicación de la teoría fundamentada al estudio del proceso de creación de empresas. *Decisiones Globales*, *pp. 1-13*. Recuperado desde
https://dialnet.unirioja.es/descarga/articulo/2499458.pdf

Da Veiga, A. Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. *Computer&Security, 29(2), p196-207.* Recuperado el 05 de febrero de 2014 desde

http://www.sciencedirect.com/science/article/pii/S0167404809000923

[ENRIAP, 2010] ONGEI. Análisis de Encuesta Nacional de Recursos Informáticos y Tecnológicos de la Administración Pública 2010 - VIII ENRIAP.

[HERNANDEZ, 2010] Hernández Sampieri, R., Fernández, C. & Baptista, P. Metodología de la Investigación. Quinta edición, Ed. Mc. Graw Hill.

[JACKSECURITY, 2008] JackSecurity. Gobierno de Seguridad de la Información. Nivel de Maduración - Perú 2008. Recuperado el 11 de enero de 2014 desde

http://www.jacksecurity.com/download.php?idP=82&ida=83

KPMG. (2012). Informe de fraude en el Perú 2012. Recuperado el 02 de febrero de 2014 desde

http://www.kpmg.com/PE/es/IssuesAndInsights/ArticlesPublications/Documents/Informe-del-Fraude-en-Peru-2012.pdf

[KU, 2009] Ku, Ch. Chang, Y. Yen, D. National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy, 33(7), p371-384.* Recuperado el 13 de diciembre de 2013 desde

http://www.sciencedirect.com/science/article/pii/S0308596109000263

[MARIÑO, 2010] Mariño, A. *Factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basados en la NTP-ISO/IEC 17799 en la administración pública.* Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas. (2010). Lima, Perú. Recuperado el 30 de noviembre de 2013 desde

http://cybertesis.unmsm.edu.pe/handle/cybertesis/1058

Matas Terrón, A. (2010). Computadoras e investigación cualitativa. AIDESOC. Recuperado desde

http://riuma.uma.es/xmlui/bitstream/handle/10630/4712/computadoras_inves_cualitativa.pdf?sequence=1

[MERCADO, 2016] Mercado, J. *Modelo de Gestión de Seguridad de la Información para el Gobierno Electrónico.* Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas. (2016). Lima, Perú.

[ONGEI, 2016] Resolución Ministerial N° 004-2016-PCM. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición.

ONGEI. (2013). La Seguridad de la Información en el Gobierno Peruano. En Colegio de Ingenieros del Perú. Lima, Perú. Recuperado el 09 de diciembre de 2013 desde http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada.html

ONGEI. (2013). Resolución Ministerial N° 310-2013-PCM. Autorización para la ejecución de la "Encuesta Nacional de Recursos Informáticos en la Administración Pública - ENRIAP".

ONGEI. (2012). Resolución Ministerial N° 129-2012-PCM. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

ONGEI. (2010). Resolución Ministerial N° 187-2010-PCM. Autorización para la ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010".

[PEREYRO, 2011] Pereyro, M. Seguridad de la información en el Uruguay: políticas de Estado en la Administración Pública. *Revista de la Asociación de Escribanos del Uruguay, Tomo 97.* Recuperado el 03 de enero de 2014 desde

http://documentos.aeu.org.uy/090/097-1-137-156.pdf