UNIVERSIDAD NACIONAL DEL CALLAO

ESCUELA DE POSGRADO

UNIDAD DE POSTGRADO DE LA FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

"RELACIÓN DE LA NTP ISO/IEC 27001:2008 EDI Y LA SEGURIDAD DE LA INFORMACIÓN EN LOS MINISTERIOS DEL ESTADO PERUANO AL 2015"

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS

AUTORES:

Bach. FERNANDO ROLYN FLORES SOLÍS

Bach. JESÚS ANTONIO GUERRA FARFÁN

Callao – 2017

PERÚ

UNIVERSIDAD NACIONAL DEL CALLAO

ESCUELA DE POSGRADO

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

MAESTRÍA EN INGENIERÍA DE SISTEMAS

RESOLUCIÓN N° 029-2017-UPG-FIIS

JURADO EXAMINADOR

DR. ALEJANDRO DANILO AMAYA CHAPA	PRESIDENTE
MG. ERIKA JUANA ZEVALLOS VERA	SECRETARIA
MG. GERMÁN ELÍAS POMACHAHUA PEREZ	VOCAL

ASESORA: MG. SALLY KARINA TORRES ALVARADO

N° DE LIBRO DE ACTA DE SUSTENTACIÓN: 001-2012-SPG-FIIS

N° DE ACTA DE SUSTENTACIÓN: 005-2017-UPG-FIIS

N° DE ACTA DE SUSTENTACIÓN: 006-2017-UPG-FIIS

FECHA DE APROBACIÓN DE LA TESIS: 24 DE MARZO DEL 2017

ÍNDICE

ÍNDICE 1
INTRODUCCION 7
RESUMEN 8
ABSTRACT 10
CAPÍTULO I PLANTEAMIENTO DE LA INVESTIGACIÓN 12
1.1. Descripción de la Realidad Problemática 12
1.2. Formulación del Problema 16
1.2.1. Problema General 16
1.2.2. Problemas Específicos 16
1.3. Objetivo de la Investigación 17
1.3.1. Objetivo General 17
1.3.2. Objetivos Específicos 17
1.4. Justificación e Importancia de la Investigación 17
1.5. Limitaciones del Estudio 18
1.6. Viabilidad del estudio 18
CAPÍTULO II MARCO TEORICO CONCEPTUAL 20
2.1. Antecedentes de la Investigación 20
2.2. Bases Teóricas 21
2.2.1. ISO/IEC 27001:2005 Sistema de Gestión de Seguridad de la Información 21
2.2.2. Evolución de la Norma 21
2.2.3. Familia de la ISO 27001 22
2.2.4. Naturaleza de un SGSI 23
2.2.5. NTP/IEC 27001:2008 Sistema de Gestión de Seguridad de la Información 24
2.2.6. NTP/IEC 27001:2014 Sistema de Gestión de Seguridad de la Información 25
2.2.7. Marco regulatorio Legal 25
2.3. Definiciones Conceptuales 36
2.3.1. Análisis de Log de Seguridad 36

2.3.2. Auditabilidad 36
2.3.3. Auditoría Informática 36
2.3.4. Autenticación 38
2.3.5. Autenticidad 38
2.3.6. Confiabilidad 39
2.3.7. Confianza 39
2.3.8. Confidencialidad 39
2.3.9. Control 40
2.3.10. Credencial 40
2.3.11. Disponibilidad 40
2.3.12. Estándar 41
2.3.13. Evaluación De Riesgos 41
2.3.14. Gestión De Riesgos 42
2.3.15. Información 43
2.3.16. Incidente de Seguridad 43
2.3.17. Integridad 44
2.3.18. No Repudio 44
2.3.19. Observación 45
2.3.20. Riesgo 45
CAPÍTULO III HIPÓTESIS Y VARIABLES 46
3.1. Hipótesis General 46
3.2. Hipótesis Específicas 46
3.3. Identificación de Variables 46
3.4. Operacionalización de Variables 47
CAPÍTULO IV METODOLOGÍA 48
4.1. Tipo de Investigación 48
4.2. Diseño de la Investigación 48
4.3. Población – Muestra 48
4.4. Técnicas e instrumentos de recolección de datos 49
4.5. Plan de Análisis estadísticos de datos 49
CAPÍTULO V RESULTADOS 52

5.1. Norma Técnica Peruana ISO/IEC 27001:2008 52
5.2. Seguridad de la Información 65
5.3. Determinación de Datos Adicionales 68
5.4. Análisis de Confiablidad 70
CAPÍTULO VI DISCUSION DE RESULTADOS 72
6.1. Contrastación de Hipótesis con los resultados 73
CAPÍTULO VII CONCLUSIONES 82
CAPÍTULO VIII RECOMENDACIONES 83
CAPÍTULO IX REFERENCIAS BIBLIOGRÁFICAS 84
ANEXOS 86

INDICE DE TABLAS

Tabla N° 2.1 Evolución de la norma 22
Tabla N° 2.2 Clasificación de la norma 23
Tabla N° 3.1 Operacionalización de variables 47
Tabla N° 4.1 Técnicas e instrumentos de estudio por indicador 49
Tabla N° 4.2 Valorización de variables 50
Tabla N° 5.1 Grado de implantación por ministerio 68
Tabla N° 5.2 Nivel de incidentes 69
Tabla N° 5.3 Resumen del procesamiento relación de la ntp iso/iec 27001:2008 edi y la seguridad de la información 70
Tabla N° 5.4 Estadísticos de fiabilidad 70
Tabla N° 5.5 Estadísticos de total de elemento 71
Tabla N° 6.1 Interpretación de los valores de los coeficientes de correlación 72
Tabla N° 6.2 Coeficiente de correlación de spearman entre el grado de implantación y el número de incidentes que afectaron la confidencialidad de la información 73
Tabla N° 6.3 Coeficiente de correlación de spearman entre el grado de implantación y el número de incidentes que afectaron la integridad de la información 75
Tabla N° 6.4 Coeficiente de correlación de spearman entre el grado de implantación y el número de incidentes que afectaron la disponibilidad de la información 77
Tabla N° 6.5 Coeficiente de correlación de spearman entre el grado de implantación y el número de incidentes que afectaron la seguridad de la información 79

INDICE DE GRAFICOS

Gráfico N° 5.1 Documento del alcance del SGSI 52
Gráfico N° 5.2 Documento de política de SGSI 53
Gráfico N° 5.3 Documento de criterios de evaluación y aceptación de riesgos 54
Gráfico N° 5.4 DOcumento de evaluación de riesgo 55
Gráfico N° 5.5 Documento de plan de tratamiento de riesgo 56
Gráfico N° 5.6 Documento de declaración de aplicabilidad 57
Gráfico N° 5.7 Documento de plan de trabajo 58
Gráfico N° 5.8 Controles de seguridad 59
Gráfico N° 5.9 Registros que evidencien el monitoreo de desempeño del SGSI 60
Gráfico N° 5.10 Registros de la mejora de la gestión de incidentes 61
Gráfico N° 5.11 Auditorias al SGSI 62
Gráfico N° 5.12 Acciones correctivas 63
Gráfico N° 5.13 Acciones preventivas 64
Gráfico N° 5.14 Número de incidentes que afectaron la confidencialidad de la información 65
Gráfico N° 5.15 Número de incidentes que afectaron la integridad de la información 66
Gráfico N° 5.16 Número de incidentes que afectaron la disponibilidad de la información 67
Gráfico N° 6.1 Dispersión entre el grado de implantación y el número de incidentes que afectaron la confidencialidad de la información 74
Gráfico N° 6.2 Dispersión entre el grado de implantación y el número de incidentes que afectaron la integridad de la información 76
Gráfico N° 6.3 Dispersión entre el grado de implantación y el número de incidentes que afectaron la disponibilidad de la información 78
Gráfico N° 6.4 Dispersión entre implantación y la seguridad de la información 80

INDICE DE ILUSTRACIONES

Figura N° 1.1 Implementación incremental de la NTP-ISO/IEC 27001:2008 15
Figura N° 2.1 Modelo PDCA aplicado al proceso SGSI 24

INTRODUCCION

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) tiene una agenda digital que prioriza el fortalecimiento de la sociedad de la Información a través de un plan de desarrollo de la sociedad de la información, también denominada Agenda Perú. Dicho plan incluye entre sus estrategias implementar mecanismos para la mejora de la seguridad de la información. Con tal fin en mayo de 2012 la ONGEI publica con carácter de obligatoria a través de la Resolución Ministerial N° 129-2012-PCM, la implantación incremental de la "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos"

Habiendo transcurrido más de tres años de publicada la resolución y habiéndose cumplido el plazo para la implantación, el presente estudio tiene como objetivo determinar si existe relación entre la implantación y la seguridad de la información en el Estado Peruano, además de determinar en qué grado de implantación en promedio se encuentran los ministerios del Perú.

Para lograr los objetivos se realizaron encuestas a cada uno de los 18 ministerios y la Presidencia de Consejo de Ministros realizándose la prueba estadística de correlación que permitiera probar la hipótesis declarada.

RESUMEN

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) publicó el 23 de mayo de 2012 la Resolución Ministerial N° 129-2012-PCM que aprueba el uso obligatorio en todas las instituciones del Estado de la NTP-ISO/IEC 27001:2008 EDI para implementar un sistema de gestión de seguridad de la información que permita garantizar la seguridad de la información.

Para comprobar si la implantación de la norma ha permitido mejorar la seguridad de la información en los Ministerios del Estado Peruano, se realizó un estudio de investigación cuantitativo correlacional de tipo no experimental y transversal, para lo cual, se tuvo que determinar el grado de implantación de la norma y el nivel de incidentes de seguridad de la información en la población seleccionada, que para efecto de este estudio fueron los 18 ministerios y la Presidencia del Consejo de Ministros.

Del análisis se obtuvo -0.636 como coeficiente de correlación, lo cual indica que existe una correlación negativa considerable y una magnitud de la significancia de 0.003 siendo esta menor a 0.05, que indica el rechazo de la hipótesis nula, aceptándose la hipótesis principal, existe relación entre la implantación de la NTP-ISO/IEC 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado peruano al 2015. Asimismo, se ha determinado que el grado de implantación de la norma en los ministerios es de 2.80 encontrándose en el nivel de planificación respecto a los 5 niveles de implantación incremental (Organización, Planificación, Despliegue, Revisión y Consolidación) propuesto por la ONGEI.

Finalmente, se confirma que la implantación de la NTP-ISO/IEC 27001:2008 EDI permite mejorar la seguridad de la información de las

ministerios del Estado, por lo que, se recomienda que los ministerios concluyan con el proceso de implantación de la norma.

Palabras Claves: NTP ISO/IEC 27001:2008, sistema de Gestión de seguridad de la información, seguridad de la información

ABSTRACT

The National electronic and informatics government's office (ONGEI) had issued in May 13th 2012 the ministerial resolution N° 129-2012-PCM that it applies the obligatory use in all the state's institutions of the NTP-ISO/IEC 27001:2008 EDI to implement an information security management system that it can ensure the information security.

For checking if the implementation of the standard have allowed to improve the information security on the Peruvian government ministries, a correlational-quantitative research study was done, it is of type no experimental and transversal, that is the reason It had to determine the implantation grade of the standard and the level of information security incidents in the population selected, it is about 18 ministries and the Council presidency of ministers.

The results of the analysis is -0.636 as a correlation coefficient, it shows that there is a significant negative correlation and a magnitude of the significance of 0.003 which is lower to 0.05, it shows a rejection of the null hypothesis, thus approving the main hypothesis, there is a relation between the implantation of the NTP-ISO/IEC 27001:2008 EDI and the information security on the Peruvian government ministries in 2015. Likewise, it has been determined that the degree of implementation of the standard in the ministries is 2.80 being in the planning level regarding the 5 levels of incremental implantation (Organization, Planning, Deployment, Review and Consolidation) proposed by the ONGEI.

Finally, it is confirmed that the implantation of the ISO / IEC 27001: 2008 EDI allows to improve information security of state ministries, so it is recommended that the ministries completed the process of implantation of the standard.

Keywords: NTP ISO/IEC 27001:2008, information security management system, information security.

CAPÍTULO I
PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. Descripción de la Realidad Problemática

(CODESI, 2011) 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 eso, 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 "La Agenda Digital Peruana".

(CODESI, 2011) La Agenda Digital Peruana establece en el objetivo N° 7 "Promover una administración Pública de Calidad Orientada a la Población" donde la estrategia N° 4 de la misma 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.

Por otro lado, como modelos se puede analizar la estrategia de ciberseguridad española (Departamento de Seguridad Nacional, 2013) que define como elementos esenciales de su política la de 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 la de garantizar la implantación del Esquema Nacional de Seguridad.
(Presidencia del Estado Español, 2010)

> *"El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será 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."*

Otro modelo que se puede tomar en cuenta 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 : (Mexico, 2014):

> *"Ante la necesidad de homologar los procesos contenidos en dicho manual a 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, por lo que hemos tenido a bien expedir el siguiente acuerdo que tiene por objeto emitir las políticas y disposiciones para la estrategia digital nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el manual*

administrativo de aplicación general en dichas materias"

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 17799:2004 publicada con resolución ministerial N° 244-2004-PCM. En el año 2007 se realiza la actualización de la norma con resolución ministerial N° 246-2007-PCM donde aprueba el uso obligatorio de la NTP ISO/IEC 17799:2007 EDI Tecnologías de la Información. Código de buenas prácticas para la gestión de la seguridad de la información 2ª edición en todas las entidades integrantes del Sistema Nacional de Informática.

Para el 13 de mayo de 2012, se publica la resolución ministerial N° 129-2012-PCM donde se aprueba el uso obligatorio Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática. 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 (ver cuadro 1) y establece una lista de instituciones prioritarias que deberán iniciar el proceso.

Figura N° 1.1
IMPLEMENTACIÓN INCREMENTAL DE LA NTP-ISO/IEC 27001:2008

PERÚ | Presidencia del Consejo de Ministros | Oficina Nacional de Gobierno Electrónico e Informática - ONGEI

Implementación incremental de NTP-ISO/IEC 27001:2008

Resolución Ministerial N° 129-2012-PCM

FASE	Nombre	Objetivo	Actividades Principales	Plazo máximo por fase
I	ORGANIZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implantación del SGSI.	* Obtener el apoyo institucional * Determinar el alcance del Sistema de Gestión de Seguridad de la Información * Determinar la declaración de Política de Seguridad de la Información y objetivos * Desarrollar documentos necesarios para la Fase II * Determinar criterios para la evaluación y aceptación de riesgos	Hasta 3 meses
II	PLANIFICACIÓN	Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	* Realizar evaluación de Riesgos * Conducir un análisis entre los riesgos identificados y las medidas correctivas existentes * Desarrollar un plan de tratamiento de riesgos * Desarrollar documentos necesarios para la Fase III * Desarrolla la declaración de Aplicabilidad	Hasta 4 meses
III	DESPLIEGUE	Desplegar las actividades de implementación del SGSI	* Elaborar el plan de trabajo priorizado * Desarrollar documentos y registros necesarios * Implementar los controles seleccionados	Hasta 12 meses
IV	REVISIÓN	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la norma	* Monitorear el desempeño del SGSI * Fortalecer la gestión de incidentes * Desarrollar documentos y registros necesarios * Desarrollar las actividades para evidenciar la mejora continua	Hasta 4 meses
V	CONSOLIDACIÓN	Auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.	* Auditar internamente el SGSI * Implementar las acciones correctivas * Implementar las acciones preventivas pertinentes * Desarrollar, corregir y mejorar documentación nueva o existente	Hasta 4 meses

FASE OPCIONAL:

VI	CERTIFICACIÓN		* Iniciar el proceso de certificación internacional en ISO/IEC 27001:2005 y obtener la certificación	No Aplica

Fuente: Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)

A agosto de 2015 la ONGEI no ha emitido ningún reporte o documento oficial que permita saber el porcentaje de instituciones del Estado que han implantado la "NTP-ISO/IEC 27001:2008.

1.2. Formulación del Problema

1.2.1. Problema General

¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la Seguridad de la Información en los Ministerios del Estado Peruano al 2015?

1.2.2. Problemas Específicos

- ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano al 2015?

- ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano al 2015?

- ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano al 2015?

1.3. Objetivo de la Investigación

1.3.1. Objetivo General

Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la Seguridad de la Información en los Ministerios del Estado Peruano al 2015.

1.3.2. Objetivos Específicos

- Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano al 2015.

- Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano al 2015.

- Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano al 2015.

1.4. Justificación e Importancia de la Investigación

El presente trabajo de investigación tiene importancia y se justifica por lo siguiente:

- Es conveniente, porque servirá para conocer el grado de implantación de la NTP 27001:2018 EDI que permita determinar si la estrategia propuesta por la ONGEI ha causado algún impacto positivo en la seguridad de la información de las instituciones del Estado.

- Tiene relevancia social, porque sus resultados beneficiarán al aseguramiento de la información que los ciudadanos intercambian en la sociedad de la información; así como, la protección de los bancos de datos personales que se encuentran en custodia de las instituciones del estado, en la medida que la ONGEI mejore la estrategia de implantación de la norma.

- El artículo 1 de la Resolución Ministerial N° 129-2012-PCM, establece el uso oblig atorio 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. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

1.5. Limitaciones del Estudio

Podríamos señalar como limitante la falta de veracidad en el desarrollo de las encuestas y cuestionarios, ya que es los oficiales de seguridad que serán encuestados, ante el incumplimiento de la implantación puedan brindar información no real.

Además, es importante tener en cuenta que por cuestiones propias a la seguridad es posible que las instituciones no respondan a las encuestas.

1.6. Viabilidad del estudio

El estudio es viable, debido a que se cuenta con información amplia en las normas técnicas y la metodología de la

implantación de sistemas de gestión de seguridad de la información, así como también se cuenta con acceso al Pe-Cert, que es el Centro de Coordinación de Seguridad Telemática del Perú y oficiales de seguridad de los ministerios del Estado Peruano quienes serán entrevistados y resolverán las encuestas y cuestionarios acerca del estudio.

CAPÍTULO II
MARCO TEORICO CONCEPTUAL

2.1. Antecedentes de la Investigación

(Calizaya de la Sota, 2012), en sus tesis, 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.

(Chávez Bravo, 2013), en su tesis, Aplicación del Modelo de Seguridad en Capas Basado en el Esquema de Defensa en Profundidad en Computación para Instituciones del Estado, 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.

(Aguirre Mollehuaca, 2014), en su tesis, muestra los procesos realizado 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 emitida en mayo del 2012.

(Huamán Monzón, 2014), en su tesis, 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.

2.2. Bases Teóricas

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

(ISO & IEC, 2005) 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 han sido elaborados para ser aplicados en todas las organizaciones, independientes del tipo, tamaño y naturaleza.

2.2.2. Evolución de la Norma

(Alexander, 2007), 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.

Tabla N° 2.1

EVOLUCIÓN DE LA NORMA

NORMA	BASE
BS 7799-1:1995 (Norma Británica)	Antecesora del código para la práctica de la gestión de la seguridad de la información.
BS 7799-2:1999	Norma creada para que las empresas se certificaran y es auditable.
ISO/IEC 17799:2000	La ISO adopta y oficializa en base de la norma británica BS 7799-1:1999
BS 7799-2:2002	Revisión de la BS 7799-2:1999
ISO 17799:2005	Revisión de la ISO 17799:2000
ISO 27001:2005	Revisión al BS 7799-2:2002
ISO 27001:2013	Revisión de la ISO/IEC 27001:2005

Fuente: Elaboración propia

2.2.3. Familia de la ISO 27001

(Lopez Neira & Javier, 2015) En la página web ISO2700.es donde se encuentra material para la implantación de la ISO 27000, encontramos la descripción de cada uno de las normas integrantes de la familia ISO 27000.

Tabla N° 2.2

CLASIFICACIÓN DE LA NORMA

NORMA	DESCRIPCIO
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

Fuente: ISO2700.es

2.2.4. Naturaleza de un SGSI

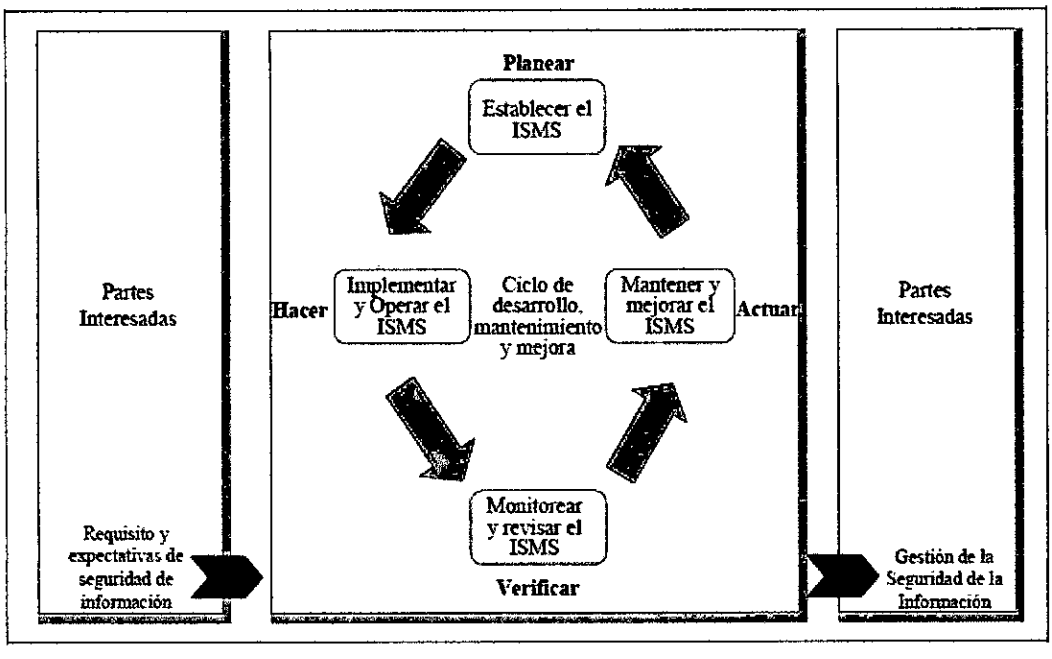
(Alexander, 2007), nos exhorta a entender la ISO/IEC 27001 como un modelo para el establecimiento, implantación, operación, monitoreo, revisión, mantenimiento y mejora de

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).

Figura N° 2.1

MODELO PDCA APLICADO AL PROCESO SGSI



Fuente: NTP ISO/IEC 27001:2008

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

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

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

(INDECOPI, Norma Técnica Peruana NTP-ISO/IEC 27001:2014, 2014) 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, y ya no solamente mediante el enfoque de procesos. Además, la nueva estructura contiene 10 elementos sincronizados con las demás ISO's de gestión.

2.2.7. Marco regulatorio Legal

- Oficina Nacional de Gobierno Electrónico e Informática - ONGEI

  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, para este caso se han aprobado la 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. 1ª Edición", 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. Este plazo venció el mes de Diciembre del 2005.

- 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. 2da edición" 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

  Esta 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. Sistemas de gestión de seguridad de la Información. Requisitos" 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. 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. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición", dispuesto por la Resolución Ministerial N° 246-2007-PCM.
  Las entidades que a continuación se detallan deben cumplir con implementar dichos sistemas:

  PODER LEGISLATIVO

  1. Congreso de la República

PODER JUDICIAL

2. Poder Judicial (PJ)

ORGANISMOS AUTÓNOMOS

1. Asamblea Nacional de Rectores (ANR)
2. Banco Central de Reserva del Perú (BCRP)
3. Consejo Nacional de la Magistratura (CNM)
4. Defensoría del Pueblo (DP)
5. Jurado Nacional de Elecciones (JNE)
6. Contraloría General de la República (CGR)
7. Ministerio Público-Fiscalía de la Nación (MPFN)
8. Oficina Nacional de Procesos Electorales (ONPE)
9. Registro Nacional de Identificación y Estado Civil (RENIEC)
10. Superintendencia de Banca, Seguros y AFP (SBS)
11. Tribunal Constitucional (TC).

PODER EJECUTIVO

Sector: Comercio Exterior y Turismo

12. Comisión de Promoción del Perú para la Exportación y el Turismo (PROMPERU)
13. Ministerio de Comercio Exterior y Turismo (MINCETUR).

Sector: Defensa

14. Instituto Geográfico Nacional (IGN)
15. Ministerio de Defensa (MINDEF)

Sector: Economía y Finanzas

16. Agencia de Promoción de la Inversión Privada (PROINVERSION)

17. Superintendencia de Mercado de Valores (SMV)
18. Ministerio de Economía y Finanzas (MEF)
19. Organismo Supervisor de las Contrataciones del Estado (OSCE)
20. Superintendencia Nacional de Aduanas y Administración Tributaria (SUNAT)
21. Oficina de Normalización Previsional (ONP)

Sector: Educación

22. Ministerio de Educación (MED)

Sector: Energía y Minas

23. Instituto Geológico Minero y Metalúrgico (INGEMMET)
24. Instituto Peruano de Energía Nuclear (IPEN)
25. Ministerio de Energía y Minas (MEM)

Sector: Interior

26. Ministerio del Interior (MININTER)
27. Policía Nacional del Perú (PNP)

Sector: Justicia

28. Ministerio de Justicia y Derechos Humanos (MINJUSDH)
29. Superintendencia Nacional de los Registros Públicos (SUNARP)

Sector: Mujer y Poblaciones Vulnerables

30. Ministerio de la Mujer y Poblaciones Vulnerables (MIMP)

Sector: Presidencia del Consejo de Ministros

31. Autoridad Nacional del Servicio Civil (SERVIR)
32. Centro Nacional de Planeamiento Estratégico (CEPLAN)
33. Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA)
34. Despacho Presidencial (DP)
35. Dirección Nacional de Inteligencia (DINI)
36. Instituto Nacional de Defensa Civil (INDECI)
37. Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
38. Instituto Nacional de Estadística e informática (INEI)
39. Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre (OSINFOR)
40. Organismo Supervisor de Inversión Privada en Telecomunicaciones. (OSIPTEL)
41. Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN)
42. Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (OSITRAN)
43. Presidencia del Consejo de Ministros (PCM)
44. Superintendencia Nacional de Servicios y Saneamiento (SUNASS)
45. Instituto Nacional de Radio y Televisión del Perú (IRTP)

Sector: Producción

46. Ministerio de la Producción (PRODUCE)

47. Fondo Nacional de Desarrollo Pesquero (FONDEPES)
48. Instituto del Mar del Perú (IMARPE)

Sector: Relaciones Exteriores

49. Agencia Peruana de Cooperación Internacional (APCI)
50. Ministerio de Relaciones Exteriores (RREE)

Sector: Salud

51. Instituto Nacional de Enfermedades Neoplásicas (INEN)
52. Instituto Nacional de Oftalmología (INO)
53. Instituto Nacional de Salud (INS)
54. Instituto Nacional de Salud Mental (ÍINSMHDHN)
55. Instituto Nacional Materno Perinatal (INMP)
56. Instituto Nacional de Salud del Niño (INSN)
57. Ministerio de Salud (MINSA)
58. Superintendencia Nacional de Aseguramiento en Salud (SUNASA)

Sector: Trabajo y Promoción del Empleo

59. Ministerio de Trabajo y Promoción del Empleo (MTPE)
60. Seguro Social de Salud (ESSALUD)

Sector: Transportes y Comunicaciones

61. Corporación Peruana de Aeropuertos y Aviación Comercial S.A. (CORPAC S.A.)
62. Empresa Nacional de Puertos S.A. (ENAPU S.A.)
63. Ministerio de Transportes y Comunicaciones (MTC)

64. Servicios Postales del Perú S.A. (SERPOST S.A.)

Sector: Vivienda, Construcción y Saneamiento

65. Banco de Materiales SAC (BANMAT SAC)

66. Fondo MI VIVIENDA S.A. (FMV S.A.)

67. Ministerio de Vivienda, Construcción y Saneamiento (VIVIENDA)

68. Servicio de Agua Potable y Alcantarillado de Lima (SEDAPAL)

69. Superintendencia Nacional de Bienes Estatales (SBN)

70. Comisión de la Formalización de la Propiedad Informal (COFOPRI)

Sector: Desarrollo e Inclusión Social

71. Ministerio de Desarrollo e Inclusión Social (MIDIS)

Las demás entidades de la Administración Pública no mencionadas en la presente resolución establecerán su cronograma de implantación de la fase uno, de acuerdo a sus recursos institucionales y a la naturaleza de sus funciones, los cuales deberán ser remitidas a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM), en un plazo no mayor de 180 días calendarios, contados a partir de la fecha de publicación de la presente resolución.

2.3. Definiciones Conceptuales

2.3.1. Análisis de Log de Seguridad

Un log es un registro de actividad de un sistema que se guarda en un archivo de texto sobre el cual podemos ver las acciones que se han realizado sobre un sistema de información en particular. Los log de seguridad nos permiten descubrir posibles ataques a los sistemas informáticos, ya que registran datos relevantes que nos permiten detectar información sobre posibles problemas o incidencias de seguridad. El procedimiento de seguridad que explota los log de seguridad es cuando se tiene un sistema de correlación de eventos, siendo estos eventos los registros o log de seguridad que permiten tener una visión y panorama de lo que ocurre en la seguridad de un sistema informático y dar respuesta oportuna ante incidentes de seguridad.

2.3.2. Auditabilidad

Propiedad que garantiza que todos los eventos de un sistema sean registrados para posteriores controles o auditorias.

2.3.3. Auditoría Informática

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto. La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo organizacional,

mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. En si la auditoria informática tiene dos tipos: Auditoría Interna, es aquella que se hace adentro de la empresa; sin contratar a personas de afuera; y la Auditoría Externa, aquella en la cual la empresa contrata a personas fuera de la organización para que realice la auditoria. Por lo tanto, auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia. Asimismo, los objetivos de una auditoría Informática son: el análisis de la eficiencia de los sistemas informáticos; la verificación del cumplimiento de la normativa en este ámbito; la revisión de la eficaz gestión de los recursos informáticos. Además, tiene como beneficios: la mejora de la imagen pública; la confianza en los usuarios sobre la seguridad y control de los servicios de TI; la optimización de las relaciones internas y del clima de trabajo; la disminución de los costos de la mala calidad; la generación de un balance de los riesgos en TI; la realización

de un control de la inversión en un entorno de TI. También, la auditoría informática sirve para mejorar ciertas características en la organización como: el desempeño; la fiabilidad; la eficacia; la rentabilidad; la seguridad; y la privacidad. Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas: el gobierno corporativo; la administración del ciclo de vida de los sistemas; el servicio de entrega y soporte; la protección y seguridad; y los planes de continuidad y recuperación de desastres. La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como los siguientes estándares: COBIT, COSO e ITIL.

2.3.4. Autenticación

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado.

2.3.5. Autenticidad

Propiedad que permite asociarla a una entidad (proceso o usuario). La preservación de esta propiedad permite asegurar el origen de la información, validando a la entidad emisora de la misma, evitándose el acceso descontrolado a la información y a los recursos, y la suplantación de identidades. La aplicación más evidente de la autenticación es en el control de accesos. En general, el proceso de

control de accesos consiste típicamente de dos etapas: identificación y autenticación. En la identificación, la entidad (proceso o usuario) dice quién es, y en la autenticación, la entidad demuestra ser quién dice ser. Identificar y autenticar no es lo mismo, la autenticación verifica la identificación.

2.3.6. Confiabilidad

Propiedad que garantiza que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones. Garantiza que la información es válida y utilizable en tiempo, forma y distribución.

2.3.7. Confianza

La confianza es un estado que es alcanzado cuando se tiene un nivel de confiabilidad cubierto y cuando una entidad es capaz de actuar de manera adecuada en una determinada situación adversa al reducir un escenario de incertidumbre. La confianza se verá más o menos reforzada en función del nivel de confiabilidad y seguridad.

2.3.8. Confidencialidad

Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada. Es la propiedad de que esta se

mantiene secreta y no revelada a entidades (individuos o procesos)no autorizados a conocerla. Al preservar dicha propiedad, se garantiza que la información es conocida y accedida sólo por aquellas personas autorizadas a hacerlo.

2.3.9. Control

Propiedad que permite asegurar que sólo los usuarios autorizados pueden decidir quién accede a la información, cuándo y cómo.

2.3.10. Credencial

Una credencial es un documento de identificación que atestigua o autoriza la identidad otorgada a un individuo por un tercero con autoridad. Su fin es que una entidad acreditada mediante una credencial tenga acceso a recursos de información que le son asignados por una autoridad responsable. Asimismo, permite que esta entidad pueda ser ubicada por diversas razones, tanto administrativas como dentro del alcance de la seguridad de la información.

2.3.11. Disponibilidad

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Es la propiedad de que esta se mantiene accesible y usable cada vez que una entidad autorizada a hacerlo lo requiera. La preservación de dicha propiedad garantiza que la información estará siempre disponible para ser usada bajo demanda, ya sea para su consulta o procesamiento, por las personas o procesos autorizados. La disponibilidad de un sistema es la propiedad de que los recursos del mismo se

mantienen operativos, cada vez que una entidad autorizada los necesite. La preservación de esta propiedad requiere que la información se mantenga correctamente almacenada, en los formatos preestablecidos para su recuperación en forma satisfactoria, con el hardware que la contiene y el software correspondiente con el funcionamiento correcto.

2.3.12. Estándar

Es un proceso, protocolo o técnica utilizada para hacer algo concreto y contienen documentos técnico-legales con las siguientes características: contienen especificaciones técnicas de aplicación voluntaria; son elaborados por consenso de las partes interesadas: fabricantes; administraciones; usuarios y consumidores; centros de investigación y laboratorios; asociaciones y Colegios Profesionales; agentes sociales, entre otros; están basados en los resultados de la experiencia y el desarrollo tecnológico; son aprobados por un organismo nacional, regional o internacional de normalización reconocido; y están disponibles al público. Por ello, los estándares ofrecen un lenguaje de punto común de comunicación entre las empresas, la administración pública, los usuarios y consumidores.

2.3.13. Evaluación De Riesgos

La evaluación de riesgos es una consideración sistemática de los siguientes puntos: el Impacto potencial, por falla de seguridad, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos; y la probabilidad de ocurrencia de dicha falla, tomando en

cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados. Por ello, la evaluación del riesgo debe incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de estos (evaluación del riesgo). Asimismo, los resultados de esta evaluación ayudarán a: orientar y a determinar las prioridades y las acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información; para la implantación de los controles seleccionados a fin de brindar protección contra dichos riesgos; guiar y determinar las acciones de gestión apropiadas para la administración de los riesgos concernientes a seguridad de la información, y establecer las prioridades para manejar los riesgos de la seguridad de la información para implementar los controles seleccionados para protegerse contra estos riesgos.

2.3.14. Gestión De Riesgos

La gestión de riesgos es un proceso iterativo y recurrente a lo largo del desarrollo de cualquier proyecto. El propósito de la gestión de riesgos es minimizar la probabilidad y consecuencias de los riesgos negativos (o amenazas) y maximizar la probabilidad y consecuencias de los riesgos positivos (u oportunidades) identificados para un en particular de tal forma que los objetivos se cumplan. Esto se consigue siguiendo una serie de pautas: la identificación de todos los riesgos conocidos del proyecto; la realización de una evaluación de la probabilidad de ocurrencia y del impacto potencial; la cuantificación del coste de los riesgos

en caso de que ocurrieran; la creación de planes de acción para gestionar los riesgos de alta prioridad; y el reconocimiento y gestión de los riesgos lo antes posible. Asimismo, los beneficios que se obtienen al llevar a cabo una buena gestión de los riesgos son: la reducción de costos; la mejora de la satisfacción de los beneficiarios; el incremento de la capacidad y probabilidades de éxito; y la disminución drástica del factor incertidumbre. Por otro lado, ayuda a la organización a conseguir sus objetivos e intereses evitando problemas que podrían causar pérdidas inesperadas y no planificadas. Por ello, en toda gestión de riesgos es necesario desarrollar un plan de gestión de riesgos.

2.3.15. Información

Es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando técnicas criptográficas entre otras herramientas.

2.3.16. Incidente de Seguridad

Es un hecho, evento o amenaza que atenta contra la confidencialidad, integridad y disponibilidad de un sistema de información; entonces un incidente de seguridad es un evento adverso, que puede comprometer o compromete o degrada los atributos de seguridad de la información. Un incidente de seguridad se divide en diferentes fases: la fase inicial (preparación y prevención, y detección y pre análisis); la. Contención, erradicación y recuperación (notificación, análisis, contención y erradicación); la recuperación del

incidente (recuperación); y la actividad después del incidente (reflexión y documentación).

2.3.17. Integridad

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos seria la correspondencia entre los datos y los hechos que refleja. Es la propiedad de que esta permanece coherente, completa e inalterada, a menos, en este último caso, que sea modificada por una entidad (individuo o proceso) autorizada, y lo haga en forma pertinente y correcta. La preservación de dicha propiedad garantiza la exactitud, coherencia y totalidad de la información y los métodos de procesamiento. La integridad de un sistema es la propiedad de que los recursos del mismo permanecen inalterados, ya sean recursos de almacenamiento, procesamiento o distribución. La integridad de un activo es la propiedad que salvaguarda su exactitud y totalidad.

2.3.18. No Repudio

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades: el No Repudio en origen, el emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor

recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario; y el No Repudio en destino, el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor. Por lo tanto, si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el No Repudio prueba que el autor envió la comunicación (No Repudio en origen) y que el destinatario la recibió (No Repudio en destino). En otras palabras, el No Repudio es el atributo de seguridad o propiedad de la información que garantiza que cualquier entidad que envió o recibió información, no pueda alegar ante terceros, que no la envió o no la recibió.

2.3.19. Observación

En auditoria se entiende por observación a un aspecto de un requisito que podría mejorarse y que de manera obligatoria debe realizarse. Sin embargo, no requiere que se efectúe de manera inmediata.

2.3.20. Riesgo

Es la probabilidad de materialización de una amenaza con un determinado impacto, mediante la explotación de las vulnerabilidades de un activo crítico.

CAPÍTULO III
HIPÓTESIS Y VARIABLES

3.1. Hipótesis General

Existe relación entre implantación de la NTP 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado peruano.

3.2. Hipótesis Específicas

- Existe relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano.

- Existe relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano.

- Existe relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano.

3.3. Identificación de Variables

Las variables de estudio son:

- Variable Independiente: Norma Técnica Peruana ISO/IEC 27001:2008.
- Variable Dependiente: Seguridad de la Información.

3.4. Operacionalización de Variables

Tabla N° 3.1

OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	CONCEPTUALIZACIÓN DE LA VARIABLE	DIMENSIONES	INDICADORES
Norma Técnica Peruana ISO/IEC 27001:2008	Modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de Información (SGSI)	Organización	¿Se obtuvo apoyo institucional?
			¿Se determinó el alcance del sistema de Gestión de Seguridad de Información?
			¿Se determinó la declaración de Política de Seguridad de la Información y objetivos?
			¿Se determinó los criterios para la evaluación y aceptación de riesgos?
		Planificación	¿Se realizó la evaluación de Riesgos?
			¿Se desarrolló el plan de tratamiento de riesgo?
			¿Se desarrolló el documento de Declaración de Aplicabilidad?
		Despliegue	¿Se elaboró el Plan de trabajo priorizado?
			¿Se desarrolló los Documentos y registros necesarios?
			¿Se Implementaron los controles seleccionados?
		Revisión	¿Se cuenta con registros que evidencien el Monitoreo de desempeño del SGSI?
			¿Se cuenta con registros de la mejora de la Gestión de incidentes?
		Consolidación	¿Se realizaron auditorías al SGSI?
			¿Se implementaron Acciones correctivas a las observaciones encontradas en las auditorias?
			¿Se implementaron Acciones preventivas?
Seguridad de la Información	(Standardization & Commission, 2014) Es la preservación de la confidencialidad, integridad y disponibilidad de la información. También, consiste en la aplicación y gestión de las medidas de seguridad apropiadas que implica la consideración de una amplia gama de amenazas	Confidencialidad	¿# de incidentes que afectaron la confidencialidad de la información?
		Integridad	¿# de incidentes que afectaron la integridad de la información?
		Disponibilidad	¿# de incidentes que afectaron la disponibilidad de la información?

CAPÍTULO IV
METODOLOGÍA

4.1. Tipo de Investigación

El presente estudio según (Hernandez, Fernandez, & Baptista, 2010) 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.

4.2. Diseño de la Investigación

La presente investigación es de tipo No experimental - Transversal (Hernandez, Fernandez, & Baptista, 2010), 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.

4.3. Población – Muestra

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 codificaran los nombres de cada una de ellas con la denominación "Ministerio NN".

Se utilizará un muestreo probabilístico de tipo aleatorio simple, el cual se caracteriza porque el investigador elige de manera aleatoria la población que estudia (Carrasco Díaz, 2005).

4.4. Técnicas e instrumentos de recolección de datos

Para la presente investigación se han empleado 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.

Tabla N° 4.1

TÉCNICAS E INSTRUMENTOS DE ESTUDIO POR INDICADOR

VARIABLE	TÉCNICA	INSTRUMENTO
NTP 27001:2008 EDI	Encuesta	Cuestionario
Seguridad de la información	Encuesta	Cuestionario

Fuente: Elaboración propia

4.5. Plan de Análisis estadísticos de datos

Los datos recolectados serán procesados en el software estadístico IBM SPSS Statistics versión 23.0, donde cada dimensión tendrá un peso de 1, por lo cual, este valor debe ser dividido entre la cantidad de ítems por dimensión. La suma del

valor obtenido por cada uno de los ítems permitirá saber el grado de implantación de cada ministerio siendo 5 el valor máximo de implantación.

Tabla N° 4.2

VALORIZACIÓN DE VARIABLES

DIMENSION		ITEM	PESO	VALOR
Organización	1	Se ha elaborado el Documento del Alcance del SGSI	0.33	1
	2	Se ha elaborado el Documento de Política de SGSI	0.33	
	3	Se ha elaborado el Documento de Criterios de evaluación y aceptación de riesgos	0.33	
Planificación	4	Se ha elaborado el Documento de Evaluación de riesgo	0.33	1
	5	Se ha elaborado el Documento de plan de tratamiento de riesgo	0.33	
	6	Se ha elaborado el Documento de Declaración de Aplicabilidad	0.33	
Despliegue	7	Se ha elaborado el Documento Plan de Trabajo	0.50	1
	8	Se implementaron controles de seguridad	0.50	
Revisión	9	¿Se cuenta con registros que evidencien el Monitoreo de desempeño del SGSI?	0.50	1
	10	¿Se cuenta con registros de la mejora de la Gestión de incidentes?	0.50	
Consolidación	11	¿Se realizaron auditorías al SGSI?	0.33	1
	12	¿Se implementaron Acciones correctivas a las observaciones encontradas en las auditorias?	0.33	
	13	¿Se implementaron Acciones preventivas?	0.33	

Fuente: Elaboración propia

Para el caso de la variable de la seguridad de la información, se obtendrá el nivel de Seguridad de la Información del promedio de cada una de sus dimensiones.

Para analizar la relación entre la implantación de la NTP 27001:2008 EDI y la Seguridad de la Información en los Ministerios del Estado Peruano se realizará a través del método estadístico de Coeficiente de Correlación de Spearman donde la significancia estadística a considerarse es a partir del 5% de probabilidad.

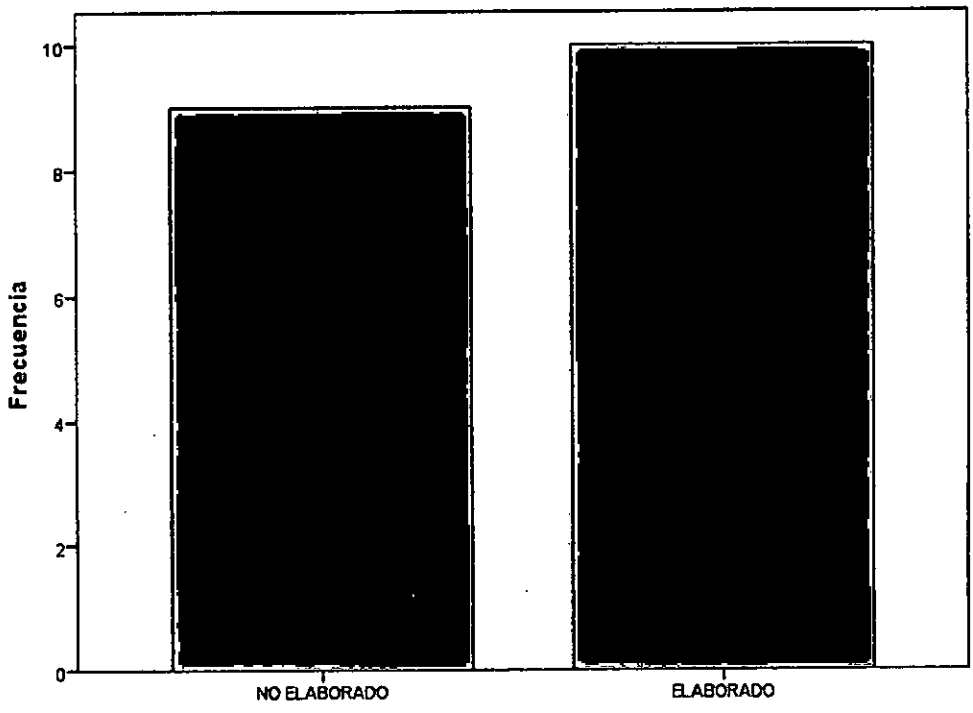
CAPÍTULO V
RESULTADOS

En este punto se presentan los resultados del estudio. En primer lugar se presentan los hallazgos en cuanto a los indicadores de la variable Norma Técnica Peruana ISO/IEC 27001:2008; luego, se presenta los resultados de los indicadores de la variable Seguridad de la información; por último se presenta el análisis de confiabilidad

5.1. Norma Técnica Peruana ISO/IEC 27001:2008

Gráfico N° 5.1

DOCUMENTO DEL ALCANCE DEL SGSI



Documento del alcance del SGSI

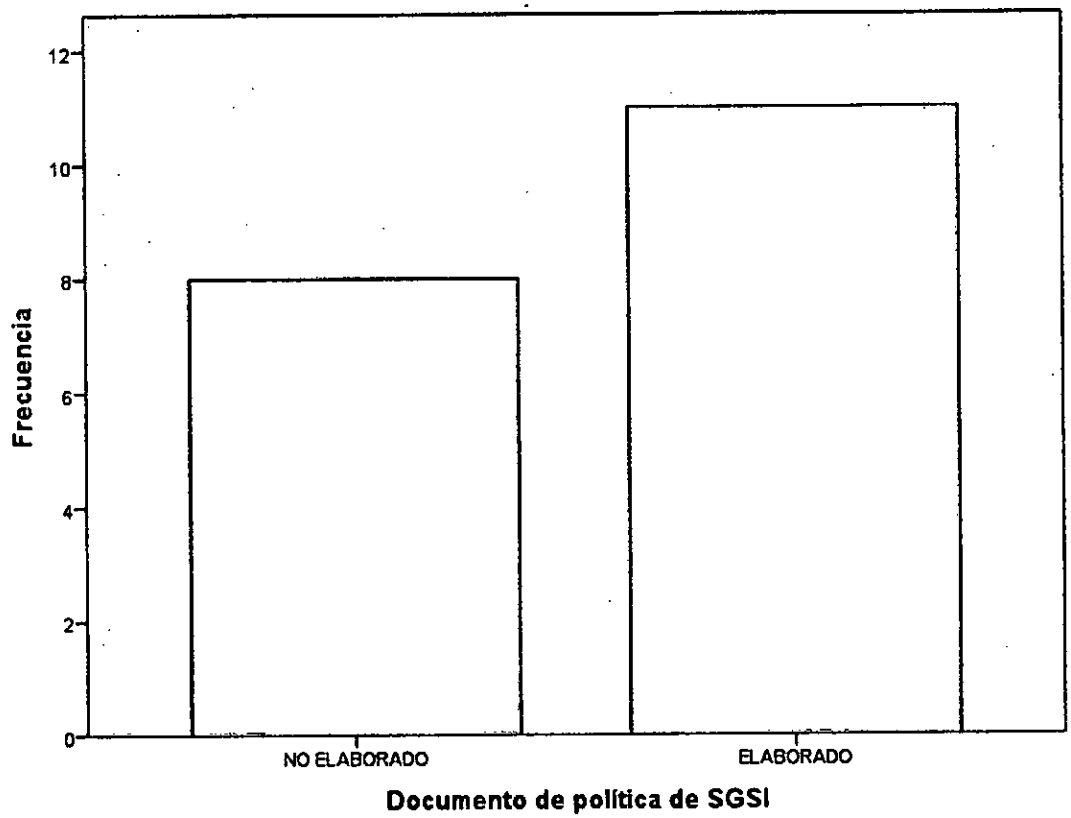
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	9	47,4	47,4	47,4
	ELABORADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 52.6% de los ministerios han elaborado el documento del alcance del SGSI, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.2

DOCUMENTO DE POLÍTICA DE SGSI



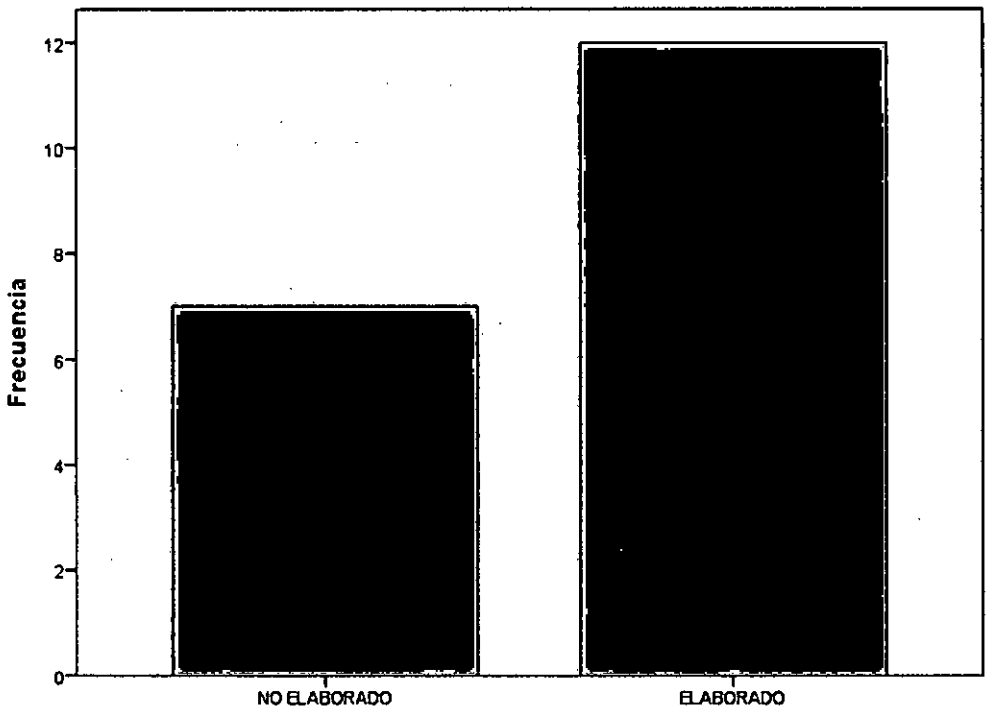
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	8	42,1	42,1	42,1
	ELABORADO	11	57,9	57,9	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 57.9% de los ministerios han elaborado el documento de política de SGSI, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.3

DOCUMENTO DE CRITERIOS DE EVALUACIÓN Y ACEPTACIÓN DE RIESGOS



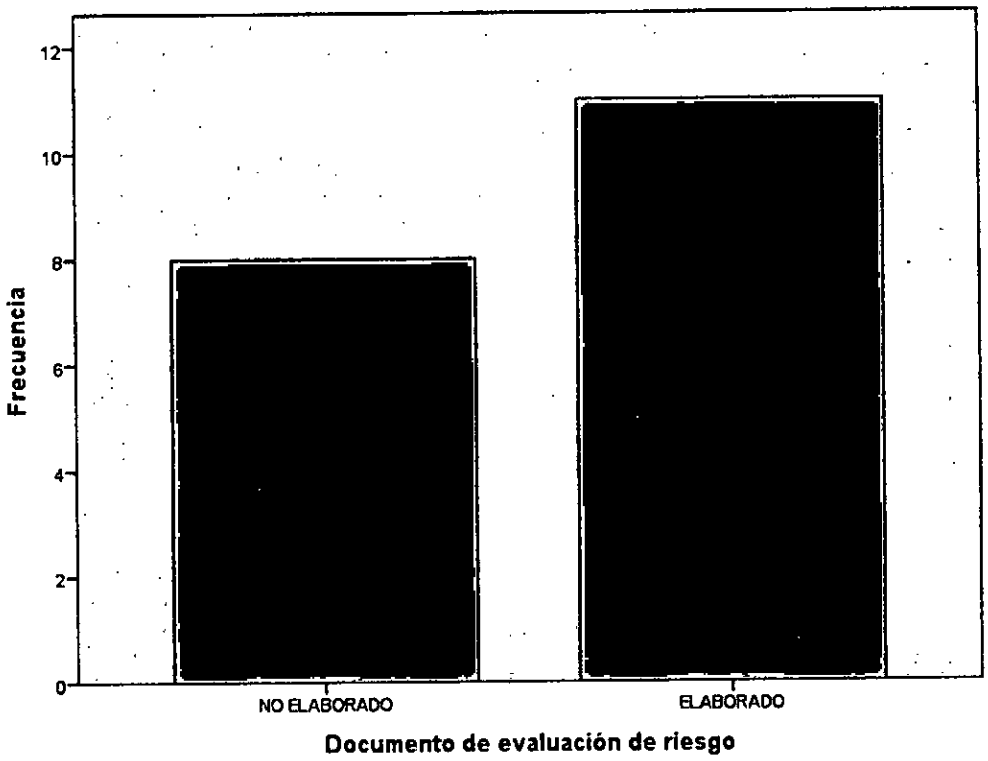
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	7	36,8	36,8	36,8
	ELABORADO	12	63,2	63,2	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 63.2% de los ministerios han elaborado el documento de criterios de evaluación y aceptación de riesgos, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.4

DOCUMENTO DE EVALUACIÓN DE RIESGO



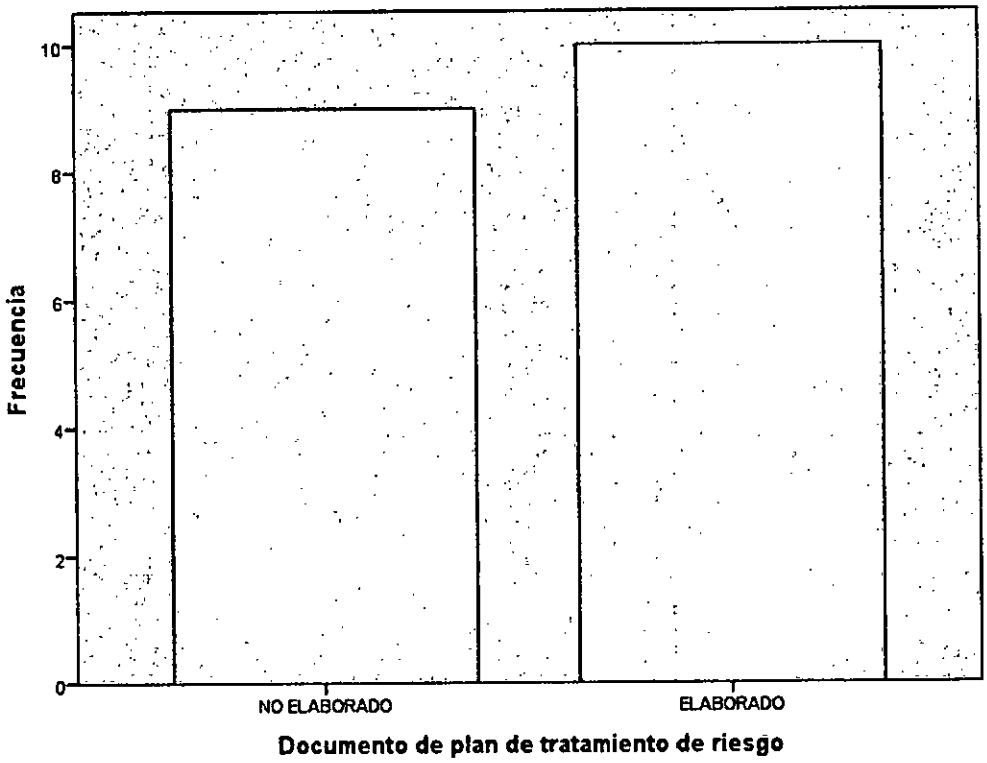
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	8	42,1	42,1	42,1
	ELABORADO	11	57,9	57,9	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 57.9% de los ministerios han elaborado el documento de evaluación de riesgos, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.5

DOCUMENTO DE PLAN DE TRATAMIENTO DE RIESGO



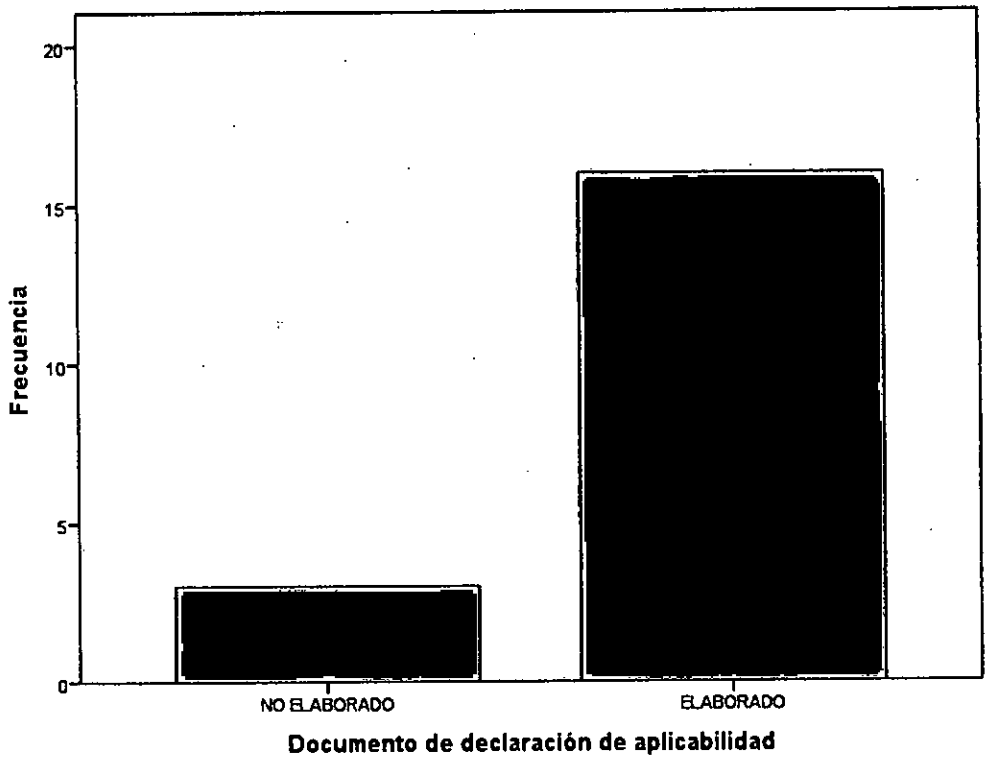
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	9	47,4	47,4	47,4
	ELABORADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 52.6% de los ministerios han elaborado el documento de plan de tratamiento de riesgo, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.6

DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD



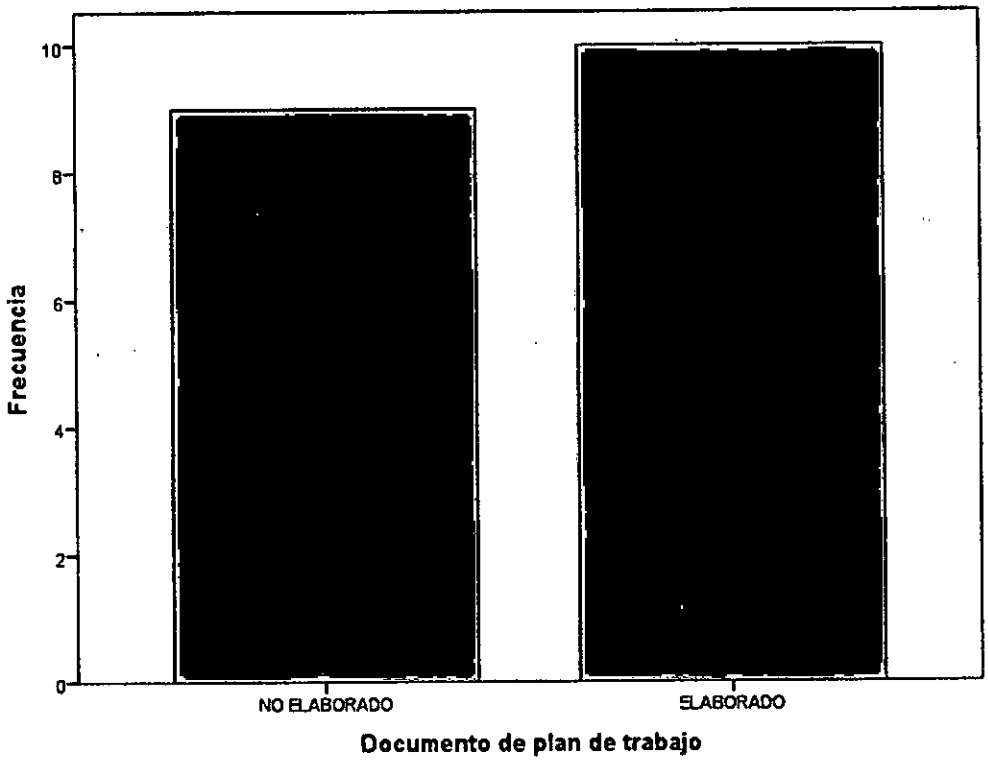
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	3	15,8	15,8	15,8
	ELABORADO	16	84,2	84,2	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 84.2% de los ministerios han elaborado el documento de declaración de aplicabilidad, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.7

DOCUMENTO DE PLAN DE TRABAJO



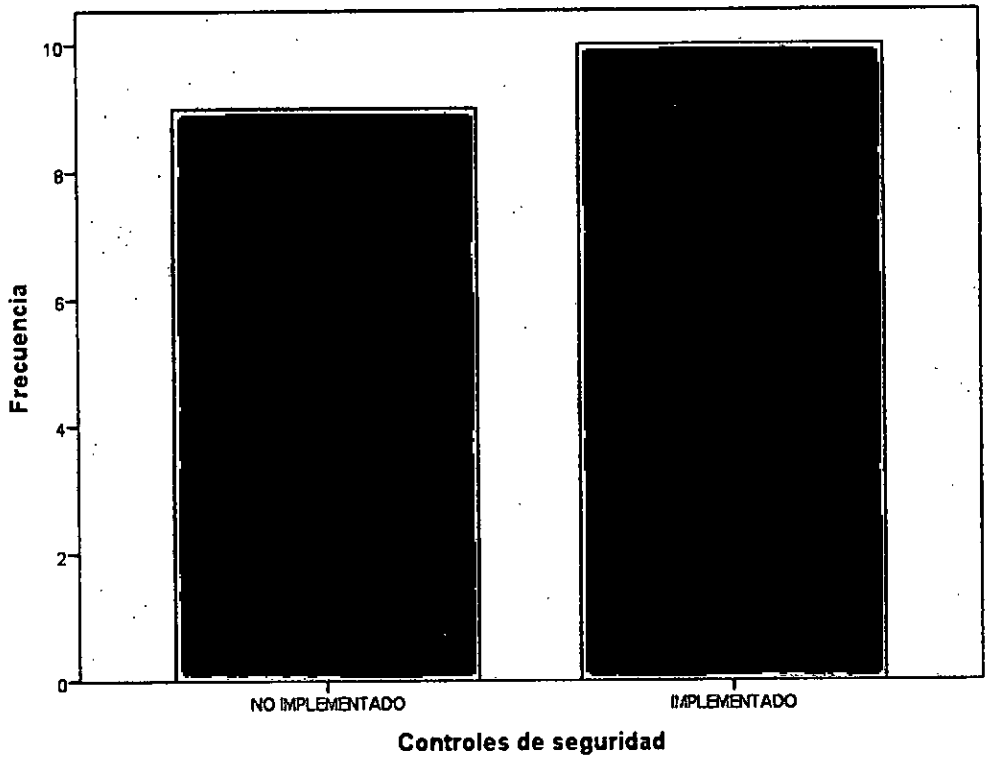
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO ELABORADO	9	47,4	47,4	47,4
	ELABORADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 52.6% de los ministerios han elaborado el documento de plan de trabajo, lo que indica que el mayor número de ministerios han elaborado este documento.

Gráfico N° 5.8

CONTROLES DE SEGURIDAD



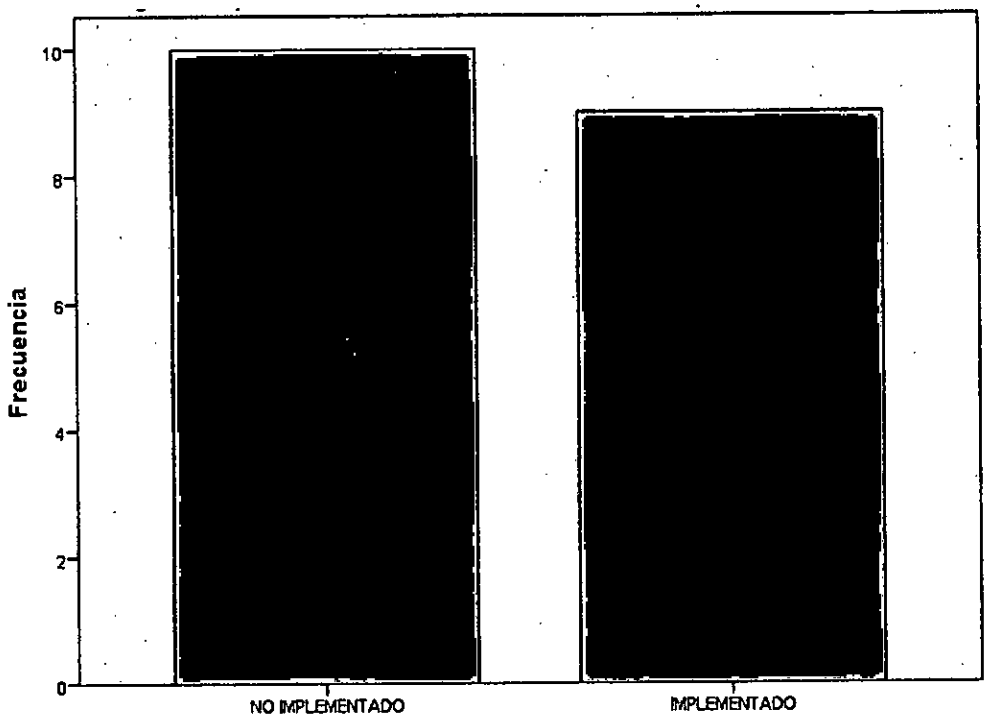
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO IMPLEMENTADO	9	47,4	47,4	47,4
	IMPLEMENTADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 52.6% de los ministerios han implementado los controles de seguridad, lo que indica que el mayor número de ministerios han implementado los controles de seguridad.

Gráfico N° 5.9

REGISTROS QUE EVIDENCIEN EL MONITOREO DE DESEMPEÑO DEL SGSI



Registros que evidencien el Monitoreo de desempeño del SGSI

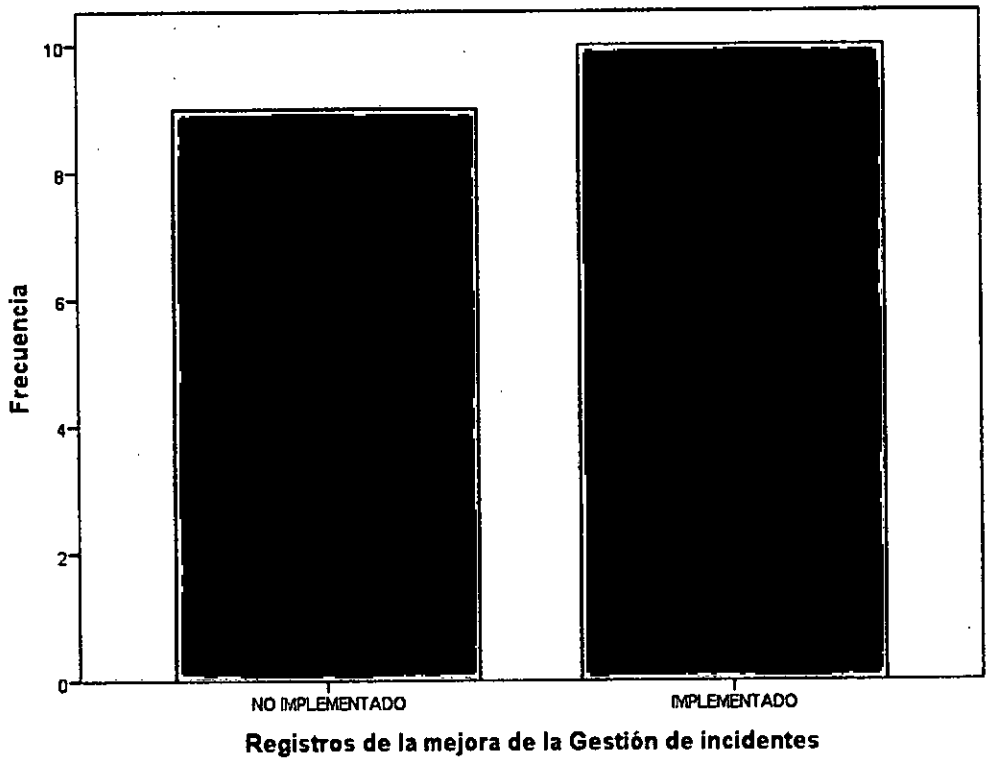
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO IMPLEMENTADO	10	52,6	52,6	52,6
	IMPLEMENTADO	9	47,4	47,4	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 47.9% de los ministerios han implementado los registros que evidencien el monitoreo de desempeño del SGSI, lo que indica que el menor número de ministerios han implementado estos registros

Gráfico N° 5.10

REGISTROS DE LA MEJORA DE LA GESTIÓN DE INCIDENTES



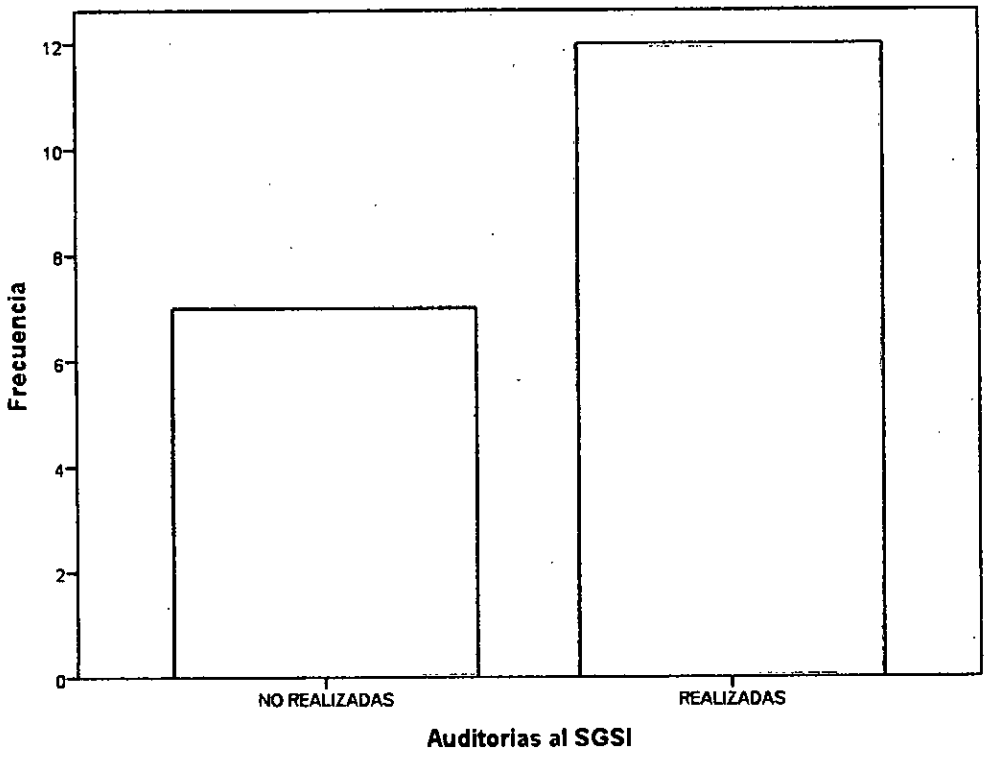
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO IMPLEMENTADO	9	47,4	47,4	47,4
	IMPLEMENTADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 52.6% de los ministerios han implementado los registros de mejora de la gestión de incidentes, lo que indica que el mayor número de ministerios han implementado estos registros.

Gráfico N° 5.11

AUDITORIAS AL SGSI



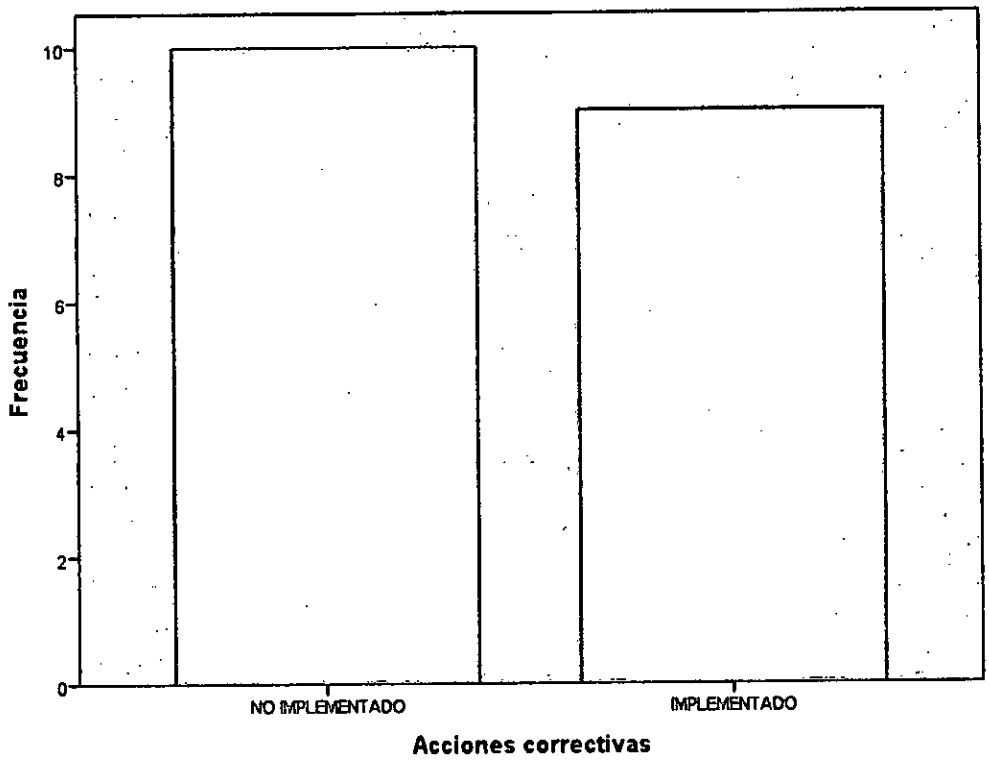
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO REALIZADAS	7	36,8	36,8	36,8
	REALIZADAS	12	63,2	63,2	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 63.2% de los ministerios han implementado los controles de seguridad, lo que indica que el mayor número de ministerios han realizado las auditorias al SGSI.

Gráfico N° 5.12

ACCIONES CORRECTIVAS



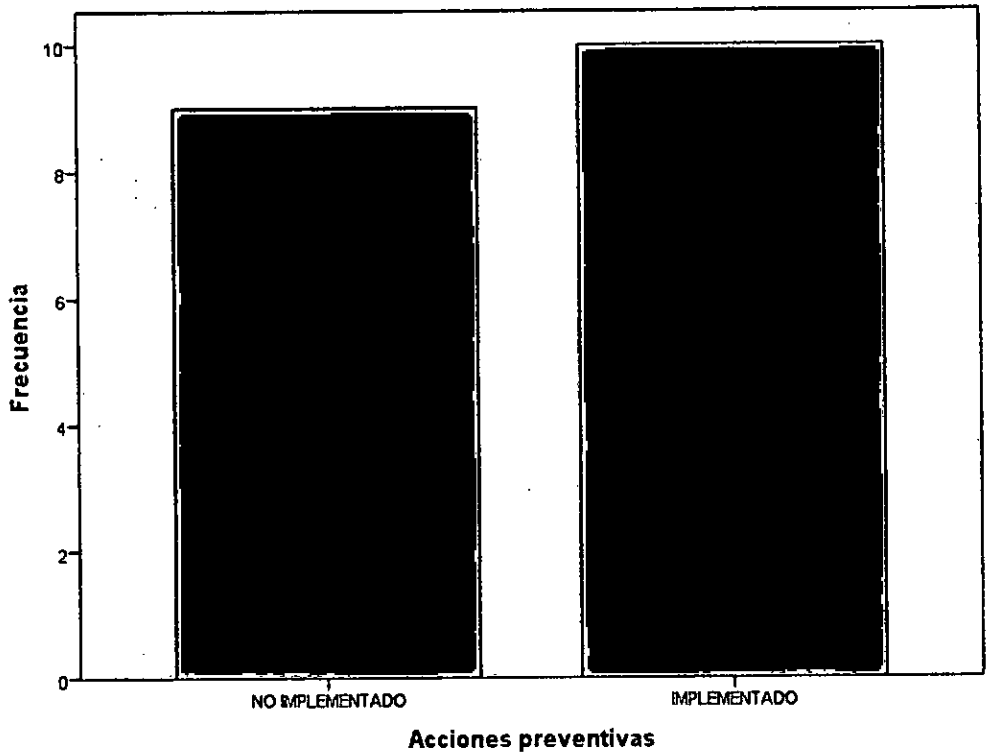
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO IMPLEMENTADO	10	52,6	52,6	52,6
	IMPLEMENTADO	9	47,4	47,4	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 47.9% de los ministerios han implementado las acciones correctivas, lo que indica que el menor número de ministerios han elaborado las acciones correctivas.

Gráfico N° 5.13

ACCIONES PREVENTIVAS



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO IMPLEMENTADO	9	47,4	47,4	47,4
	IMPLEMENTADO	10	52,6	52,6	100,0
	Total	19	100,0	100,0	

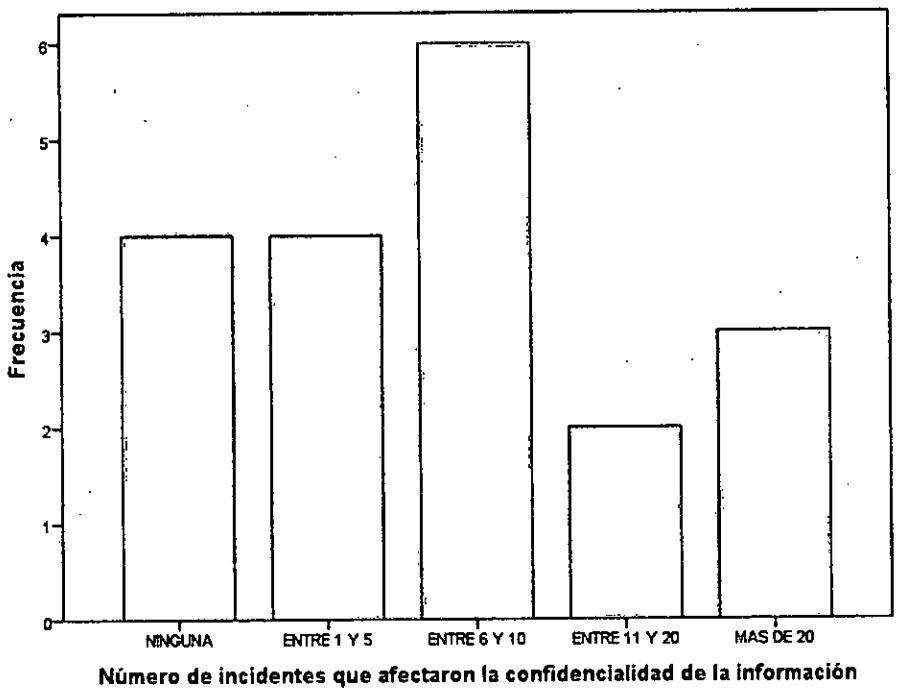
Fuente: Elaboración propia

El 52.6% de los ministerios han implementado las acciones preventivas, lo que indica que el mayor número de ministerios han implementado las acciones preventivas.

5.2. Seguridad de la Información

Gráfico N° 5.14

NÚMERO DE INCIDENTES QUE AFECTARON LA CONFIDENCIALIDAD DE LA INFORMACIÓN



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NINGUNA	4	21,1	21,1	21,1
	ENTRE 1 Y 5	4	21,1	21,1	42,1
	ENTRE 6 Y 10	6	31,6	31,6	73,7
	ENTRE 11 Y 20	2	10,5	10,5	84,2
	MAS DE 20	3	15,8	15,8	100,0
	Total	19	100,0	100,0	

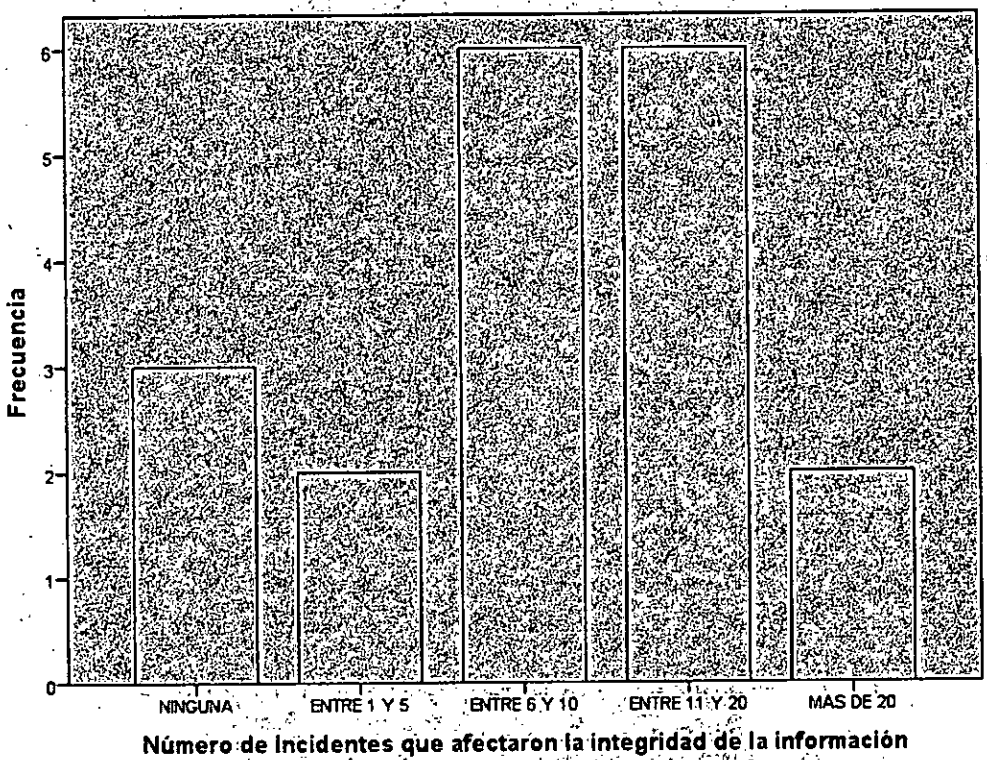
Fuente: Elaboración propia

El 31.6% de los ministerios han sufrido entre 6 y 10 incidentes que afectaron la confidencialidad de la información, el 10.5% de los ministerios

entre 11 y 20 incidentes y el 15.8% de los ministerios más de 20 incidentes, lo que equivale al 57.9% de ministerios que han sufrido un alto número de incidentes que afectaron la confidencialidad de la información.

Gráfico N° 5.15

NÚMERO DE INCIDENTES QUE AFECTARON LA INTEGRIDAD DE LA INFORMACIÓN



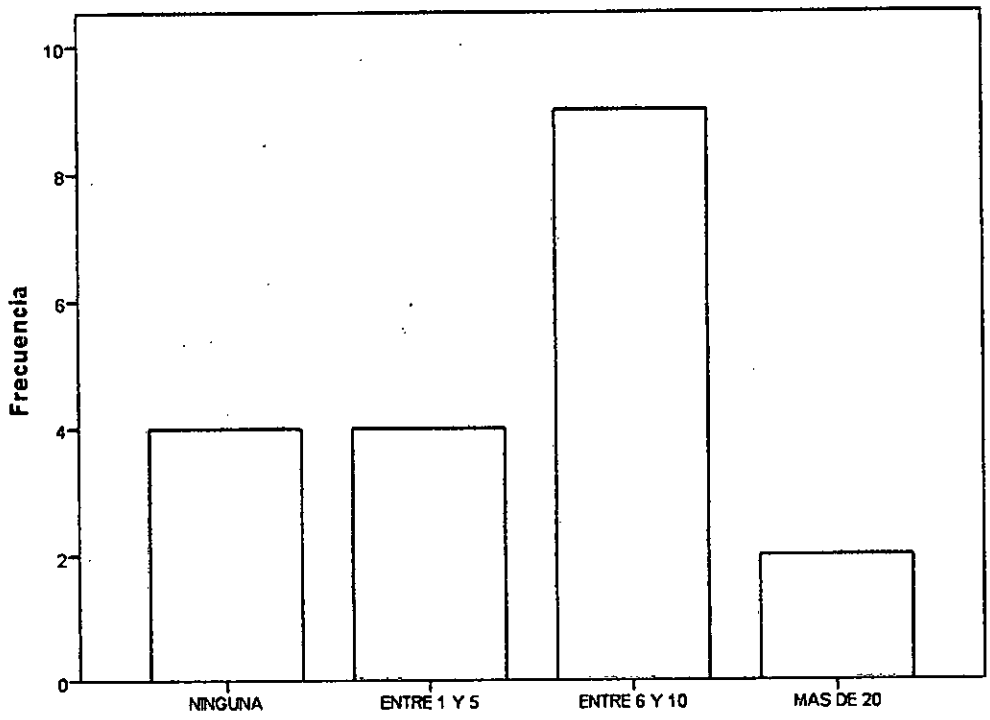
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NINGUNA	3	15,8	15,8	15,8
	ENTRE 1 Y 5	2	10,5	10,5	26,3
	ENTRE 6 Y 10	6	31,6	31,6	57,9
	ENTRE 11 Y 20	6	31,6	31,6	89,5
	MAS DE 20	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 31.6% de los ministerios han sufrido entre 6 y 10 incidentes que afectaron la integridad de la información, el 31.6% de los ministerios entre 11 y 20 incidentes y el 10.5% de los ministerios más de 20 incidentes, lo que equivale al 73.4% de los ministerios que han sufrido un alto número de incidentes que afectaron la integridad de la información.

Gráfico N° 5.16

NÚMERO DE INCIDENTES QUE AFECTARON LA DISPONIBILIDAD DE LA INFORMACIÓN



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NINGUNA	4	21,1	21,1	21,1
	ENTRE 1 Y 5	4	21,1	21,1	42,1
	ENTRE 6 Y 10	9	47,4	47,4	89,5
	MAS DE 20	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Fuente: Elaboración propia

El 47.4% de los ministerios han sufrido entre 6 y 10 incidentes que afectaron la integridad de la información y el 10.5% de los ministerios más de 20 incidentes, lo que equivale al 57.9% de los ministerios que han sufrido un alto número de incidentes que afectaron la disponibilidad de la información.

5.3. Determinación de Datos Adicionales

- Para determinar el grado de implantación de la NTP 27001:2008 EDI en los Ministerios del Estado Peruano al 2015 se ha calculado el promedio entre los grados obtenidos en cada uno de ellos.

Tabla N° 5.1

GRADO DE IMPLANTACIÓN POR MINISTERIO

Ministerios	Grado
Ministerio 01	4.33
Ministerio 02	2.33
Ministerio 03	3.17
Ministerio 04	2.33
Ministerio 05	2.17
Ministerio 06	5.00
Ministerio 07	4.50
Ministerio 08	1.17
Ministerio 09	0.33
Ministerio 10	5.00
Ministerio 11	1.33
Ministerio 12	5.00
Ministerio 13	2.00
Ministerio 14	2.00
Ministerio 15	1.17
Ministerio 16	0.67
Ministerio 17	5.00
Ministerio 18	5.00
Ministerio 19	0.67
Promedio	**2.80**

Fuente: Elaboración propia

- Para determinar el nivel de incidentes a la Seguridad de la información sufridos por los Ministerios del Estado Peruano al 2015 se calculó el promedio del nivel de incidentes por cada uno de ellos.

Tabla N° 5.2

NIVEL DE INCIDENTES

Ministerios	Nivel de Incidencias
Ministerio 01	1.00
Ministerio 02	4.67
Ministerio 03	3.00
Ministerio 04	3.33
Ministerio 05	3.67
Ministerio 06	1.67
Ministerio 07	3.00
Ministerio 08	3.00
Ministerio 09	4.00
Ministerio 10	1.67
Ministerio 11	3.67
Ministerio 12	2.33
Ministerio 13	4.00
Ministerio 14	3.00
Ministerio 15	3.00
Ministerio 16	3.00
Ministerio 17	1.00
Ministerio 18	1.67
Ministerio 19	3.00
Promedio de Nivel de Incidentes	**2.83**

Fuente: Elaboración propia

5.4. Análisis de Confiablidad

Para realizar la prueba de confiabilidad de Alfa de Cronbach se debe tener variables categóricas, las numéricas no se les aplican esta prueba, por ello la variable implantación de la NTP 27001:2008 EDI, fue evaluado utilizando la tabla de valorización de variables y obteniendo un valor de 0.907 cercano a 1, dándole alta confiabilidad.

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Tabla N° 5.3

RESUMEN DEL PROCESAMIENTO RELACIÓN DE LA NTP ISO/IEC 27001:2008 EDI Y LA SEGURIDAD DE LA INFORMACIÓN

		N	%
Casos	Válido	19	100,0
	Excluido	0	,0
	Total	19	100,0

Fuente: Elaboración propia

Tabla N° 5.4

ESTADÍSTICOS DE FIABILIDAD

Alfa de Cronbach	N de elementos
,907	13

Fuente: Elaboración propia

Tabla N° 5.5

ESTADÍSTICOS DE TOTAL DE ELEMENTO

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
Alcance	6,84	16,807	,702	,897
Politica	6,79	17,287	,588	,902
EvaAceRiesgo	6,74	17,871	,455	,907
EvaRiesgo	6,79	17,509	,532	,904
PlanTrataRiesgo	6,84	17,585	,506	,906
Aplicabilidad	6,53	18,374	,470	,906
PlanTrabajo	6,84	17,807	,451	,908
ControlesSeguridad	6,84	16,474	,789	,893
RegistroMonitoreo	6,89	16,988	,655	,899
RegMejoraIncidente	6,84	16,807	,702	,897
Auditoria	6,74	17,316	,597	,902
AccionesCorrectivas	6,89	16,211	,859	,890
AccionesPreventivas	6,84	16,474	,789	,893

Fuente: Elaboración propia

CAPÍTULO VI
DISCUSION DE RESULTADOS

A continuación se presenta la tabla de interpretación de los valores de los coeficientes de correlación, en donde se muestra el rango de valores de los coeficientes de correlación, a fin de interpretar los resultados de correlación de las variables de este estudio de investigación. Esta tabla ha sido elaborada como un derivado según estudio de (Hernandez, Fernandez, & Baptista, 2010)

Tabla N° 6.1

INTERPRETACIÓN DE LOS VALORES DE LOS COEFICIENTES DE CORRELACIÓN

Rango coeficiente	Interpretación
-1	Correlación negativa perfecta
(-)0.9 – (-)0.75	Correlación negativa muy fuerte
(-)0.75 – (-)0.5	Correlación negativa significativa
(-)0.5 – (-)0.1	Correlación negativa media
(-)0.1 – 0	Correlación negativa débil
0	Correlación nula
0 – (+)0.1	Correlación positiva débil
(+)0.1 – (+)0.5	Correlación positiva media
(+)0.5 – (+)0.75	Correlación positiva significativa
(+)0.75 – (+)0.9	Correlación positiva muy fuerte
1	Correlación positiva perfecta

Fuente: Elaboración propia

Nivel de significancia: Usando un nivel de significancia ($\propto$ = 0.05) del 5%. El nivel de confianza (1- $\propto$ = 0.95) es del 95%

6.1. Contrastación de Hipótesis con los resultados

Sub Hipótesis 1

Tabla N° 6.2

COEFICIENTE DE CORRELACIÓN DE SPEARMAN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA CONFIDENCIALIDAD DE LA INFORMACIÓN

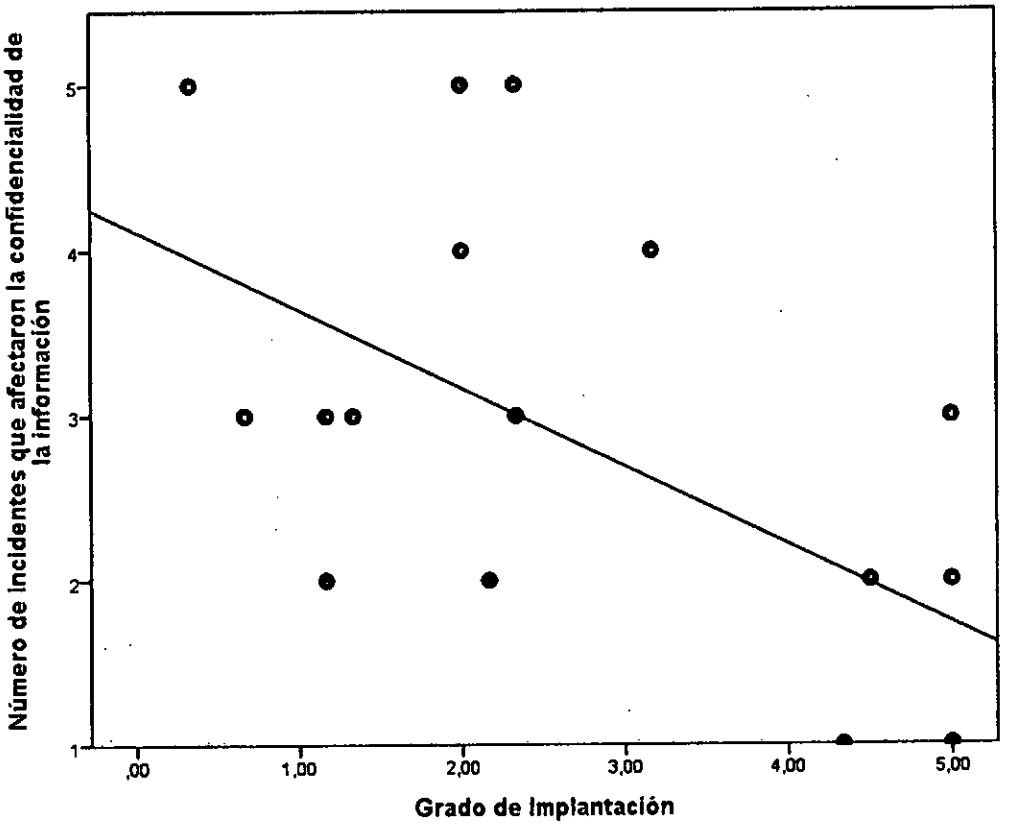
			Grado de Implantación	Número de incidentes que afectaron la confidencialidad de la información
Rho de Spearman	Grado de Implantación	Coeficiente de correlación	1,000	-,574*
		Sig. (bilateral)	.	,010
		N	19	19
	Número de incidentes que afectaron la confidencialidad de la información	Coeficiente de correlación	-,574*	1,000
		Sig. (bilateral)	,010	.
		N	19	19

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia

Gráfico N° 6.1

DISPERSIÓN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA CONFIDENCIALIDAD DE LA INFORMACIÓN



Contrastación de Hipótesis N° 1

NC0: No existe relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano.

NC1: Existe relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano.

Método estadístico: Coeficiente de correlación de Spearman

Coeficiente de correlación: -0.574

Nivel de Significancia: $\alpha = 0.05$

Resultado nivel de significancia: 0.010

Decisión: El coeficiente de correlación indica que existe una correlación negativa significativa. Además la magnitud de significancia es menor a 0.05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Conclusión: La implantación de la NTP 27001:2008 EDI tiene relación con la confidencialidad de la información en los Ministerios del Estado peruano.

Sub Hipótesis 2

Tabla N° 6.3

COEFICIENTE DE CORRELACIÓN DE SPEARMAN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA INTEGRIDAD DE LA INFORMACIÓN

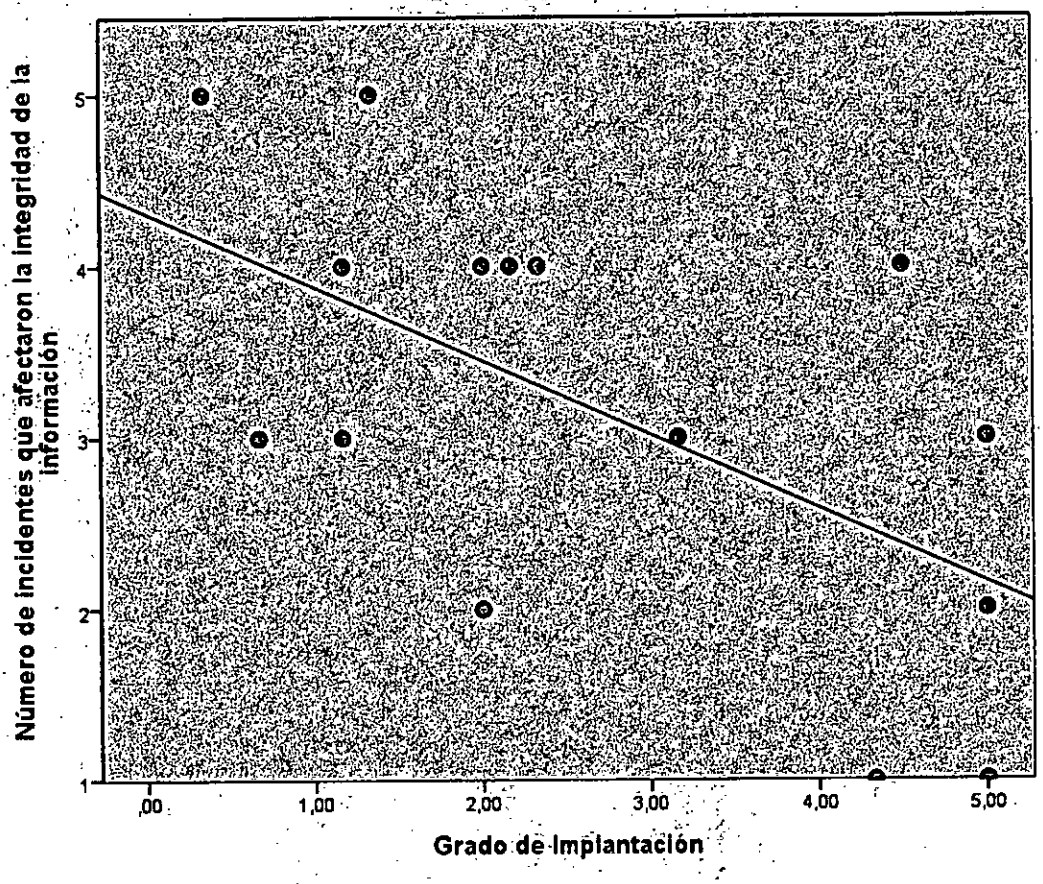
			Grado de Implantación	Número de incidentes que afectaron la integridad de la información
Rho de Spearman	Grado de Implantación	Coeficiente de correlación	1,000	-,518*
		Sig. (bilateral)	.	,023
		N	19	19
	Número de incidentes que afectaron la integridad de la información	Coeficiente de correlación	-,518*	1,000
		Sig. (bilateral)	,023	.
		N	19	19

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia

Gráfico N° 6.2

DISPERSIÓN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA INTEGRIDAD DE LA INFORMACIÓN



Contrastación de Hipótesis N° 2

NI0: No existe relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano.

NI1: Existe relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano.

Método estadístico: Coeficiente de correlación de Spearman

Coeficiente de correlación: -0.518

Nivel de Significancia: $\alpha = 0.05$

Resultado nivel de significancia: 0.023

Decisión: El coeficiente de correlación indica que existe una correlación negativa significativa. Además la magnitud de significancia es menor a 0.05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Conclusión: La implantación de la NTP 27001:2008 EDI tiene relación con la integridad de la información en los Ministerios del Estado peruano.

Sub Hipótesis 3

Tabla N° 6.4

COEFICIENTE DE CORRELACIÓN DE SPEARMAN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA DISPONIBILIDAD DE LA INFORMACIÓN

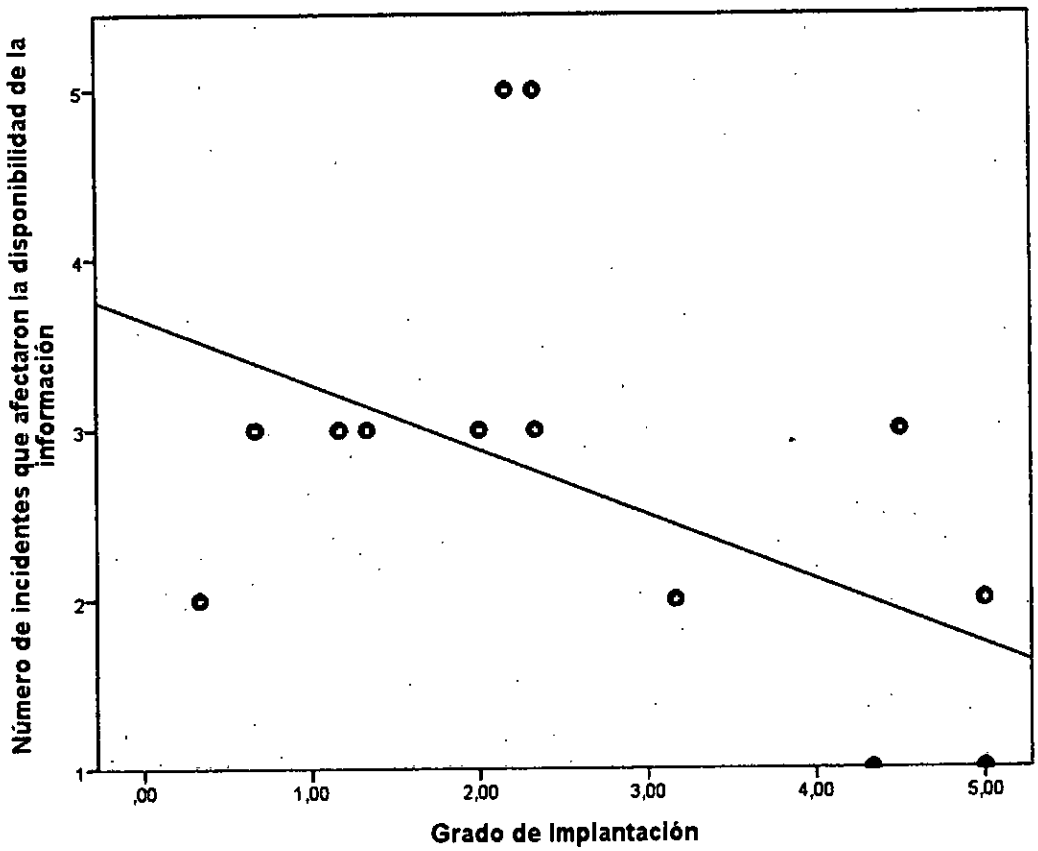
			Grado de Implantación	Número de incidentes que afectaron la disponibilidad de la información
Rho de Spearman	Grado de Implantación	Coeficiente de correlación	1,000	-,574*
		Sig. (bilateral)	.	,010
		N	19	19
	Número de incidentes que afectaron la disponibilidad de la información	Coeficiente de correlación	-,574*	1,000
		Sig. (bilateral)	,010	.
		N	19	19

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia

Gráfico N° 6.3

DISPERSIÓN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA DISPONIBILIDAD DE LA INFORMACIÓN



Contrastación de Hipótesis N° 3

ND0: No existe relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano.

ND1: Existe relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano.

Método estadístico: Coeficiente de correlación de Spearman

Coeficiente de correlación: -0.574

Nivel de Significancia: $\alpha = 0.05$

Resultado nivel de significancia: 0.010

Decisión: El coeficiente de correlación indica que existe una correlación negativa significativa. Además la magnitud de significancia es menor a 0.05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Conclusión: La implantación de la NTP 27001:2008 EDI tiene relación con la disponibilidad de la información en los Ministerios del Estado peruano.

Hipótesis General

Tabla N° 6.5

COEFICIENTE DE CORRELACIÓN DE SPEARMAN ENTRE EL GRADO DE IMPLANTACIÓN Y EL NÚMERO DE INCIDENTES QUE AFECTARON LA SEGURIDAD DE LA INFORMACIÓN

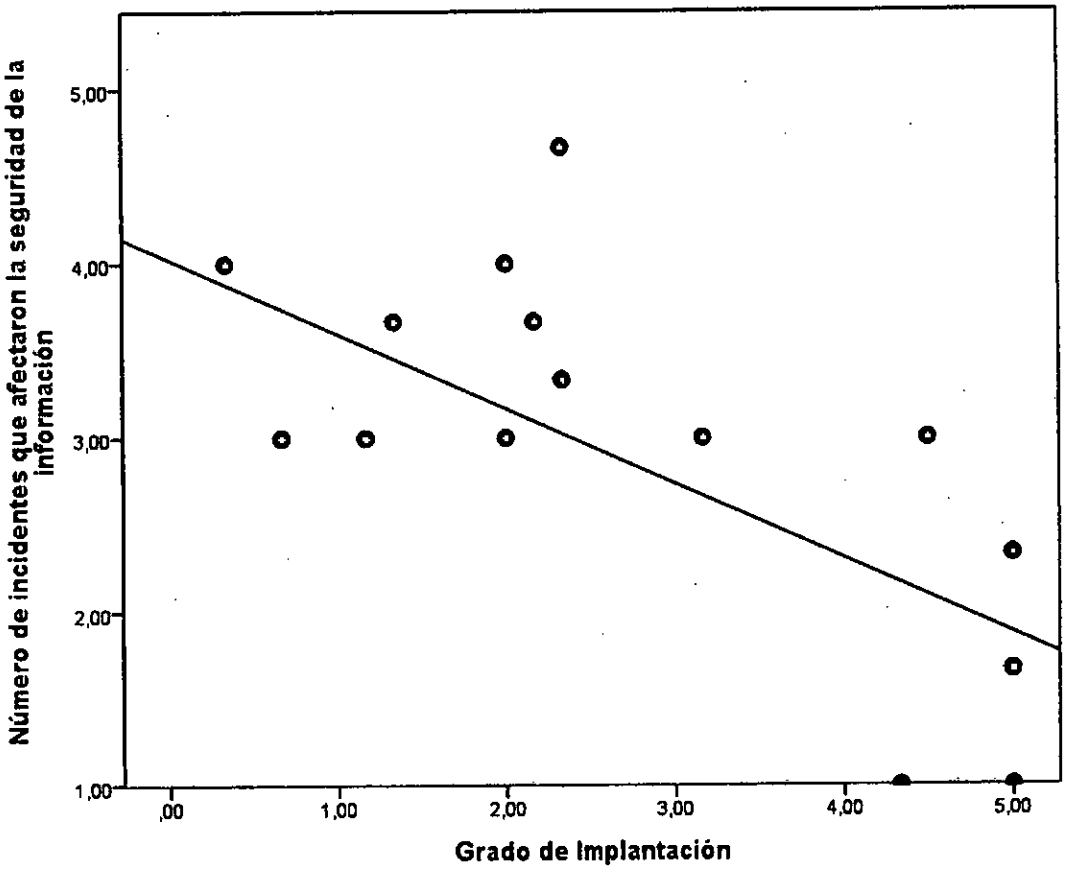
			Grado de Implantación	Número de incidentes que afectaron la Seguridad de la Información
Rho de Spearman	Grado de Implantación	Coeficiente de correlación	1,000	-,636**
		Sig. (bilateral)	.	,003
		N	19	19
	Número de incidentes que afectaron la Seguridad de la Información	Coeficiente de correlación	-,636**	1,000
		Sig. (bilateral)	,003	.
		N	19	19

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

Gráfico N° VI.4

DISPERSIÓN ENTRE IMPLANTACIÓN Y LA SEGURIDAD DE LA INFORMACIÓN



Contrastación de la Hipótesis General

H0: No existe relación entre la implantación de la NTP 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado peruano.

H1: Existe relación entre la implantación de la NTP 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado peruano

Método estadístico: Coeficiente de correlación de Spearman

Coeficiente de correlación: -0.636

Nivel de Significancia: $\alpha = 0.05$

Resultado nivel de significancia: 0.003

Decisión: El coeficiente de correlación indica que existe una correlación negativa significativa. Además la magnitud de significancia es menor a 0.05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Conclusión: La implantación de la NTP 27001:2008 EDI tiene relación con la seguridad de la información en los Ministerios del Estado peruano.

CAPÍTULO VII
CONCLUSIONES

a. 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 al 2015.

b. 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.

c. 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.

d. 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.

CAPÍTULO VIII
RECOMENDACIONES

a. Que la Oficina Nacional de Gobierno Electrónico (ONGEI) adecue el plan de implementación de la NTP-ISO/IEC 27001:2008 EDI a la reciente NTP-ISO/IEC 27001:2014 EDI.

b. Que se concluya el proceso de implantación del Sistema de Gestión de Seguridad de la Información basados en la NTP 27001:2014 EDI en todas las entidades públicas para mejorar la Seguridad de la información del Estado Peruano.

c. Que se realicen el seguimiento de la implantación a través de los Órganos de Control Institucional que existen en cada institución del Estado.

CAPÍTULO IX
REFERENCIAS BIBLIOGRÁFICAS

Aguirre Mollehuaca, D. A. (2014). *Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales Del Perú.* Lima: Pontificia Universidad Catolica del Perú.

Alexander, A. (2007). *Diseño de un Sistema de Gestion de Seguridad de Información.* Bogota Colombia: Alfaomega Colombiana.

Calizaya de la Sota, N. D. (2012). *Metodología de Auditoria Gubernamental para Revision del Cumplimiento de la Normativa Peruana por la SBS relacionada a Seguridad de la Información.* Lima: Universidad Tecnica del perú UTP.

Carrasco Díaz, S. (2005). *Metodología de la Investigación Científica.* lima: San Marcos.

Chávez Bravo, 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 Tecnologica del Perú.

CODESI. (2011, Octubre 28). *Plan de Desarrollo de la Sociedad de la Informacion en el Perú. la Agenda Digtal 2.0.* Retrieved from http://www.codesi.gob.pe/docs/AgendaDigital20_28octubre_2011.pdf

Departamento de Seguridad Nacional. (2013). *Estrategia de Ciberseguriad Nacional España.* Retrieved from www.dsn.gob.es/es/file/146/download?token=KI839vHG

Hernandez, R., Fernandez, C., & Baptista, M. d. (2010). *Metodología de la Investigación.* México: McGraw-Hill.

Huamán Monzón, F. M. (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 Catolica del Perú.

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

INDECOPI, C. d. (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.

Lopez Neira, A., & Javier, R. S. (2015, Junio 14). *iso 27000.es*. Retrieved from http://iso27000.es/

Mexico, S. d. (2014, Mayo 08). *Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de seguridad de la información.* Retrieved from www.dof.gob.mx/nota_to_doc.php?codnota=5343880

Presidencia del Estado Español. (2010, Enero 29). *Esquema Nacional de Seguridad.* Retrieved from https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

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

ANEXOS

Encuesta de Implantación de la NTP-ISO/IEC 27001:2008 EDI

Estimado profesional, el presente tiene por objetivo recoger información acerca del avance de la implantación de la NTP-ISO/IEC 27001:2008 EDI a nivel del Estado Peruano a Agosto de 2015.

Entidad:

.....

.....

Ninguna (1) **1 (2)** **2 (3)** **3 (4)** **Más de 3 (5)**

	Pregunta	1	2	3	4	5
1	¿Cuál es el número de reuniones que ha habido entre el comité SGSI y la Alta Dirección?					

	Pregunta	SI	NO
1	Se ha elaborado el Documento del Alcance del SGSI		
2	Se ha elaborado el Documento de Política de SGSI		
3	Se ha elaborado el Documento de Criterios de evaluación y aceptación de riesgos		
4	Se ha elaborado el Documento de Evaluación de riesgo		
5	Se ha elaborado el Documento de plan de tratamiento de riesgo		
6	Se ha elaborado el Documento de Criterios de evaluación y aceptación de riesgos		
7	Se ha elaborado el Documento de Declaración de Aplicabilidad		

8	Se ha elaborado el Documento Plan de Trabajo		
9	Se implementaron controles de seguridad		
10	¿Se cuenta con registros que evidencien el Monitoreo de desempeño del SGSI?		
11	¿Se cuenta con registros de la mejora de la Gestión de incidentes?		
12	¿Se realizaron auditorías al SGSI?		
13	¿Se implementaron Acciones correctivas a las observaciones encontradas en las auditorias?		
14	¿Se implementaron Acciones preventivas?		

Ninguna (1) Entre 1 y 5 (2) Entre 6 y 10 (3) Entre 11 y 20 (4) Más de 21 (5)

	Pregunta	1	2	3	4	5
1	¿Cuál es el número de incidentes que afectaron la **confidencialidad** de la información entre julio 2012 a agosto 2015?					
2	¿Cuál es el número de incidentes que afectaron la **Integridad** de la información entre julio 2012 a agosto 2015?					
3	¿Cuál es el número de incidentes que afectaron la **disponibilidad** de la información entre julio 2012 a agosto 2015?					

MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	HIPÓTESIS	OPERACIONALIZACIÓN DE VARIABLES			METODOLOGÍA
			VARIABLES	DIMENSIÓN	INDICADORES	
General: **PA:** ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la seguridad de la información en las Ministerios del Estado peruano al 2015?	**General:** **OA:** Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la Seguridad de la Información en los Ministerios del Estado Peruano al 2015	**General:** **HA:** Existe relación entre implantación de la NTP 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado peruano.	Norma Técnica Peruana 27001:2008 EDI	Organización	– Alcance – Política y Objetivos – Criterios de riesgo	**Tipo de investigación:** Aplicada. **Diseño de estudio:** Correlacionada. **Población:** 18 Ministerios y la presidencia de Consejo de Ministros. **Muestra:** 18 Ministerios y la presidencia de Consejo de Ministros.
				Planificación	– Evaluación de Riesgos – Plan de tratamiento de riesgo – Declaración de aplicabilidad	
				Despliegue	– Plan de trabajo – Documentos y registros – Implementar controles	
				Revisión	– Monitoreo de desempeño – Gestión de incidentes	
				Consolidación	– Auditar – Acciones correctivas – Acciones preventivas	
Específico: **P1:** ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano al 2015? **P2:** ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano al 2015? **P3:** ¿Cuál es la relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano al 2015?	**Específico:** **O1:** Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano al 2015. **O2:** Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano al 2015. **O3:** Determinar la relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano al 2015.	**Específico:** **H1:** Existe relación entre la implantación de la NTP 27001:2008 EDI y la confidencialidad de la información en los Ministerios del Estado peruano. **H2:** Existe relación entre la implantación de la NTP 27001:2008 EDI y la integridad de la información en los Ministerios del Estado peruano. **H3:** Existe relación entre la implantación de la NTP 27001:2008 EDI y la disponibilidad de la información en los Ministerios del Estado peruano.	Seguridad de la Información	Confidencialidad	– Nivel de incidencias	
				Integridad	– Nivel de incidencias	
				Disponibilidad	– Nivel de incidencias	