FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Salsavilca Ramos Juan Carlos

ASESOR:

Dra. Yesenia Vásquez Valencia

LINEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

Lima – Perú

2017

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 07 Fecha : 31-03-2017 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don (a) Salsavilca Ramos Juan Carlos
cuyo título es: "Implementación de la Norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017"

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: 14 (número) Catorce (letras).

Lima, San Juan de Lurigancho 16 de Diciembre del 2017

PRESIDENTE
Mg. Crispin Sanchez Ivan

SECRETARIO
Mg. Rivera Crisostomo Renee

VOCAL
Dra. Vasquez Valencia Yesenia

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado

DEDICATORIA

A mi madre que está presente en todo momento y me apoya constantemente dándome la fortaleza necesaria para salir adelante en todos los proyectos que me propongo.

A mi padre que ya no está presente pero que siempre me inculco buenos valores.

A mi familia en general por ser la que me brinda el apoyo moral para poder terminar los objetivos trazados.

AGRADECIMIENTO

Agradecer a Dios por bendecirme por fortalecerme y emprender el camino hacia el éxito.
Agradecer a mis profesores de la Universidad ya que han aportado mucho en la obtención de mis conocimientos.
A mis hermanos, por apoyarme en las buenas y en las malas y darme siempre buenos concejos para seguir adelante.

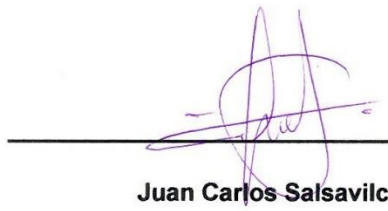
DECLARATORIA DE AUTENTICIDAD

Yo JUAN CARLOS SALSAVILCA RAMOS, con DNI N° 10721292, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad Cesar Vallejo, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y autentica.

Así mismo, declaro también bajo juramento que todos los datos e información que se presenten en la tesis son auténticos y veraces.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en las normas académicas de la Universidad de Cesar Vallejo.

Lima 16 de diciembre Del 2017



Juan Carlos Salsavilca Ramos

DNI N° 10721292

PRESENTACIÓN

Señores miembros del Jurado:

En cumplimiento de las normas establecidas en el reglamento de Grados y Títulos de la Universidad Cesar Vallejo presento ante ustedes la tesis titulada “Implementación de la norma ISO 27001 en la gestión de la seguridad de la información en la empresa Atento del Perú 2017" la misma que someto a vuestra consideración y espero que cumpla con todos los requisitos de aprobación para obtener el título profesional de Ingeniero de Sistemas.

Esta investigación tuvo como objetivo determinar el impacto de la implementación en la gestión de la seguridad de la información en la empresa Atento del Perú 2017, la cual consta de siete capítulos, el capítulo I planteó la introducción describiendo la realidad problemática trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y los objetivos, el capítulo II describió y explicó el diseño de investigación, las variables de estudio y su operacionalización. También se detalla la población, la muestra y las técnicas e instrumentos para procesamiento de la información, la validación y confiabilidad del instrumento, los métodos de análisis de los datos y aspectos éticos de la investigación, el capítulo III se refirió a lo obtenido de la investigación así como a la comprobación de las hipótesis, en el capítulo IV se presentaron y se discutieron los resultados de la investigación, en el capítulo V se presentaron las conclusiones, en el capítulo VI se presentaron las recomendaciones, en el capítulo VII se detallan las referencias bibliográficas utilizadas y finalmente se completaron con los anexos.

Esperamos señores miembros del jurado que la investigación realizada se ajuste a los requerimientos establecidos y que el trabajo realizado de origen a posteriores estudios.

Salsavilca Ramos Juan Carlos

ÍNDICE DE CONTENIDO

PÁGINAS PRELIMINARES

Página del Jurado ii
Dedicatoria iii
Agradecimiento iv
Declaratoria de autenticidad v
Presentación vi
Índice vii
RESUMEN xii
ABSTRACT xiii

I. INTRODUCCIÒN 14
1.1 Realidad Problemática 15
1.2 Trabajos Previos 17
1.3 Teorías Relacionadas Al Tema 19
1.4 formulación del problema 35
1.5 Justificación del estudio 35
1.6 Hipótesis 37
1.7 Objetivos 38

II. MÉTODO 39
2.1 Diseño de Investigación 40
2.2 Variables, operacionalización 41
2.3 Población y muestra 43
2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad 44
2.5 Métodos de análisis de datos –Aspectos éticos 45

III. RESULTADOS 47
3.1 Análisis Descriptivo 50
3.2 Análisis Inferencial 50
3.3 Prueba De Hipótesis 57

IV. DISCUSIÓN 63

V. CONCLUSIÓN 66
VI. RECOMENDACIONES 68
VII. REFERENCIAS 70
VIII. ANEXOS **73**

ÍNDICE DE TABLAS

Tabla 1: Determinación del valor de Degradación 28

Tabla 2: Determinación del valor del Impacto 28

Tabla 3: Determinación del valor de la Probabilidad 29

Tabla 4: Determinación del Riesgo 30

Tabla 5: Criterio de aceptación del riesgo 30

Tabla 6: Evaluación del Riesgo 31

Tabla 7: Evaluación del Riesgo 32

Tabla 8: Resultado de evaluación de Riesgo 32

Tabla 9: Plan de Tratamiento del Riesgo 33

Tabla 10: Variable Dependiente 42

Tabla 11 Análisis descriptivo SPSS indicador 1 47

Tabla 12 Análisis descriptivo SPSS indicador 2 48

Tabla 13 Análisis descriptivo SPSS indicador 3 49

Tabla 14: Pruebas de normalidad indicador 1 51

Tabla 15: Pruebas de normalidad indicador 2 53

Tabla 16: Pruebas de normalidad indicador 3 55

Tabla 17: Pruebas de Wilcoxon indicador 1 58

Tabla 18: Pruebas de Wilcoxon indicador 2 60

Tabla 19: Pruebas de Wilcoxon indicador 3 62

Tabla 20: Actividades de la Implementación del SGSI 84

Tabla 21 – 25 Declaración de Aplicabilidad (SOA) 85

Tabla 26 Valoración Cualitativa de los Activos 92

Tabla 27 Escala porcentual del impacto 93

Tabla 29 Pre y Post de Incidencias 101

Tabla 30 Detalle Económico de las pérdidas antes de la implementación 101

ÍNDICE DE FIGURAS

Figura 1 Promedio de Nivel de información que puede ser divulgada sin autorización Indicador 1 48

Figura 2 Promedio de Nivel de información que puede ser modificada sin autorización Indicador 2 49

Figura 3 Promedio de Nivel de información cuya inaccesibilidad es frecuente Indicador 3 50

Figura 04 Histograma del Nivel de información que puede ser divulgada sin autorización pre test 52

Figura 05 Histograma del Nivel de información que puede ser divulgada sin autorización post test 52

Figura 06 Histograma del Nivel de información que puede ser modificada sin autorización pre test 54

Figura 07 Histograma del Nivel de información que puede ser modificada sin autorización post test 54

Figura 08 Histograma del Nivel de información cuya inaccesibilidad es frecuente pre test 56

Figura 09 Histograma del Nivel de información cuya inaccesibilidad es frecuente post test 56

Figura 10 Planificación Del Proyecto 86

ÍNDICE DE ANEXOS

Anexo 1 Matriz de Consistencia 74

Anexo 2 Ficha de observación confidencialidad 75

Anexo 3 Ficha de observación integridad 76

Anexo 4 Ficha de observación disponibilidad 77

Anexo 5 Planteamiento del problema, objetivo, hipótesis 78

Anexo 6 Instrumento registro de observación 79

Anexo 7 Instrumento registro de observación 80

Anexo 8 Instrumento registro de observación 81

Anexo 9 Implementación del sistema de gestión de la seguridad de la información según ISO 27001 95

Anexo 10 Plan De Auditoria Interna (SGSI) Según Norma ISO 27001 96

Anexo 11 Plan De Auditoria Interna (SGSI) Gestión de Riesgos 108

Anexo 12 Plan De Auditoria Interna (SGSI) Control de Accesos 109

Anexo 13 Plan De Auditoria Interna (SGSI) Seguridad Física y ambiental 110

Anexo 14 Formato De Entrega De Usuarios Aplicativos 111

Anexo 15 Formato De Requerimiento 112

Anexo 16: Acciones Correctivas Y Preventivas 113

RESUMEN

El fin de realizar la investigación fue de implementar la norma ISO 27001 en la gestión de la seguridad de la información en la empresa Atento del Perú utilizando la metodología del Circulo de Deming(de Edwars Deming) o modelo continuo PDCA es una táctica de la mejora permanente de la calidad, alineados a norma ISO 27001:2014 ya que la información que es un activo primordial para la viabilidad de la empresa en sus diferentes formas, tanto software, hardware u otros medios para la transmisión y difusión en la organización debido a que existieron amenazas que pusieron en riesgo su continuidad, haciendo referencia en seguridad de la Información se define como resguardar la misma de los constantes ataques que puedan sufrir, el trabajo realizado buscó facilitar un adecuado nivel de control de riesgos que haya permitido evitar o disminuir las falencias en los sistemas, redes y todo el patrimonio de ataques o desastres que se puedan presentar.

En términos generales luego de la implementación de la Norma ISO 27001 los resultados fueron óptimos en la confidencialidad, integridad y disponibilidad ya que en sus indicadores como el nivel de información que puede ser divulgada sin autorización, el nivel de información que puede ser modificada sin autorización y el nivel de información cuya inaccesibilidad es frecuente se logró un resultado de 92.23%, 97.42% y 90,95% respectivamente lo cual demostró aumento de controles y aumento de seguridad.

En conclusión, implementar la norma ISO 27001 minimizó considerablemente los riesgos asociados a la información logrando un nivel de confianza y seguridad en sus activos

Palabra clave: NORMA ISO 27001 - GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN- ESTRATEGIA EN MEJORA CONTINUA DE LA CALIDAD ALINEADA.

ABSTRACT

The purpose of conducting the investigation was to implement the ISO 27001 standard in the management of information security in the Atento del Perú company using the methodology of the Deming Circle (from Edwars Deming) or PDCA continuous model is a tactic of improvement permanent quality, aligned to ISO 27001: 2014 as the information that is a primary asset for the viability of the company in its different forms, both software, hardware or other means for transmission and dissemination in the organization because There were threats that put their continuity at risk, referring to information security is defined as protecting it from the constant attacks that they may suffer, the work carried out sought to facilitate an adequate level of risk control that has allowed to avoid or reduce the shortcomings in the systems, networks and all the heritage of attacks or disasters that may arise.

In general terms after the implementation of ISO 27001, the results were optimal in the confidentiality, integrity and availability since in its indicators as the level of information that can be known without authorization, the level of information that can be modified without authorization and the level of information whose inaccessibility is frequent resulted in 92.23%, 97.42% and 90.95% respectively, which showed an increase in controls and an increase in security.

In conclusion, implementing ISO 27001 minimized the risks associated with information considerably, achieving a level of confidence and security in its assets.

Keyword: ISO 27001 STANDARD - INFORMATION SECURITY MANAGEMENT - STRATEGY ON CONTINUOUS IMPROVEMENT OF ALIGNED QUALITY.

I. INTRODUCCIÒN

1.1 REALIDAD PROBLEMÁTICA

Atento con sede Perú ubicada en Ate con dirección Av. la Molina 190 fue constituida en setiembre del año 1999 y desde entonces ha ido creciendo hasta 11 mil asesores. Consiste en brindar servicios de contact center post venta en telecomunicaciones. ATENTO en la Gerencia de Soporte técnico, específicamente en la Jefatura de soporte y tratamiento en línea de internet cable tv y telefonía Voip con la empresa TELEFÓNICA DEL PERÚ con firma comercial MOVISTAR, la empresa contaba con una amplia gama de equipos de hardware y software en la cual se corrió el riesgo de sufrir ataques informáticos, así como también el robo de información el cual es el principal activo de la empresa ya que cuenta con la data de muchos de sus clientes que han contratado sus servicio pos venta. Disponible en http://atento.com/es/donde-estamos/peru/ Revisado 2071172017.

Atento contaba con amplia información de los clientes que contrataban un servicio con Movistar en la cual ponía a disposición de todos los trabajadores que tienen contacto con el cliente final para la gestión diaria cuando recibíamos llamadas a través del número telefónico 104 en sus diversas consultas comerciales o técnicas referentes a cable, teléfono e internet así como para otros nuevos servicios innovadores propuestos como la redes sociales que tiene cada vez más acercamiento y de fácil acceso a nuestras áreas de atención.

Para esta gestión y como causa principal de la problemática, la masificación de la tecnología generaba que sus empleados utilicen diferentes medios periféricos que se conectan y trabajan desde cualquier equipo informático, estas modalidades se volvieron muy constantes y sobre todo vulnerables para los cibercriminales que a través de estos dispositivos tenían más posibilidades de robar información confidencial, instalar aplicaciones no permitidas, modificar las configuraciones del sistema, instalar virus y como consecuencia generaba daño a nivel software y hardware y también toda la información de los clientes y es por ello la importancia de proteger estos

medios informáticos ya que la información es manipulada constantemente y esto causa perdida económica y sobre todo que puede generar mala reputación en la empresa.

Se habían detectado carencias puntuales en la cual se permitió sustraer información importante por personas ajenas a la empresa y esto dejó en alto riesgo su activo principal. El área no contaba con una buena dirección para detectar y minimizar los riesgos en la información, no tenían procedimientos estandarizados y esto iba afectando más a la empresa por no tener métodos establecidos.

La empresa no contaba con políticas específicas y requería un cambio en su método de seguridad en información alineado a ISO.

Se había detectado que los trabajadores del área implementada utilizaban sus celulares y memorias USB conectándolos a las computadoras, también se detectaron que ingresaban a páginas que tienen alto riesgo de virus logrando que los equipos se infectaran de virus ocasionando problemas serios en el funcionamiento de los aplicativos instalados en las computadoras, problemas de suplantación de identidad, robo de datos confidenciales, robos de copias de seguridad entre otros, esto generaba crisis empresarial y daña la imagen y por esta razón tenía como finalidad primordial proteger, mejorar, atenuar amenazas y todo lo necesario para tener mayor control y seguridad en la empresa, de ahí la importancia de buscar métodos para mejorar su gestión con procesos de alta calidad.

1.2 TRABAJOS PREVIOS INTERNACIONALES

Análisis en seguridad Informática y Seguridad de la Información Basado en la norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros. KELLY GABRIELA BERMÚDES MOLINA. Guayaquil-Ecuador. 2015. El objetivo fue el análisis del método de la empresa sobre su seguridad basado en la disponibilidad, confidencialidad e integridad usando ISO /IEC 27001. La metodología implementada fue Magerit. Se concluyó que mediante esta metodología se detectaron potenciales amenazas que exponen los datos en el cual dañan los activos de información.

Diseño de un Sistema de Gestión de la Información para Comercio Electrónico basado en la ISO 27001 para pequeñas empresas y medianas empresas en la ciudad de quito. ANGEL PATRICIO SÁNCHEZ SOLÁ. Quito – Ecuador, 2013. El objetivo fue desarrollar un método sobre la seguridad en comercio electrónico cual contenga las principales políticas de seguridad de una Pyme de la ciudad en Quito. La metodología fue la norma ISO27001. Se concluyó que al implementar la norma permitió salvaguardar la información en la empresa de posibles amenazas y riesgos.

Modelo de Gestión de Seguridad de la Información para la Universidad de Loja basado en la norma ISO/IEC 27001.María Gabriela Pardo Cuenca. Loja-Ecuador, 2015. El objetivo fue brindar seguridad en los activos con referencia a la información controlada desde nuestra torre principal, la metodología empleada fue MAGERIT v3. Concluye que ISO/IEC 27001 permitió superar los inconvenientes propios de su desarrollo en toda la universidad.

NACIONALES

Implementación de un sistema de Gestión en Seguridad de la Información, aplicado a los Riesgos Asociados a los Activos de Información en la Empresa NET Consultores S.A.C. ADRIÁN GARCÍA PAREDES. SAN MARTIN, Perú, 2016. El proyecto titulación tuvo como objetivo diseñar un SGSI ISO 27001 capaz de resguardar la información y ponerla libre de peligros en nuestra sede. La muestra se realizó a 142 personas que son el total de la población. La metodología aplicada fue ciclo PDCA. Concluyó que cumplió con el objetivo solicitado y se determinó que si impacta en el modelo empleado.

Diseño de un Sistema de Gestión de Seguridad de la Información en la Compañía de Seguros. Ampuero Chang, Carlos Enrique, Lima, Perú, 2011. El proyecto tuvo como objetivo diseñar un SGSI alineado por NTP ISO /IEC 27001 de Seguridad de la Información para mitigar las distintas modalidades de ataques informáticos que sufrieron las compañías aseguradoras debido a que cuenta con abundante información de los clientes. La metodología empleada era Magerit II. Se concluyó que es importante contar con un SGSI para lograr un nivel óptimo en todos sus procesos en la compañía de seguros peruanos enfocado en todas sus necesidades para hacerlo más óptimo.

Diseño de un SGSI para servicios portales del Perú S.A. Aguirre Mollehuanca David. Lima, 2014. El proyecto de titulación tuvo como objetivo diseñar un SGSI según lo indicado por la NTP ISO/IEC 27001:2008 y NTP-17999:2007 de seguridad de la información lo cual se detectó mucha deficiencia en su seguridad, además de peligros que podrían afectar la continuidad del negocio. La metodología empleada fue el ciclo PDCA muy conocido, esta tesis concluyó en que existe la necesidad de modificar lo gestionado actualmente a sus procesos SGSI para minimizar el riesgo de sus activos, y que es necesario mejorar las comunicaciones en todas sus áreas dentro de la empresa.

1.3 TEORÍAS RELACIONADAS AL TEMA

La información siempre fue amenazada ya que estaban expuestas a distintas amenazas informáticas, la seguridad con referencia en información es parte de la seguridad corporativa y por lo tanto tiene que estar alineado a las políticas de seguridad corporativa. Poner en práctica un SGSI basado en ISO 27001 puede considerarse como el inicio de la mejora continua del SGSI en cuestión, y como este se gestiona mediante un modelo PDCA, existe una relación entre ambas partes en la cual lleva a una transformación para su mejora. Merino y Cañizares,2011, p92).

CONCEPTO SGSI

En referencia a un SGSI, se define información al conjunto de datos recopilados por una organización cual le da un valor importante, ya sea impresa, escrita, oral en sus distintas formas para ser usadas según sus necesidades.

Importancia de la Gestión de Riesgos de Seguridad de la Información en la Empresa Atento del Perú

Es importante debido que redujo los riesgos en los datos de la empresa, así como garantizar a través de sus dimensiones ya mencionadas la información en la empresa. El método fue uno de los más importantes aciertos de la dirección que se tomó y fue fijar el umbral de riesgo que la dirección está dispuesta a asumir. Los riesgos pueden clasificarse en Aceptable, Tolerable, Inaceptable, una vez definido los umbralas este fue tratado según cada caso y tomado los planes de acción a las medidas oportunas en los plazos establecidos (Merino y Cañizares, 2011, p131).

Seguridad de la Información

Confidencialidad: No se revela datos a la persona no autorizada.
Integridad: mantenimiento de la exactitud y completitud de la Información y sus métodos de proceso.
Disponibilidad: acceso y tratamiento si es requerido.

Información que puede ser divulgada sin autorización: Información que es utilizada por cualquier persona no autorizada cuya divulgación ocasione perdida para la empresa.

Información que puede ser modificada sin autorización: Información que es utilizada sin autorización pierde integridad al realizarse cambios ya sea parcial o total en los sistemas.

Información cuya inaccesibilidad es frecuente: Información no disponible para sus usuarios autorizados por pérdida o destrucción que afecta la operatividad de la empresa.

Disponible en:
(http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu..ar/files/site/material_taller_gestion_de_riesgo.pdf).

Organismos responsables de la estandarización

"La Comisión Electrotécnica Internacional (IEC) es el ente responsable en elaborar normas de electrotecnia y electrónica, así como, la Organización Internacional de Normalización (ISO) tiene la responsabilidad especializada en la estandarización". (Gómez, 2011, 147).

Proceso de Certificación

"La certificación es el esfuerzo obtenido al método bien empleado, una garantía de "calidad de la seguridad", que beneficia a la organización y le da mucho más valor y prestigio. Pero hay que mencionar que esto no necesariamente garantiza la seguridad a los problemas de seguridad que es en forma variada, pero que, si logra reducir el riesgo y conviene recordar una vez más que la seguridad en su totalidad no existe". (Gómez, 2011, 169).

Familia ISO/IEC 27000

"ISO/27000 es un estándar relacionado con los Sistemas de Gestión que se enfocan en temas puntuales, cuyos rangos de numeración van del 27000 al 27019 y también del 27030 al 27044, fue publicado en el año 2009 y proporciona una visión general de toda la serie 27000 con los términos y definiciones básicas ya conocidas". (Gómez, 2011, 159).

Estándar Internacional ISO/IEC 27001

"Tuvo como publicación en mes octubre de 2005, diseñando los requisitos para un SGSI. Se trata de la Norma principal de esta serie, que tiene su origen en la anterior BS 7799-2:2002". (Gómez, 2011, 160).

Estándar Internacional COBIT

"El estándar COBIT (Control Objetives for Information and releated Technology) brinda un modelo de "mejores prácticas" y están enfocadas en el control que en la realización de metodos". Disponible en: (http://www.aec.es/web/guest/centro-conocimiento/cobit).

ITIL DEFINICIÓN

ITIL (Information Technology Infraestructure Library), tiene como referencia a las mejores prácticas en la industria de TI. Consta de un conjunto de libros en los cuales se encuentran documentos referentes a procesos de servicios de tecnologías de información destinadas a empresas. Es una Biblioteca de Tecnologías de información que fue creada a fines de los 1980 y desde ahí es un referente internacional de la Gestión de Servicios. Disponible en http://infoitilv3.weebly.com/

Fases del ciclo PDCA en el caso de un Sistema de Gestión de Seguridad de información.

"Estas son las etapas que se cumplen en el ciclo PDCA". (Merino y Cañizares, 2011, p 38).

PLAN

- Diseño del plan de gestión de riesgos que detecte amenazas.

DO

- Realización de la implantación diseñada
- Cambios en sus estatutos como políticas y otros.
- Toma de conciencia y capacitación.

CHECK

- Revisar los controles implantados en eficacia y eficiencia.
- Revisión constante en sus indicadores.
- Revisión del funcionamiento de acuerdo a SGSI.

ACT

- . Acciones preventivas para el funcionamiento en sus sistemas
- . Acciones para la mejora.

Fases y actividades en las que se organiza un SGSI según el estándar ISO 27001

Las fases en las que se organiza la implantación de SGSI según el estándar 27001. (Merino y Cañizares, 2011, p90).

FASE I

- Planificación del proyecto
- Análisis de situación respecto de la norma (GAP ANALISIS)
- Definición de la sociedad de la seguridad de la información

FASE II

- Revisión de los riesgos
- Proceso de los riesgos
- Realizar plan de acción

FASE III

- Buscar métodos para la comunicación y capacitación.
- Evaluación del control operativo
- Elaboración de los indicadores de gestión
- Aplicar todo lo diseñado.

FASE IV

- Indicadores
- Auditoria interna

FASE V

- Corregir y modificar el sistema de gestión.

Plan para el análisis y gestión de Riesgos de los procesos en la información (MAGERIT).

. El equipo asignado de la etapa evaluadora debe de contar con toda la experiencia previa, así como tener disponible los recursos necesarios para su realización, con el soporte y consentimiento de la dirección. (Gómez, 2011, p59).

Inventario de Activos de Información

Todo inventario debe incluir, al menos, la información necesaria para poder recuperarnos ante un desastre, debe ser claro y permitir localizar físicamente en todo momento cualquier activo, incluso en situaciones de contingencia. Se deberá documentar en el inventario el valor del activo, su clasificación de seguridad, importancia o criticidad. Además de una breve descripción de código, identificador de red, usuario, fecha, de adquisición, fecha de baja. (Merino y Cañizares, 2011, p105).

Análisis del Riesgo

Llegado a este punto, hemos identificado los activos y a sus propiedades, hemos identificado las amenazas las vulnerabilidades hemos calculado el impacto en sus Dimensiones que pueden tener en los activos. Todas estas tareas se han realizado en base a la metodología definida y alineada con el negocio en cuanto a políticas, directivas y estrategias de negocio. (Merino y Cañizares, 2011, p120).

Identificación de Activos

Consiste en identificar todos los activos que se encuentran dentro y fuera de la empresa por lo que este proceso es muy importante ya que si no conocemos lo que tenemos no conoceremos el verdadero riesgo al que se expondrá. Adicionalmente se refiere a elementos que son tangibles como intangibles y que tienen alto valor en el negocio, estos pueden ser hardware, software, documentos, base de datos, informes, procesos, productos, infraestructura tecnológica, personas y cualquier elemento que la empresa decida protegerse. (Merino y Cañizares, 2011, p 104)

Identificación de amenazas

Las amenazas pueden ser de diversos tipos o diversas clases, y se pueden clasificar inicialmente en base a su origen: amenazas internas, externas, intencionadas o no. No necesariamente las amenazas o riesgos afectan a los activos, ya que hay una cierta relación entre el tipo de activo y las consecuencias que se pueden derivar. (Merino y Cañizares, 2011, p107).

A través de la metodología Magerit 2.0 menciona algunas amenazas existentes, tales como desastres naturales, de origen industrial, perdida energía eléctrica, temperaturas no adecuadas en la zona, proliferación de programas que ponen en peligro, escape de información, vulnerabilidades de las aplicaciones, caída de sistemas, ataques malintencionados, manipulación de la configuración, adulteración de identidades, acceso no autorizado y otros similares (Merino y Cañizares, 2011, p116)

Identificación de Vulnerabilidades

Es necesario conocer las vulnerabilidades que podrían ser tomadas por las amenazas identificadas en la tarea anterior. Cuando hablamos de vulnerabilidades no nos referimos sólo a aquellas que afectan a los sistemas, existen vulnerabilidades que afectan a otros recursos como a las infraestructuras, al personal, etc. Como ocurre con las amenazas, debemos disponer de un listado de vulnerabilidades a las que estamos expuestos para las amenazas que hemos identificado en su momento. (Merino y Cañizares, 2011, p118)

Determinación del valor de Degradación

Es el nivel en el cual se afecta un activo de información cuando una vulnerabilidad es explotada por las amenazas.

Tabla 1: Determinación del valor de Degradación

Escala	Valor de Importancia	Descripción
1	MUY BAJO	Nivel de degradación del activo es muy bajo
2	BAJO	Nivel de degradación del activo es bajo
3	MEDIO	Nivel de degradación del activo es medio
4	ALTO	Nivel de degradación del activo es alto
5	MUY ALTO	Nivel de degradación del activo es muy alto

Determinación del valor del Impacto

Se debe tener en cuenta tanto los daños tangibles como la proyección de las perdidas intangibles, ya que es de apoyo hacia los responsables de cada área, buscando determinar el impacto o perdida de la información en la organización. (Gómez, 2011, p 62).

Tabla 2: Determinación del valor del Impacto

Escala	Valor del Impacto	Significado
1 - 1.4	1	MUY BAJO
1.5 – 2.4	2	BAJO
2.5 – 3.4	3	MEDIO
3.5 – 4.4	4	ALTO
4.5 - 5	5	MUY ALTO

Determinación del valor de la Probabilidad

"Cuál es la posibilidad que se manifieste la amenaza". (Magerit, 2012, p 28).

Tabla 3: Determinación del valor de la Probabilidad

Escala	Valor de Importancia	Descripción
1	MUY BAJO	Nivel de degradación del activo es muy bajo
2	BAJO	Nivel de degradación del activo es bajo
3	MEDIO	Nivel de degradación del activo es medio
4	ALTO	Nivel de degradación del activo es alto
5	MUY ALTO	Nivel de degradación del activo es muy alto

Determinación del Riesgo

Viene ser el posible perjuicio de al sistema. Identificando el impacto de amenazas respecto a los activos es necesario aislar el riesgo. Ello aumenta debido a la existencia del impacto y la probabilidad. (Magerit, 2012, p 29).

Riesgo= (Impacto + Probabilidad) / 2

Tabla 4: Determinación del Riesgo

MATRIZ RIESGO			IMPACTO				
			MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
			1	2	3	4	5
PROBABILIDAD	MUY BAJO	1					
	BAJO	2					
	MEDIO	3					
	ALTO	4					
	MUY ALTO	5					

Criterio de aceptación del riesgo

Tabla 5: Criterio de aceptación del riesgo

Escala	**Valor del Riesgo**	**Significado**
1	MUY BAJO	Es aceptable cuando el activo se expone a riesgos leves
2	BAJO	
3	MEDIO	
4	ALTO	Es cuando se encuentra expuesto a riesgos altos y se requiere ser tratado.
5	MUY ALTO	

Evaluando el Riesgo

Para este cuadro se observa cuáles son los criterios a tomar en cuenta.

Tabla 6: Evaluación del Riesgo

CRITERIOS	DETALLE
ECONÓMICO	Si el costo de la amenaza es mayor al costo de la implementación de software y hardware.
CONTINUIDAD	Si la amenaza detiene la gestión operativa en el área.
LEGAL	Si la amenaza ocasiona que se genere denuncia por parte del usuario final o cliente contratante.
IMAGEN	Si la amenaza ocasiona que la imagen de nuestra área institucional se vea afectada.
CONTRACTUAL	Si la amenaza ocasiona incumplimiento de contrato con nuestro cliente.

Tabla 7: Evaluación del Riesgo

Análisis de Riesgo			**Evaluación del Riesgo**				
Activo	Amenaza	Riesgo	Económico	Continuidad	Legal	Imagen	Contractual
Base 1	Robo	4		x			x
Base 2	Adulteración de activos	5	x		x	X	
reporte	Código malicioso	4				X	

Tabla 8: Resultado de evaluación de Riesgo

Subtotal	total
2	8
3	15
1	4

En la evaluación de riesgo se logra identificar los riesgos que toman mayor relevancia para su control y disminución.

Plan de Tratamiento del Riesgo

Se refiere al modelo de cómo se implementará el presente tratamiento. (Merino y Cañizares, 2011, p166).

Tabla 9: Tratamiento del Riesgo

TRATAMIENTO	DESARROLLO
TRANSFERIR	Se traspasa a un tercero con capacidad para su administración.
EVITAR	Si el presente servicio es un riesgo no asumible, se deja de prestar.
REDUCIR	Se aplican medidas que vayan a disminuir o reducir el impacto.
ACEPTAR	Se acepta el riesgo sin aplicar las medidas correctivas cuando el costo supero es demasiado elevado.

Selección de objetivos de control

Es necesario implementar de tal forma que permitan cumplir los requisitos encontrados en la evaluación de riesgo. Es necesario tomar en cuenta los criterios de aceptación identificados en trabajos anteriores. (Merino y Cañizares, 2011, p135).

Aceptación por la Dirección

Los riesgos que se identifican en la en el proceso no dejan de ser peligros lo cual afectan al negocio y es la dirección la que debe elegir su tratamiento. Por ello antes de la implantación debe de existir documentación de la medida adoptada. (Merino y Cañizares, 2011, p135).

Declaración de Aplicabilidad (SOA)

Consiste en elaborar una declaración de aplicabilidad (Statement Of Applicability – SOA) en la cual es una lista de todos los elementos seleccionados y el motivo de su elección, este control se tomó como base el anexo A de la norma 27001. (Merino y Cañizares, 2011, p135).

1.4 formulación del problema

1.4.1 Problema General

¿Qué resultados tendría gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017?

1.4.2 Problema Específico

¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017?

¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la integridad para la seguridad de la información en la empresa Atento del Perú 2017?

¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017?

1.5 Justificación del estudio

1.5.1 Justificación Institucional.

Comenzando desde la directiva y sus ramificaciones debe garantizar sus buenas prácticas en cada uno de los procesos en los riesgos de la información ya que esto permitió su certificación, en la cual contribuyó al reconocimiento por parte de sus clientes, trabajadores, y demás empresas del mismo rubro.

1.5.2 Justificación tecnológica

Hoy en día los tiempos van cambiando y a la par las amenazas informáticas se van sofisticando cada vez más y es por este motivo que la Empresa Atento del Perú se modernizó implementando la norma ISO 27001 para que interactúe con los cambios tecnológicos. Según la ISO 27001(2005, p7) Organización Mundial de Estandarización, y (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial.

1.5.3 Justificación legal

Los estatutos estratégicos de Atento contemplan dentro de sus normas a la SGSI como parte de su plan de reestructuración. "El hacer cumplir todas las etapas en ATENTO para obtener el mejor rendimiento es la característica principal que se debe tomar en cuenta en los procesos de las organizaciones." Disponible en http://www.iso27000.es/sgsi.html Revisado 20/11/2017

1.5.4 Justificación Económica

Mediante el proceso que se realizó se logró minimizar los costos ocasionados por las pérdidas ocasionadas en la data de sus clientes. Las pérdidas son muy elevadas debido a un mal proceso. (Alexander, 2007).

1.5.5 Justificación Operativa

Debido a los acontecimientos ocurridos en la seguridad de la Información la metodología implementada cumple un rol estratégico e importante logrando minimizar los riesgos asegurando sus activos.

La norma adopta un enfoque basado en procesos para poder mejorar el Sistema. (Alexander, 2007, p132).

1.6 Hipótesis

1.6.1 Hipótesis General

Gestionar en base a la norma ISO 27001 tiene un efecto significativo para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2 Hipótesis Específica

1.6.2.1 Hi: Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2.2 Ho: Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2.3 Hi: Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2.4 Ho: Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2.5 Hi: Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.

1.6.2.6 Ho: Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.

1.7 Objetivos

1.7.1 Objetivo General

Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017.

1.7.2 Objetivos Específicos

Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.

Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.

Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.

ii. MÉTODO

2.1 Diseño de Investigación

El modelo pre experimental menciona que los grupos ya estaban formados antes del experimento y que son grupos intactos, los sujetos no son asignados al azar a los grupos ni emparejados, sino que, han sido identificados con antelación y se ha buscado determinar en ellos un criterio de convivencia con el fin de describir la situación actual y así mismo avizorar las posibilidades de cambiar los elementos. (Ávila Baray, 2006).

Experimental

A través de esta experiencia la manipulación es deliberada de uno o más variables y así poder analizar las consecuencias de esta manipulación. (Rodríguez, 2012).

Se utilizará el sistema de representación universal, como es utilizado por COOK Y Campbell (1979) y Campbell y Stanley (1963).

R: Azar (random)
O: Observación, se toma en cuenta en el pretest o en el postest
X: Tratamiento (los variables 1 a n mencionan diferentes tratamientos)

G: 01 X 02

2.2 Variables, operacionalización.

2.2.1 Definición Conceptual

2.2.1.1 Variable Independiente (VI): Norma ISO 27001

Basado en los riesgos del negocio que establece, monitorizar y mejorar los procesos. Incluye las políticas, las responsabilidades. Por tanto, hace referencia a los esfuerzos sistemáticos y organizados de las organizaciones. (Areito, 2008, p 200)

2.2.1.2 Variable Dependiente (VD): Seguridad de la información

Es el amplio número de elementos de tipo tecnológicos, de recursos humanos, del tipo económico, negocios, legal, de cumplimiento, la cual considera no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales. (Areito, 2008, p. xvi).

2.2.2 Definición Operacional

2.2.2.1 Variable Independiente (VI): Norma ISO 27001

Tiene como escala de medición a la integridad, la confidencialidad y la disponibilidad a la cual es aplicada a la valorización.

2.2.2.2 Variable Dependiente (VD): Seguridad de la información

Contempla procesos adecuados para implementación de controles en la cual se requiere mantener una exposición mucho menor al que la gerencia ha decidido.

2.2.3 Operacionalización de Variables

Tabla 10: Variable Dependiente

Variables	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA
Seguridad de la Información	Es un proceso en el que se da cabida a un amplio número de elementos de tipo tecnológicos, de gestión organizacional, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, abarcando no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales. (Areito, 2008, p. xvi).	Contempla procesos adecuados de planificación e implementación de en la cual el propósito es evitar que la exposición sea mayor al que la gerencia ha detectado.	Confidencialidad	Nivel de información que puede ser divulgada sin autorización	Razón
			Integridad	Nivel de información que puede ser modificada sin autorización	Razón
			Disponibilidad	Nivel de información cuya inaccesibilidad es frecuente	Razón

2.3 Población y muestra

Se define como elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Para ello queda señalado por problema y por los objetivos del estudio. (ARIAS, 2006 PAG 81)

En este proyecto se contó con un total de 20 registros del periodo de 30 días para poder analizar el estado en el cual se encontró el área y cumplir con los objetivos de la implementación encomendados por la empresa.

Muestra

La muestra se aplicó al promedio del total de registros del periodo de 30 días, con un test que mide los niveles de gestión y alineación aplicados específicamente a la seguridad en referencia a la información día a día en el Site del Callao mediante los registros respectivos obtenidos a cada uno de los involucrados y por áreas.

Si la población es mínima o pequeña debe ser seleccionada en su totalidad para así reducir el error en la muestra. (Ary, W. 1996)

2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.4.1 Técnicas

La Observación

"Tiene como fin el de recoger datos para realizar las formulaciones o revisar las hipótesis" (Fernández- Ballesteros, 1980, Pág. 135).

2.4.2 Instrumentos

Ficha de Observación

Se utiliza la ficha de observación ya que permite conocer cómo se desarrollan todas las actividades en la empresa tales como rendimiento de equipos, seguridad ante desastres naturales, desempeño de personas. Disponible en: http://basicaespecial.perueduca.edu.pe/web/libros_digebe/7/files/assets/downloads/page0135.pdf Revisado 10/04/2017

2.4.3 Validación y confiabilidad del Instrumento

Tiene como características principales en todos los instrumentos de carácter científico para obtener los datos. Si el instrumento tiene las características habrá cierta garantía de los resultados en un determinado estudio y, por lo tanto, se puede concluir que puede generar mayor credibilidad. (Pérez (1998:71).

2.5 Métodos de análisis de datos

Luego de la recolección de datos utilizaremos la herramienta llamada SPSS para la realización de pruebas estadísticas, pudiendo explorar los datos, evaluar la confiabilidad y validez obtenidas por el instrumento de validación la cual nos permite técnicamente demostrar todo el análisis

2.6 Aspectos éticos

En referencia al trabajo realizado se brindará siempre el respeto en el cual está incluida en nuestra bibliografía. Se ha considerado como parte de la ética el anonimato de las personas involucradas sólo el cargo.

Toda investigación que incluya sujetos debe ser realizada de acuerdo con los principios básicos que son el respeto, la beneficencia, la no maleficencia los principios de moral y la justicia en todo sentido.

III. RESULTADOS

3.1 ANÁLISIS DESCRIPTIVO.

Se contempló la norma ISO 27001 para verificar su impacto para la Confidencialidad, Integridad y Disponibilidad y para esto se aplicaron un pre test la cual visualiza las actuales circunstancias del momento en los indicadores de estudio, luego se puso en práctica la norma ISO 27001 y se registró la información obtenida. Para la observación de los resultados veremos las siguientes tablas:

Tabla 11: Análisis descriptivo SPSS – Indicador 1 - Pre – Post Test

	N	Rango	Mínimo	Máximo	Media	Coeficiente de variación
Pretest	30	20	15	35	23,53	9,39%
Postest	30	2	1	3	1,83	12,42%
N válido (por lista)	30					

Se obtuvo como media del Nivel de información que puede ser divulgada sin autorización., en el pre test de la muestra 23,53, mientras que para el post test el valor fue de 1,83; mencionan un contraste entre el antes y después de la norma ISO así mismo los registros mínimos fueron 15 antes y 1 después.

Como la dispersión de los registros en el pre test fue de 9,39% y en el post test de 12,42%, se corrobora que la variabilidad con respecto a los datos no difiere en gran medida y se considera adecuada.

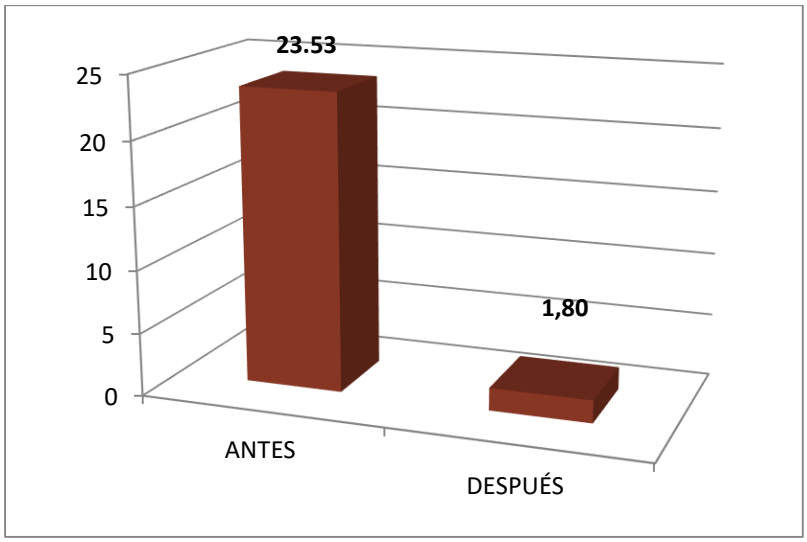


Figura 1: La figura muestra el promedio de Nivel de información que puede ser divulgada sin autorización

Tabla 12 Análisis descriptivo SPSS – Indicador 2 - Pre – Post Test

	N	Rango	Mínimo	Máximo	Media	Coeficiente de Variación
Pretest	30	29	65	94	81,37	8,35%
Postest	30	2	1	3	2,10	3,50%
N válido (por lista)	30					

Se obtuvo como media del Nivel de información que puede ser modificada sin autorización, en el pre test de la muestra 81,37, mientras que para el post test el valor fue de 2,10 mencionan un contraste entre el antes y después de la norma ISO así mismo los registros mínimos fueron 65 antes y luego 1 después.

Como la dispersión de los registros en el pre test fue de 8,35% y en el post test de 3,50%, se corrobora que la variabilidad con respecto a los datos no difiere en gran medida y se considera adecuada.

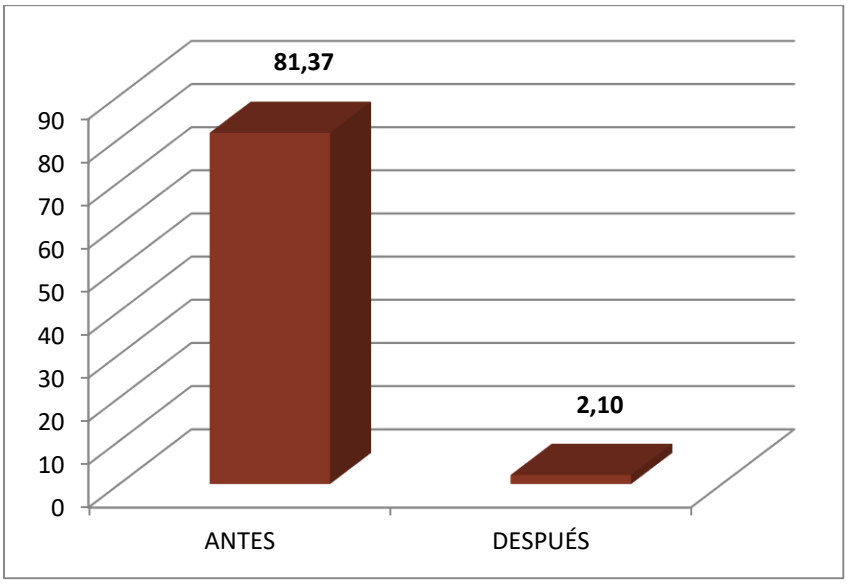


Figura 2: La figura muestra el promedio de Nivel de información que puede ser modificada sin autorización

Tabla 13: Análisis descriptivo SPSS - Indicador 3 - Pre – Post Test

	N	Rango	Mínimo	Máximo	Media	Coeficiente de Variación
Pretest	30	10	15	25	18,77	5,77%
Postest	30	2	1	3	1,70	1,44%
N válido (por lista)	30					

Se obtuvo como media del Nivel de información cuya inaccesibilidad es frecuente, en el pre test de la muestra 18,77, mientras que para el post test el valor fue de 1,70 mencionan un contraste entre el antes y después de la norma ISO así mismo los registros mínimos fueron 15 antes y luego 1 después.

Como la dispersión de los registros en el pre test fue de 5,77%% y en el post test de 1,44%, se corrobora que la variabilidad con respecto a los datos no difiere en gran medida y se considera adecuada.

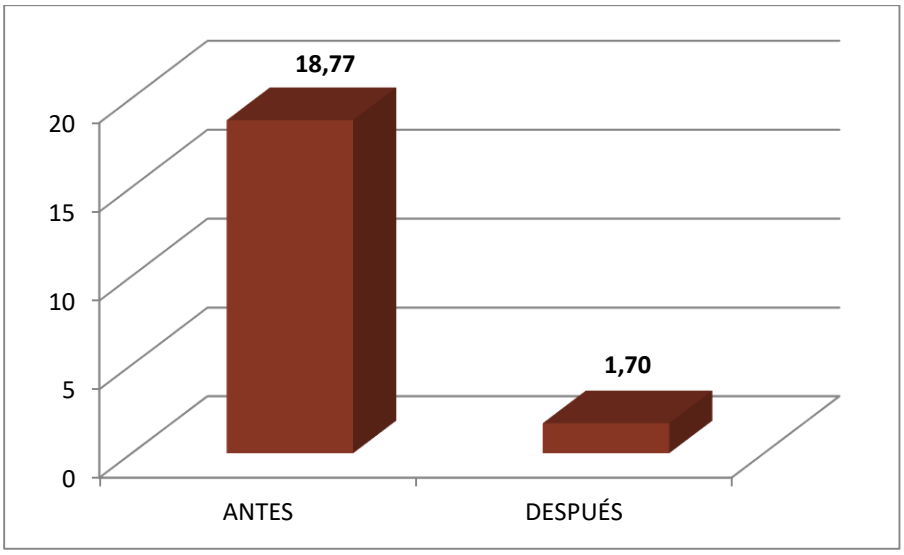


Figura 3: La figura muestra el promedio de Nivel de información cuya inaccesibilidad es frecuente

3.2 ANÁLISIS INFERENCIAL.

3.2.1 Prueba de Normalidad

Para la prueba de hipótesis todo lo recopilado fueron llevados a validar su distribución, especialmente si los puntos mencionados presentaban distribución normal; aplicando la prueba de Shapiro-Wilk ambos indicadores ya que las muestras mencionan ser menores a 50.

Indicador 1: Nivel de información que puede ser divulgada sin autorización

Para la prueba de hipótesis; los recopilado se llevó a validar su distribución, especialmente si los datos del Nivel de información que puede ser divulgada sin autorización presentaban una distribución normal.

Ho = Los datos tienen un comportamiento normal.

Ha= Los datos no tienen un comportamiento normal.

Prueba de normalidad del Nivel de información que puede ser divulgada sin autorización antes y después de puesta la Norma ISO 27001.

Tabla 14: Pruebas de normalidad – Indicador1

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
pretest	Nivel de información que puede ser divulgada sin autorización	,962	30	,346
postest	Nivel de información que puede ser divulgada sin autorización	,785	30	,001

Se observa los resultados mediante el estadístico de Shapiro-Wilk muestra = 30.

En el caso del pre test, la significancia fue 0.346, si tiene distribución normal y en el post test fue 0,001 que es menor que 0.05, por lo tanto, los valores del número de errores en los registros antes y después no corresponden de una distribución normal.

En base a lo obtenido, la comparación se realizó mediante la prueba no paramétrica W de Wilcoxon ya que los grupos son relacionados.

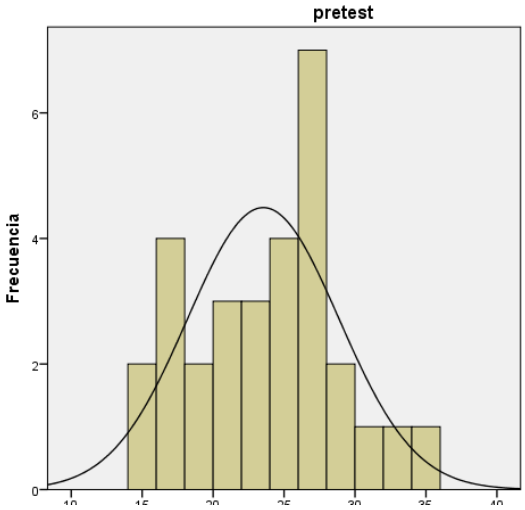


Figura 04: La figura muestra el Histograma del Nivel de información que puede ser divulgada sin autorización en el pre test

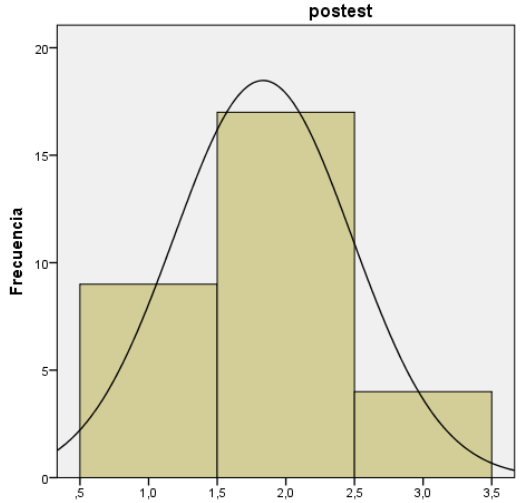


Figura 05: La figura muestra el Histograma del Nivel de información que puede ser divulgada sin autorización en el post test

Indicador 2: Nivel de información que puede ser modificada sin autorización

Con el propósito de elegir la prueba de hipótesis, lo recopilado se llevó a la corroboración de su distribución, especialmente si los datos del Nivel de información que puede ser modificada sin autorización presentaban una distribución normal.

Ho = Los datos tienen un comportamiento normal.

Ha= Los datos no tienen un comportamiento normal.

Prueba de normalidad del Nivel de información que puede ser modificada sin autorización antes y después de gestionar en base a la Norma ISO 27001.

Tabla 15: Pruebas de normalidad – Indicador 2

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pretest	Nivel de información que puede ser modificada sin autorización	,971	30	,574
Postest	Nivel de información que puede ser modificada sin autorización	,807	30	,002

Se visualizan los resultados mediante el estadístico de Shapiro-Wilk muestra = 30.

En el caso del pre test, la significancia fue 0.574, si tiene distribución normal y en el postest fue 0,002 que es menor que 0.05, por lo tanto, los valores del número de errores en los registros antes y después no corresponden de una distribución normal.

En base a los resultados, la comparación se realizó mediante la prueba no paramétrica W de Wilcoxon ya que los grupos son relacionados.

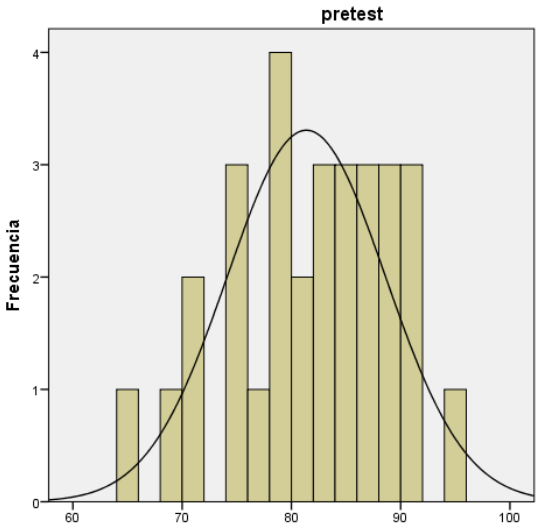


Figura 06: La figura muestra el Histograma del Nivel de información que puede ser modificada sin autorización en el pre test

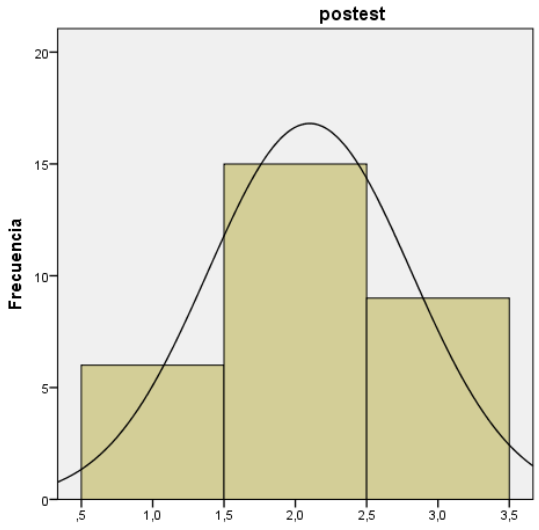


Figura 07: La figura muestra el Histograma del Nivel de información que puede ser modificada sin autorización en el post test

Indicador 3: Nivel de información cuya inaccesibilidad es frecuente

Con el propósito de elegir la prueba de hipótesis; lo recopilado se llevó a la corroboración de su distribución, especialmente si los datos del Nivel de información cuya inaccesibilidad es frecuente presentaban una distribución normal.

Ho = Los datos tienen un comportamiento normal.

Ha= Los datos no tienen un comportamiento normal.

Prueba de normalidad del Nivel de información cuya inaccesibilidad es frecuente antes y después de puesta la Norma ISO 27001.

Tabla 16: Pruebas de normalidad – Indicador 3

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pretest	Nivel de información cuya inaccesibilidad es frecuente	,940	30	,090
Postest	Nivel de información cuya inaccesibilidad es frecuente	,774	30	,001

Se visualiza los resultados mediante el estadístico de Shapiro-Wilk muestra = 30.

En el caso del pre test, la significancia fue 0,090, si tiene distribución normal y en el postest fue 0,001 que es menor que 0.05, por lo tanto, los valores del número de errores en los registros antes y después no corresponden una distribución normal.

En base a lo obtenido, la comparación se realizó mediante la prueba no paramétrica W de Wilcoxon, ya que los grupos son relacionados.

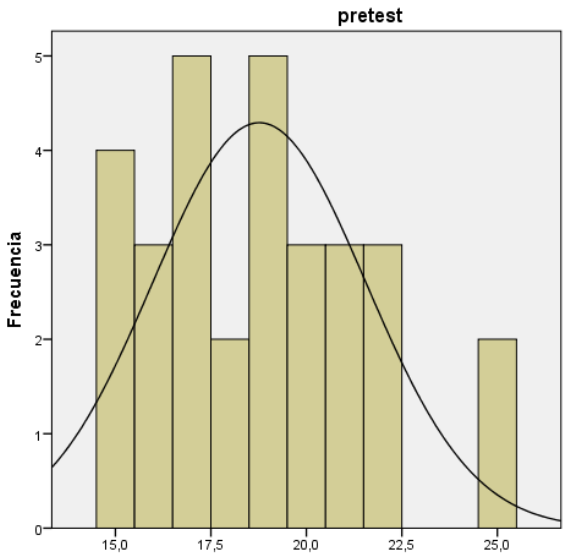


Figura 08: La figura muestra el Histograma del Nivel de información cuya inaccesibilidad es frecuente en el pre test

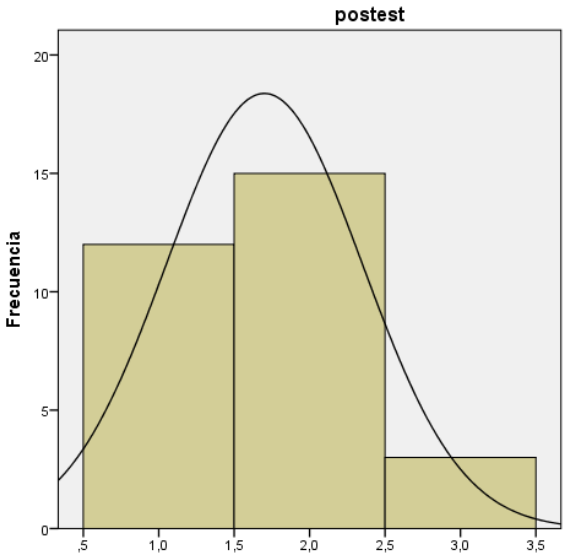


Figura 09: La figura muestra el Histograma del Nivel de información cuya inaccesibilidad es frecuente en el post test

3.3 PRUEBA DE HIPÓTESIS

Hipótesis Indicador 1

Hipótesis Alterna

Ha. Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

Hipótesis Nula

Ho. Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

$\mu 1$ = Media del nivel de información que puede ser divulgada sin autorización en la Pre Prueba.

$\mu 2$ = Media del nivel de información que puede ser divulgada sin autorización en la Post Prueba.

Ha: $\mu 2 < \mu 1$

H0: $\mu 2 \geq \mu 1$

Nivel de significación: 5%

Estadístico de prueba: “W” de Wilcoxon

Prueba W” de Wilcoxon en el Nivel de información que puede ser divulgada sin autorización antes y después de puesta la norma ISO 27001.

Tabla 17: Pruebas de Wilcoxon – Indicador 1

		N	Rango promedio	Suma de rangos	Z	Sig. asintótica (bilateral)
postest - pretest	Rangos neg.	30[a]	15,50	465,00	-4,792[b]	,000
	Rangos pos.	0[b]	,00	,00		
	Empates	0[c]				
	Total	30				

Decisión

Lo obtenido en la prueba “W” de Wilcoxon, indican que, debido al resultado hay una desviación a cero en comparación de la probabilidad asumida de 0.05, se declara rechazado la hipótesis nula, por lo que el Nivel de información que puede ser divulgada sin autorización antes es mayor que después de la puesta de la norma ISO 27001.

Por lo tanto, esta implementación para la gestión de la seguridad de la información impacta en forma positiva en Nivel de información que puede ser divulgada sin autorización en la empresa Atento del Perú 2017.

Hipótesis Indicador 2

Hipótesis Alterna

Ha. Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

Hipótesis Nula

Ho. Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

$\mu 1$ = Media del nivel de información que puede ser modificada sin autorización en la Pre Prueba.

$\mu 2$ = Media del nivel de información que puede ser modificada sin autorización en la Post Prueba.

Ha: $\mu 2 < \mu 1$

H0: $\mu 2 \geq \mu 1$

Nivel de significación: 5%

Estadístico de prueba: “W” de Wilcoxon

Prueba W” de Wilcoxon en el Nivel de información que puede ser modificada sin autorización antes y después de la norma ISO 27001.

Tabla 18: Pruebas de Wilcoxon – Indicador 2

		N	Rango promedio	Suma de rangos	Z	Sig. asintótica (bilateral)
postest - pretest	Rangos neg.	30[a]	15,50	465,00	-4,784[b]	,000
	Rangos pos.	0[b]	,00	,00		
	Empates	0[c]				
	Total	30				

Decisión

Lo obtenido en la prueba “W” de Wilcoxon, indican que, debido al resultado hay una desviación a cero en comparación de la probabilidad asumida de 0.05, se rechaza la hipótesis nula, por lo que el Nivel de información que puede ser modificada sin autorización antes es mayor que después de la puesta de la norma ISO 27001.

Por lo tanto, esta implementación para la gestión de la seguridad de la información impacta en forma positiva en Nivel de información que puede ser modificada sin autorización en la empresa Atento del Perú 2017.

Hipótesis Indicador 3

Hipótesis Alterna

Ha. Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

Hipótesis Nula

Ho. Gestionar en base a la norma ISO 27001 no tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017. (Post Prueba) con referencia de la muestra a la que no se aplicó (Pre Prueba).

$\mu 1$ = Media del Nivel de información cuya inaccesibilidad es frecuente en la Pre Prueba.

$\mu 2$ = Media del Nivel de información cuya inaccesibilidad es frecuente en la Post Prueba.

Ha: $\mu 2 < \mu 1$

H0: $\mu 2 \geq \mu 1$

Nivel de significación: 5%

Estadístico de prueba: “W” de Wilcoxon

Prueba W” de Wilcoxon en el Nivel de información cuya inaccesibilidad es frecuente antes y después de la norma ISO 27001.

Tabla 19: Pruebas de Wilcoxon – Indicador 3

		N	Rango promedio	Suma de rangos	Z	Sig. asintótica (bilateral)
postest	Rangos neg.	30[a]	15,50	465,00		
pretest	Rangos pos.	0[b]	,00	,00	-4,794[b]	,000
	Empates	0[c]				
	Total	30				

Decisión

Lo obtenido en la prueba “W” de Wilcoxon, indica que, debido al resultado hay una desviación a cero en comparación de la probabilidad asumida de 0.05, se rechaza la hipótesis nula, por lo que el Nivel de información cuya inaccesibilidad es frecuente antes es mayor que después de la puesta de la norma ISO 27001.

Por lo tanto, esta implementación para la gestión de la seguridad de la información impacta en forma positiva el Nivel de información cuya inaccesibilidad es frecuente en la empresa Atento del Perú 2017.

IV. DISCUSIÓN

Lo encontrado en la investigación se compararon los datos del Nivel de información que puede ser divulgada sin autorización, los datos del Nivel de información que puede ser modificada sin autorización, y los datos del Nivel de información cuya inaccesibilidad es frecuente antes y después de la puesta de la Norma ISO 27001 en la GSI en la empresa atento del Perú 2017.

- En el Nivel de información que puede ser divulgada sin autorización en la medición pre-test, alcanzó 23,53 esto indicaba un nivel muy alto demostrando ausencia de controles y bajo en seguridad. Con la aplicación en el post test se redujo a 1,83, este porcentaje aumentó en un 92,23%, por lo tanto, se puede afirmar que la puesta del Sistema enfocado en la Norma ISO 27001 mejora en el Nivel de información que puede ser divulgada sin autorización en la empresa Atento del Perú ya que aumenta el nivel de seguridad de este proceso.

  Por consiguiente, coincide con el trabajo de investigación de Bermúdez (2015) titulado Análisis en seguridad Informática y Seguridad de la Información Basado en la norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros. KELLY GABRIELA BERMÚDES MOLINA en la cual los resultados son similares donde se logra aumentar el nivel de seguridad para la información de los procesos de Credigestión en la cual garantiza la integridad, disponibilidad y Confidencialidad.

- En el Nivel de información que puede ser modificada sin autorización en la medición pre-test, alcanzó 81,37 esto indicaba un nivel muy alto demostrando ausencia de controles y bajo en seguridad. Con la aplicación en el post test hubo una reducción del 2,10, este porcentaje aumentó en un 97,42% por lo tanto se puede afirmar que la puesta del Sistema basado en la Norma ISO 27001 mejora en el

Nivel de información que puede ser modificada sin autorización en la empresa Atento del Perú ya que aumenta el nivel de seguridad de este proceso.

Por consiguiente, coincide con el trabajo de investigación de Pardo (2015) titulado Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001-- en la cual los resultados son similares donde se logra aumentar el nivel de seguridad de la información que puede ser modificada sin autorización en sus activos manejada desde la Unidad de Telecomunicaciones e Información.

En el Nivel de información cuya inaccesibilidad es frecuente en la medición pre-test, alcanzó 18,77 esto indicaba un nivel muy alto demostrando ausencia de controles y bajo en seguridad. Con la aplicación en el post test se redujo a 1,70, este porcentaje aumentó en un 90,95% por lo tanto se puede afirmar que la puesta del Sistema basado en la Norma ISO 27001 mejora en el Nivel de información cuya inaccesibilidad es frecuente en la empresa Atento del Perú ya que aumenta el nivel de seguridad de este proceso.

Por consiguiente, coincide con el trabajo de investigación de Aguirre (2014) titulado Diseño del sistema de Gestión de Seguridad de la Información para los servicios portales del Perú S.A -- en la cual los resultados son similares donde se logra una mayor mejora del nivel de seguridad de la información cuya inaccesibilidad es frecuente para los servicios portales del Perú S.A

V. CONCLUSIÓN

Primera:

Se ha determinado que en el Nivel de información que puede ser divulgada sin autorización utilizando la norma ISO 27001 en la empresa atento del Perú fue de 1,83 y sin el uso de la norma ISO fue de 23,53 logrando una reducción significativa de 21,70, que representa el 92,23% en la información que puede ser divulgada sin autorización.

Segunda:

Se ha determinado que en el Nivel de información que puede ser modificada sin autorización utilizando la norma ISO 27001 en la empresa atento del Perú fue de 2,10 y sin el uso de la norma ISO fue de 81,37 logrando una reducción significativa de 79,27 que representa el 97,42% en la información que puede ser modificada sin autorización.

Tercera:

Se ha determinado que en el Nivel de información cuya inaccesibilidad es frecuente utilizando la norma ISO 27001 en la empresa atento del Perú fue de 1,70 y sin el uso de la norma ISO fue de 18,77 logrando una reducción de 17,07 que representa el 90,95% en la información cuya inaccesibilidad es frecuente.

VI. RECOMENDACIONES

Primera:

Se recomienda realizar los estudios en otras áreas que tiene la empresa así sea de otra jefatura para reducir el número de registros de información que puede ser divulgada sin autorización con el propósito de asegurar la permanencia y estabilidad de toda la información en peligro dentro de la empresa.

Segundo:

Se recomienda realizar los estudios en otras áreas que tiene la empresa, así como también ampliar todo lo referente a los riesgos de la información en otra jefatura para reducir el número de registros de información que puede ser modificada sin autorización con el propósito de asegurar los procesos en la empresa.

Tercera:

Se recomienda realizar los estudios en otras áreas que tiene la empresa así sea de otra jefatura para reducir el número de registros de información cuya inaccesibilidad es frecuente con el propósito de mejorar los procesos en la empresa.

Cuarto:

Se recomienda que la empresa implemente la metodología basado en la norma ISO 27001 también en otras sedes ya que así podrán mantener a buen recaudo sus activos más importantes y mantenerlos lejos de todo tipo de amenazas o reducir las amenazas a su mínima expresión.

VII. REFERENCIAS

Análisis y Gestión de Riesgos Implementando la Metodología Magerit PDF Downnload. [Fecha de Consulta 04 de mayo de 2017]. Disponible en: https://sites.google.com/a/hohenjon.top/jacksonasrui/analisis-y-gestion-de-riesgos-implementando-la-metodologia-magerit

Areitio, Javier. Seguridad de la Información. Universidad de Deusto, 2008, pp Xvi.

Areitio, Javier. Seguridad de la Información. Universidad de Deusto, 2015, pp 53-200.

Asociación Española Para la Calidad (AEC) [Fecha de Consulta 20 de abril de 2017]. Disponible en: http://www.aec.es/web/guest/centro-conocimiento/cobit

Asymmetric, ISO 27001, [Fecha de Consulta 04 de mayo de 2017]. Disponible en: http://asymmetric.mx/servicios/iso-27000/

Ávila Baray, H.L. Introducción a la metodología de la investigación Edición electrónica. 2006.

Bernal, C. Metodología de la Investigación (2da. Edición). México: Ed. Pearson (2006). [Fecha de Consulta 10 de febrero de 2017] Disponible en: http://brd.unid.edu.mx/recursos/Taller%20de%20Creatividad%20Publicitaria/TC03/lecturas%20PDF/05_lectura_Tecnicas_e_Instrumentos.pdf

BS grupo, Seguridad de la Información, [Fecha de Consulta 20 de mayo de 2017]. Disponible en: http://bsgrupo.com/bs-campus/blog/Seguridad-de-la-Informacin-20

Ciclo PDCA, El Circulo de Deming de Mejora Continua. [Fecha de Consulta 20 de abril de 2017]. Disponible en: http://www.pdcahome.com/5202/ciclo-pdca/

Fidias G. Arias (El proyecto de Investigación-Introducción a la metodología científica 5ta edición) 2006 pag. 81.

Gomez, Álvaro. Enciclopedia de la Seguridad Informática. México. Alfa omega, 2011, pp 59- 169.

IT Consultores SAS, Certificación ITIL. [Fecha de Consulta 20 de abril de 2017]. Disponible en: http://itconsultores.com.co/celebrado-el-primer-examen-en-espanol-para-certificarse-en-itil-v3/

Merino, Cristina y Cañizares Ricardo. Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001. Madrid: Fundación Confemetal, 2011. pp 38 – 121.

PriteshGupta.com, El portal de ISO 27001 en español [Fecha de Consulta 10 de febrero de 2017]. Disponible en: http://www.iso27000.es/sgsi.html revisado 20/12/2016

Rodríguez, Metodología De Investigación Científica Aplicado A La Ingeniería. Informe. (2012).

Sena, ITIL Versión 3, Fundamentos de la Gestión de Servicios de TI [Fecha en Consulta es el 10 de febrero de 2017]. Disponible en http://infoitilv3.weebly.com/

VIII. ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA								
TÍTULO	"IMPLEMENTACIÓN DE LA NORMA ISO 27001 EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ATENTO DEL PERÚ 2017"				DISEÑO DE INVESTIGACIÓN	EXPERIMENTAL		
FORMULACIÓN DEL PROBLEMA		OBJETIVOS		HIPÓTESIS		VARIABLE DEPENDIENTE	DIMENSIONES	INDICADORES
GENERAL	ESPECÍFICOS	GENERAL	ESPECÍFICOS	GENERAL	ESPECÍFICOS			
¿Qué resultados tendría gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017?	¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017?	Establecer cuáles el resultado de gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017.	Determinar el efecto de la implementación de la norma ISO 27001 en la confidencialidad de la gestión de la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.	Seguridad de la Información (Areitio, Javier,2015,p200)	Confidencialidad (Merino, Cristina y Cañizares,2011,p12)	Nivel de información que puede ser divulgada sin autorización
	¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la integridad para la seguridad de la información en la empresa Atento del Perú 2017?	Determinar el efecto de la implementación de la norma ISO 27001 en la integridad de la gestión de la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.		Integridad (Merino, Cristina y Cañizares,2011,p12)	Nivel de información que puede ser modificada sin autorización
	¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017?	Determinar el efecto de la implementación de la norma ISO 27001 en la disponibilidad de la gestión de la seguridad de la información en la empresa Atento del Perú 2017	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.			Disponibilidad (Merino, Cristina y Cañizares,2011,p12)	Nivel de información cuya inaccesibilidad es frecuente

ANEXO 2: FICHA DE OBSERVACIÓN

INVESTIGADOR: SALSAVILCA RAMOS JUAN CARLOS

EMPRESA: TELEATENTO DEL PERÚ

DIMENSION: CONFIDENCIALIDAD

INDICADOR: NIVEL DE INFORMACIÓN QUE PUEDE SER DIVULGADA SIN AUTORIZACIÓN

OBSERVACIONES	Pretest	Postest
	Nivel de información que puede ser divulgada sin autorización	**Nivel de información en que puede ser divulgada sin autorización**
1	31	2
2	26	1
3	27	3
4	22	2
5	20	1
6	21	2
7	15	1
8	17	1
9	25	2
10	27	2
11	35	3
12	33	3
13	27	2
14	29	2
15	27	2
16	25	2
17	28	3
18	27	2
19	25	2
20	27	2
21	24	2
22	23	2
23	22	1
24	17	1
25	18	2
26	19	2
27	21	2
28	16	1
29	15	1
30	17	1
Promedio	23,53	1,83

ANEXO 3: FICHA DE OBSERVACIÓN

INVESTIGADOR: SALSAVILCA RAMOS JUAN CARLOS

EMPRESA: TELEATENTO DEL PERÚ

DIMENSION: INTEGRIDAD

INDICADOR: NIVEL DE INFORMACIÓN QUE PUEDE SER MODIFICADA SIN AUTORIZACIÓN

OBSERVACIONES	Pretest	Postest
	Nivel de información que puede ser modificada sin autorización	**Nivel de información que puede ser modificada sin autorización**
1	65	2
2	70	3
3	80	3
4	75	2
5	79	1
6	88	2
7	91	3
8	90	2
9	87	3
10	89	2
11	90	3
12	86	2
13	94	3
14	86	2
15	88	3
16	85	2
17	79	3
18	82	1
19	84	1
20	75	1
21	76	2
22	70	1
23	69	1
24	75	2
25	79	2
26	82	3
27	78	2
28	81	2
29	83	2
30	85	2
Promedio	81,37	2,10

ANEXO 4: FICHA DE OBSERVACIÓN

INVESTIGADOR: SALSAVILCA RAMOS JUAN CARLOS

EMPRESA: TELEATENTO DEL PERÚ

DIMENSION: DISPONIBILIDAD

INDICADOR: NIVEL DE INFORMACIÓN CUYA INACCESIBILIDAD ES FRECUENTE

OBSERVACIONES	Pretest	Postest
	Nivel de información cuya inaccesibilidad es frecuente	**Nivel de información cuya inaccesibilidad es frecuente**
1	20	1
2	25	2
3	22	2
4	15	1
5	15	1
6	18	2
7	17	1
8	19	2
9	21	3
10	17	2
11	18	2
12	20	2
13	22	3
14	16	1
15	22	2
16	25	3
17	21	2
18	20	2
19	17	1
20	19	2
21	15	1
22	17	1
23	16	1
24	19	2
25	16	1
26	15	1
27	17	1
28	19	2
29	21	2
30	19	2
Promedio	18,77	1,70

ANEXO 5 PLANTEAMIENTO DEL PROBLEMA, OBJETIVO, HIPÓTESIS

TITULO: IMPLEMENTACIÓN DE LA NORMA ISO 27001 EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ATENTO DEL PERÚ 2017

AUTOR: JUAN CARLOS SALSAVILCA RAMOS

DOCENTE: DRA YESENIA VÀSQUEZ VALENCIA

LINEA DE INVESTIGACION: AUDITORIA DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

Problema Principal	**Objetivo principal**	**Hipótesis Principal**
¿ Qué resultados tendría gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017?	Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo para la seguridad de la información en la empresa Atento del Perú 2017..
Problema Específico	**Objetivo Específico**	**Hipótesis Específico**
¿ Qué resultados tendría gestionar en base a la norma ISO 27001 en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017?	Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la confidencialidad para la seguridad de la información en la empresa Atento del Perú 2017.
¿Qué resultados tendría gestionar en base a la norma ISO 27001 en la integridad para la seguridad de la información en la empresa Atento del Perú 2017?	Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la integridad para la seguridad de la información en la empresa Atento del Perú 2017.
¿ Qué resultados tendría gestionar en base a la norma ISO 27001 en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017?	Establecer cuál es el resultado de gestionar en base a la norma ISO 27001 en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.	Gestionar en base a la norma ISO 27001 tiene un efecto significativo en la disponibilidad para la seguridad de la información en la empresa Atento del Perú 2017.

ANEXO 6: INSTRUMENTO REGISTRO DE OBSERVACIÓN

Dimensión 1 CONFIDENCIALIDAD
1- ¿Existe políticas necesarias para la seguridad de la información?
2-¿Cambias con frecuencia la clave de tu cuenta?
3- Existe administrador de aplicaciones de gestión?
4- ¿Se utilizan políticas de controles de acceso?
5-¿Solo personal autorizado puede acceder fácilmente a la información?
6- Existe responsable de cancelar las cuentas de personal cesado?
7- ¿la información es sólo para personal autorizado?
8-¿Existen registros de usuarios autorizados?
9-¿Existe gestión de claves?
10- ¿Son frecuentes las copias de seguridad?
11- ¿Los jefes o responsables tienen cuentas de administrador?
12- ¿La divulgación de la información personal afecta a la empresa?
13- ¿las cuentas de personal cesado se desactivan?
14- ¿Se utiliza protección de registros?
15- ¿Las copias de seguridad sólo lo realiza personal autorizado?
16- ¿Existe administrador de usuarios?
17- ¿Los trabajadores tienen usuarios personalizados?
18- ¿Cumple con la confidencialidad al enviar y recibir información vía correo?
19- ¿La cuenta de usuario es personal?
20- - ¿Como supervisor la percepción de Confidencialidad de la información es óptima?
21- ¿Se cumplen las políticas en seguridad de información?
22- ¿Tus archivos se pierden con facilidad?
23-¿Ofrece la confidencialidad necesaria cuando se conecta a la red de internet?
24-¿Cualquier usuario puede ingresar a otros correos?
25- ¿Su cuenta de usuario tiene acceso ilimitado?
26- ¿Cumple con la confidencialidad al colocar clave alfanumérica en su cuenta?
27- ¿Las cuentas se bloquean después de varios intentos de ingreso?
28- ¿Has tenido perdida de información en tu cuenta?
29-¿Se utiliza controles adecuados del uso de la información?
30-¿Las claves de acceso de aplicaciones son según los protocolo?

ANEXO 7: INSTRUMENTO REGISTRO DE OBSERVACIÓN

Dimensión 2 INTEGRIDAD
1- Las configuraciones de los equipos con Windows son estandarizados?
2-¿La información recuperada luego de mantenimiento es completa?
3- ¿ La información está protegida de amenazas como virus
4- ¿La información que solicitas es completa?
5- ¿la información puede ser modificada fácilmente por cualquier usuario?
6-¿Es disponible toda la información en el momento que se solicite?
7- ¿la información solicitada es completa y válida?
8-¿Los indicadores recibidos están completos?
9- ¿Utilizan controles de registro de fallos e incidencias?
10- ¿Existe control de códigos maliciosos?
11- ¿Los controles de red son permanentes?
12- El antivirus cumple con proteger la integridad de la información así como a las aplicaciones?
13- ¿Existen políticas de procedimientos de manejo de información?
14- - ¿Cumple con la integridad necesaria al evitar que personal ajeno no modifique o altere la información?
15- Se cumple con la reposición completa de los headphones ?
16- - ¿Como supervisor la percepción de Integridad de la información es óptima?
17- ¿Existe políticas para la seguridad en sistema?
18- ¿La data es cifrada?
19- ¿Cuenta con back up ?
20- Existen políticas de configuración base?
21- ¿Existe diagnostico remoto del pc?
22- Las aplicaciones se encuentran físicamente seguras?
23-¿Se recupera la información mediante requerimientos?
24-¿Se cumplen los plazos de atención de los requerimientos solicitados?
25- ¿Se cumple con la reparación total de los equipos?
26- ¿Es común la perdida de archivos?
27- ¿Los usuarios pueden modificar las aplicaciones?
28-¿La información de tu cuenta fue modificada sin autorización tuya?
29-¿Existen bitácoras en la cual se puede encontrar intentos de modificación de aplicaciones o de información?
30- ¿Los usuarios no autorizados participan en funciones de análisis?

ANEXO 8: INSTRUMENTO REGISTRO DE OBSERVACIÓN

Dimensión 3 DISPONIBILIDAD
1- considera aceptable el tiempo de la recuperación de la información tras ataque virus
2-¿Se puede acceder a la información rápidamente?
3- Los indicadores solicitados a los responsables se envían dentro de plazo?
4- ¿Con que frecuencia se cambian las claves y llaves de cifrado?
5- ¿Se encuentra satisfecho el personal con la disponibilidad de la información?
6- ¿Existe disponibilidad de los equipos de cómputo para todo el personal en turno?
7- ¿Existe buen desempeño al trabajar con todas las aplicaciones en las pc?
8- Existe más personal que equipos de cómputo?
9- ¿Los correos corporativos se encuentran personalizados?
10- ¿Existe restricción de acceso a la información?
11- ¿Todos los supervisores tienen disponibilidad de correos corporativos?
12- ¿Los indicadores son actualizados para ser disponibles de los usuarios?
13- - ¿Pueden conectarse todas las usuarios a la vez sin afectar la disponibilidad de la información?
14- ¿Se siente cómodo con la Disponibilidad de las computadoras?
15- ¿Puedes acceder a la información las 24 horas del día?
16- - ¿Pueden trabajar con facilidad todas las aplicaciones instaladas en las PC sin que exista criticidad de colapso?
17- - ¿Existe la disponibilidad inmediata de la información en la red?
18- ¿Cumple con la Disponibilidad cualquiera de las computadoras del área?
19- ¿La disponibilidad de las pc satisface las necesidades del equipo de trabajo?
20- ¿Los sistemas informáticos brindan la disponibilidad oportuna?
21- ¿Como supervisor la percepción de disponibilidad de la información es óptima?
22- ¿La No optimización de los sistemas informáticos afecta la disponibilidad?
23-¿Cumple con la Disponibilidad del internet en la red?
24- ¿Cuál es la frecuencia de actualización de indicadores?
25- ¿Las páginas web presentan caída constante?
26- ¿Las computadoras presentan caída o lentitud extrema?
27- Consideras adecuado los sistemas informáticos en nuestros áreas?
28-- ¿Existe criticidad al estar conectadas todas las computadoras a la vez?
29- ¿La falta de disponibilidad en general afecta económicamente?
30- ¿Encuentra disponible pc en su jornada laboral?

Implementación del Sistema de Gestión de la Seguridad de la Información según ISO 27001

A continuación, las fases y las actividades en las que se organiza la instalación de un SGSI con el estándar ISO 27001.

FASE I

- Planificación del proyecto
- Análisis de situación respecto de la norma (GAP ANALISIS)

FASE II

- Análisis de riesgos
- Gestión de riesgos
- Elaboración de los planes y programas de acción

FASE III

- Elaborar documentos del Sistema de gestión (PDCA)
- Definición de las acciones para la comunicación, formación y concienciación
- Evaluación del control operativo
- Elaboración de los indicadores de gestión
- Puesta en funcionamiento del sistema de gestión

FASE IV

- Rodaje y mejora del sistema de gestión
- Indicadores
- Auditoria interna

FASE V

- Planes para mejorar el sistema de la gestión.

Tabla 20: Actividades de la implementación del SGSI

Actividad	Proyecto De Implementación	Implementación SGSI (1° Ciclo PDCA)	Mejora Continua
Planificación del Proyecto	FASE I		
Análisis de situación	FASE I		
Definición de Organización	FASE I	PLAN	
Análisis y Gestión de Riesgos.	FASE II	PLAN	PLAN Nuevo Análisis de Riesgos
Definición de las acciones para la comunicación, formación y concienciación.	FASE III	DO	Revisión
Evaluación de los indicadores de gestión.	FASE III	DO	Elaboración de nuevos planes.

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

TABLA 21: Actividades de la implementación del SGSI

Actividad	**Proyecto Implementación**	**Implementación SGSI (1° Ciclo PDCA)**	**Mejora Continua Ciclo PDCA**
Puesta en funcionamiento del Sistema de Gestión	FASE III	DO	
Rodaje y mejora del Sistema de Gestión	FASE IV	DO	
Indicadores	FASE IV	DO	
Auditoría Interna	FASE IV	CHECK	

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

PLANIFICACIÓN DEL PROYECTO

Para esta actividad se ajustarán los plazos y se definirán las actuaciones a realizar, elaborando una planificación definitiva. Adicionalmente se establecerán las pautas a seguir para la gestión.

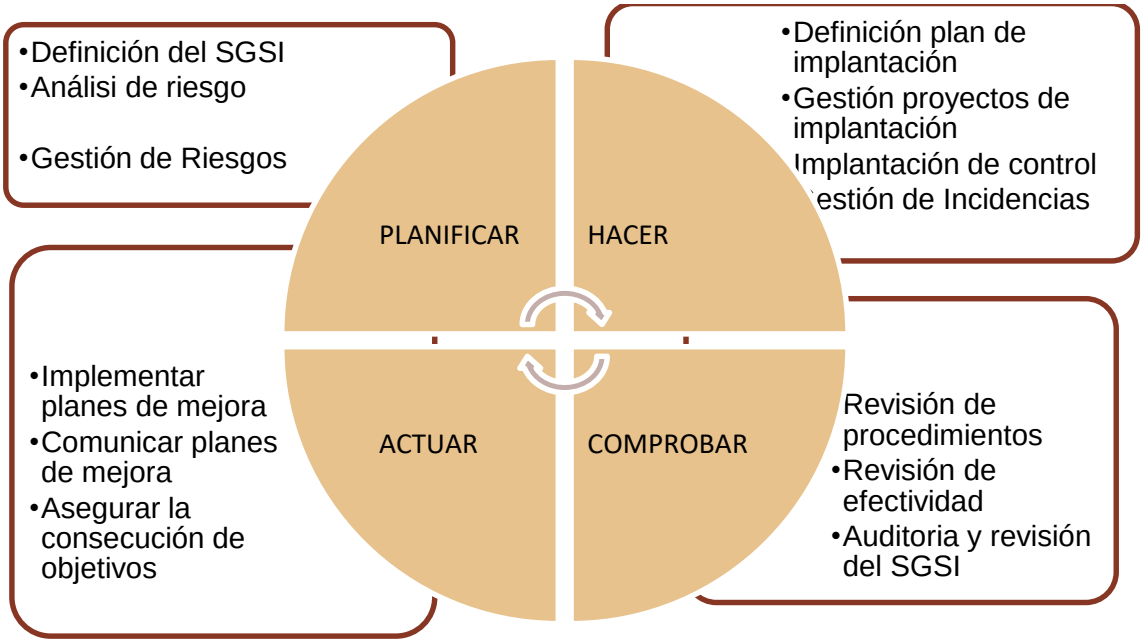


Figura 10: Planificación del proyecto en base al ciclo Continuo PDCA

De esta actividad se obtuvo:

- Una mejor visión inicial de la situación y del funcionamiento de la organización y del cuerpo normativo que brinda el soporte.
- La primera aproximación al plan de trabajo y al perfil de los grupos de trabajo.
- La organización interna del proyecto y los riesgos que afectan a su ejecución.
- La presentación del proyecto a todos los interesados y participantes de la organización.

La norma ISO 27001 está basada como ya se mencionó anteriormente en el modelo PDCA en el cual se planifican las diferentes tareas dentro del plan.

Aceptación de la Dirección

La dirección es quien decide sobre la aceptación formal o sobre su tratamiento, es por esto que previamente a las actividades de implementación del SGSI debe existir la constancia documental de la decisión que se tomó.

Declaración de Aplicabilidad (SOA)

En esta etapa consiste en elaborar una declaración de aplicabilidad (STATEMENT OF APPLICABILITY - SOA) donde la norma ISO 27001 hace hincapié, en la cual consiste en contar con los controles y el motivo de su selección.

Las declaraciones de aplicabilidad muestrean los controles que son presentados a la dirección y además identifica si cada control esta implementado o no.

TABLA 22: DECLARACIÓN DE APLICABILIDAD (SOA)

DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivos de control	Control	Aplicable	Justificación	Referencia en el SGSI
2. Responsabilidad sobre los activos				
2.1.6 Cooperación con todas las autoridades	Es necesario estar en contacto con las autoridades que correspondan	SI	Requerimiento ISO 27001 Y LEGAL	Plan continuidad del negocio
3. Clasificación de la información				
3.1 Uso adecuado de los activos	El uso de reglas en la información y en sus recursos es necesario que sean identificadas así como documentadas.	SI	Requerimiento ISO 27001	Manual de operaciones técnicas
3.2. Directrices de clasificación	Se debería clasificar dependiendo su importancia, ya sean legales así como su sensibilidad y criticidad para la organización.	SI	Requerimiento ISO 27001	Clasificación, y tratamiento

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

TABLA 23: DECLARACIÓN DE APLICABILIDAD (SOA)

DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivos de control	Control	Aplicable	Justificación	Referencia en el SGSI
4. Seguridad Física y del entorno				
4.1. Áreas Seguras				
4.1.1 Perímetro físico de seguridad	Es necesario contar con parámetros de seguridad idóneos con la finalidad de resguardar la información.	SI	Existen controles físicos de entrada proporcionales al tamaño y actividad de la organización	Protección física y del entorno
4.1.2. Controles físicos de entrada	La plataforma física y lógica deben ser resguardadas al máximo para el control y solamente se permite el ingreso al personal con la autorización debida.	SI	Existen controles físicos de entrada proporcionales al tamaño y actividad de la organización	Protección física y del entorno

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

TABLA 24: DECLARACIÓN DE APLICABILIDAD (SOA)

DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivos de control	Control	Aplicable	Justificación	Referencia en el SGSI
5.2. Seguridad de los equipos				
5.2.1 Mantenimiento de equipos	Es necesario el mantenimiento preventivo de todos los equipos que hagan continuar su integridad.	SI	Existe mantenimiento de equipos.	Protección física y del entorno
5.2.2. Suministros	Se requiere contingencia ante cortes de fluido de electricidad por cualquier tipo de causa.	SI	Se dispone de sistemas de alimentación interrumpida	Protección física y del entorno

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

TABLA 25: DECLARACIÓN DE APLICABILIDAD (SOA)

DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivos de control	Control	Aplicable	Justificación	Referencia en el SGSI
6.2. Gestión en seguridad de red				
6.2.1 Seguridad en los servicios de red	Los requerimientos de los servicios de red deberían estar identificados e incluidos en todo acuerdo de servicios de red,	SI	Se hacen auditorías de red periódicamente	Manual de sistemas de información.
7. Utilización de soportes de información				
7.1. Seguridad de la documentación de sistemas	El sistema de documentación debería estar protegido contra accesos no autorizado.	SI	Requerimiento legal	Manual de sistemas de información.

Fuente: Cristina, Merino - Cañizares Implantación de un SGSI según ISO 27001

Tabla 26: Valoración Cualitativa de los Activos

Nombre Activo	Dimensiones		
	Confidencialidad	Integridad	Disponibilidad
Información de Licencias	3	3	0
Archivos de Clientes.	3	3	0
Copia de seguridad de la data	0	3	0
Manual en configurar equipos	3	3	0
Contraseñas de acceso de empleados.	3	0	3
Acceso internet de los empleados	3	3	0
Uso de correo corporativo del trabajador	3	3	0
Soporte en servidor de bases de datos.	3	3	0
Servidor de aplicaciones	3	3	0
Responsable en base de datos.	3	3	0
Office 2013	0	0	3
Mcafee original con actualizaciones automáticas.	3	0	1
Sistema operativo Windows actualizado.	0	0	2
Equipos de mesa	3	3	1
Servidor de Base de Datos	3	3	1
Impresoras	0	0	2
Red local	3	3	1
Almacenamientos en Disco Duro	0	2	2
Ups computadores	0	0	2
Edificio de la empresa	0	0	2

Fuente: Enciclopedia de la Seguridad Informática.

Tabla 27: Escala porcentual del impacto

1) Muy alto (Escala porcentual del impacto) 2) Medio 3) Bajo 4) Muy Bajo ---------- Nombre Activos con riesgos	Antes de SGSI Impacto	Después de SGSI impacto
Equipos informáticos frecuencia de la amenaza	Alto	Muy bajo
Software - Aplicaciones Informáticas	Alto	Muy bajo
Ups computadores	Alto	Muy bajo
Internet en redes de comunicaciones internas	Muy Alto	Bajo
Archivos de Clientes	Muy Alto	Bajo
Copia de seguridad de la data	Bajo	Muy bajo
Soporte en servidor de bases de datos.	Alto	Muy bajo
Contraseñas de acceso de Empleados	Alto	Muy bajo
Acceso internet de los empleados	Alto	Muy bajo
Manejo de correos electrónicos	Muy Alto	Bajo
Servidor de aplicaciones	Bajo	Bajo
Mcaafe original con Actualizaciones automáticas.	Alto	Muy bajo
Acceso de personas no autorizadas a la empresa	Alto	Muy bajo
Claves de acceso frecuencia de amenaza	Muy alto	Muy bajo
Acceso de aplicaciones y/o programas no autorizados	Muy alto	Muy bajo
Zonas seguras contra desastres naturales	Alto	Muy Bajo
Muebles de cómputo inflamables	Alto	bajo

Fuente: Enciclopedia de la Seguridad Informática.

Tabla 28: Mejoras en Dimensiones

DISPONIBILIDAD	ANTES	DESPUÉS	¿HAY MEJORA?
NÚMERO DE INCIDENCIAS	2 A 30 AL MES	1 A 2	SI
INFORMACIÓN ACCESIBLE	INTERMITENTE	7 X 24	SI
SOLICITUD DE INFO	2 A 3 HORAS	0 HORAS	SI
CONFIDENCIALIDAD			
COPIAS DE SEGURIDAD	MENSUAL	DIARIA	SI
REGISTRO DE USUARIOS	15 REGISTRADOS	25 USUARIOS (TODOS)	SI
USUARIOS BLOQUEDOS EX TRABAJADORES	4	8 TODOS	SI
INTEGRIDAD			
INFORMACIÓN UNICA Y ESPECÍFICA	1 CONTROL QUE LO GARANTIZA	5 CONTROL QUE LO GARANTIZA	SI
PERMISOS DE ACCESO	NO HAY FORMATO NI POLÍTICA	2 FORMATOS, UNA POLÍTICA	SI
REPORTE DE MODIFICACIONES	NINGUNO	EXISTE CONTROL DE VERSIÓN DE DOCUMENTOS	SI
RESTRICCIÓN A USUARIOS	NO EXISTE	TODOS MENOS EL PERSONAL RESPONSABLE	SI
MODIFICACIONES POR PERSONAL NO AUTORIZADO	3 A 4 CASOS AL MES	NINGÚN CASO	SI

ANEXO 9: AUDITORIA INTERNA

	AUDITORIA INTERNA (SGSI) SEGÚN NORMA ISO 27001									2017-04
N°	**ACTIVO**	**TIPO DE ACTIVO**	**VULNERABILIDAD**	**SISTEMA OPERATIVO**	**LICENCIA**	**AREA**	**OBSERVACIÓN**	**USUARIO**	**ESTADO**	**FECHA**

ANEXO 10: AUDITORIA INTERNA

	AUDITORIA INTERNA (SGSI) CONTROL DE ACCESOS								2017-04
N°	**RESGISTRO DE USUARIO**	**TIPO DE ACTIVO**	**GESTION DE PRIVILEGIOS**	**ADMINISTRADOR DE CONTRASEÑAS**	**LIMITE DE TIEMPO DE CONEXION**	**ACCESO A LA INFORMACION**	**OBSERVACIÓN**	**RIESGO**	FECHA

ANEXO 11: AUDITORIA INTERNA

	AUDITORIA INTERNA (SGSI) SEGURIDAD FISICA Y AMBIENTAL							2017-04
N°	**AREA DE SEGURIDAD**	**SEGURIDAD EN OFICINAS**	**CONTROLES DE ENTRADA**	**AMENAZAS DE INCENDIO**	**SEGURIDAD DE CABLEADO**	**MANTENIMIENTO DE EQUIPOS**	**MATERIALES INFAMABLES**	FECHA

ANEXO 12: AUDITORIA INTERNA

FORMATO DE ENTREGA DE USUARIOS APLICATIVOS (CARGO) JEFATURA DE SOPORTE				
N°	**ASESOR**	**APLICATIVOS**	**FIRMA**	**FECHA**

ANEXO 13: PLAN DE AUDITORIA INTERNA

FORMATO DE REQUERMIENTO (CARGO) JEFATURA DE SOPORTE				
FECHA	**PROVEEDOR**	**DESCRIPCIÓN**	**RESPONSABLE**	**N° DE REQUERIMEINTO**

ANEXO 14: ACCIONES CORRECTIVAS Y PREVENTIVAS

ACCIONES CORRECTIVAS Y PREVENTIVAS EN BASE AL CICLO PDCA (ISO 27001)					
HALLAZGO	**CONFORMIDAD**	**NO CONFORMIDAD**	**OBSERVADO**	**ACCIÓN CORRECTIVA**	**ACCIÓN PREVENTIVA**
Control de registros		NC		Se implementó registros de control por áreas	Se implementó registros diarios
Resposabilidades			OB	Se implementó responsables por áreas	Informes diarios
Fallas de los procesos		NC		Reparación y cambio de hardaware y software	Se realizó mantenimiento por periodos
Control de documentos		NC		Se habilitó Bitacora de documentos por tipo de incidencias	Revisión periódica de bitácoras
Capacitación			OB	Se creó área capacitación para personal	Evaluaciones periódicas
Comunicación Eficiente			OB	Nivel de seguridad mejorada	Cambio de claves periódicas
Copias de seguridad de Información		NC		Se instaló hardware para el almacenamiento de datos	Se realizaron Backup en todas las áreas
Redes de comunicaciones seguras		NC		Se implementó firewall y redes de comunicación inalámbricas encriptadas	Cambio de clave wifi periódico
Contraseñas de acceso de Empleados		NC		Disposición de claves de acceso a computadoras	Cambio de clave periódica
Antivirus Original		NC		Adquisición de antivirus Original	Actualizaciones constantes
Zonas seguras contra desastres naturales			OB	Señalizaciones de zonas seguras	Reemplazo de equipos inflamables

Tabla 29: Pre y Post de Incidencias

Incidencias Encontradas	Después de Implementación Norma ISO 27001
Baja Productividad	Aumento de Eficiencia y Productividad
Equipos averiados software y hardware	Permite la continuidad del negocio
Pérdida de Imagen	Reconocimiento por sus clientes
Aumento de costos	Gestión y reducción de costos
Pérdida de confianza	Aumento de la confianza por parte de Telefónica del Perú.
Incumplimiento de contratos	Cumplimiento de objetivos
Pagar penalidades	Reducción de penalidades
Perdida de Integridad	**Después de la Implementación**
Uso de cuentas no autorizadas	Sólo personal autorizado
Aplicaciones mal construidas	Revisión de aplicaciones
Fallas en los sistemas de aplicación	Revisión periódica
Uso de aplicaciones no autorizadas	Revisión periódica
Perdida de la disponibilidad	**Después de la Implementación**
Se encontró virus	Instalación de Antivirus Original
Fallas en la pc tanto software y hardware	Mantenimiento constante
Perdida de confidencialidad	**Después de la Implementación**
Debilidad en la configuración de dispositivos periféricos	Protocolos de configuración
Intrusión de hackers internos y externos	Instalación de Antivirus Original

Tabla 30: Detalle Económico de las pérdidas antes de la implementación

Detalle Económico	Perdida Antes	Perdida Después
Costo Renv. Headphone C/U 128,97	X40 = 5159	X4= 515,88
Costo Pc Reposición Hp C/U 2060,00 Soles	X12= 24723	X1= 2060,00
Costo Hombre(Service) 35,00 Soles X1h.	X40 = 1400	S/ -
Total	S/ 31.282,00	S/ 2.575,88
Reducción %		91,77%

PLAN DE VISITA

ATENTO DEL PERÚ

Nº SUBEXPEDIENTE	TIPO DE ACTIVIDAD	NORMA DE APLICACIÓN O REGLAMENTO	FECHA
2017/0449/SI/01	Certificación (AR)	UNE-ISO/IEC 27001:2014	**2017-04-03, 03 y 04**

Referencia: MNC/VGC

Fecha: 2017-04-03

DTC-001.17

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : RIN-PP-PR-02.02 Versión : 07 Fecha : 31-03-2017 Página : 1 de 1

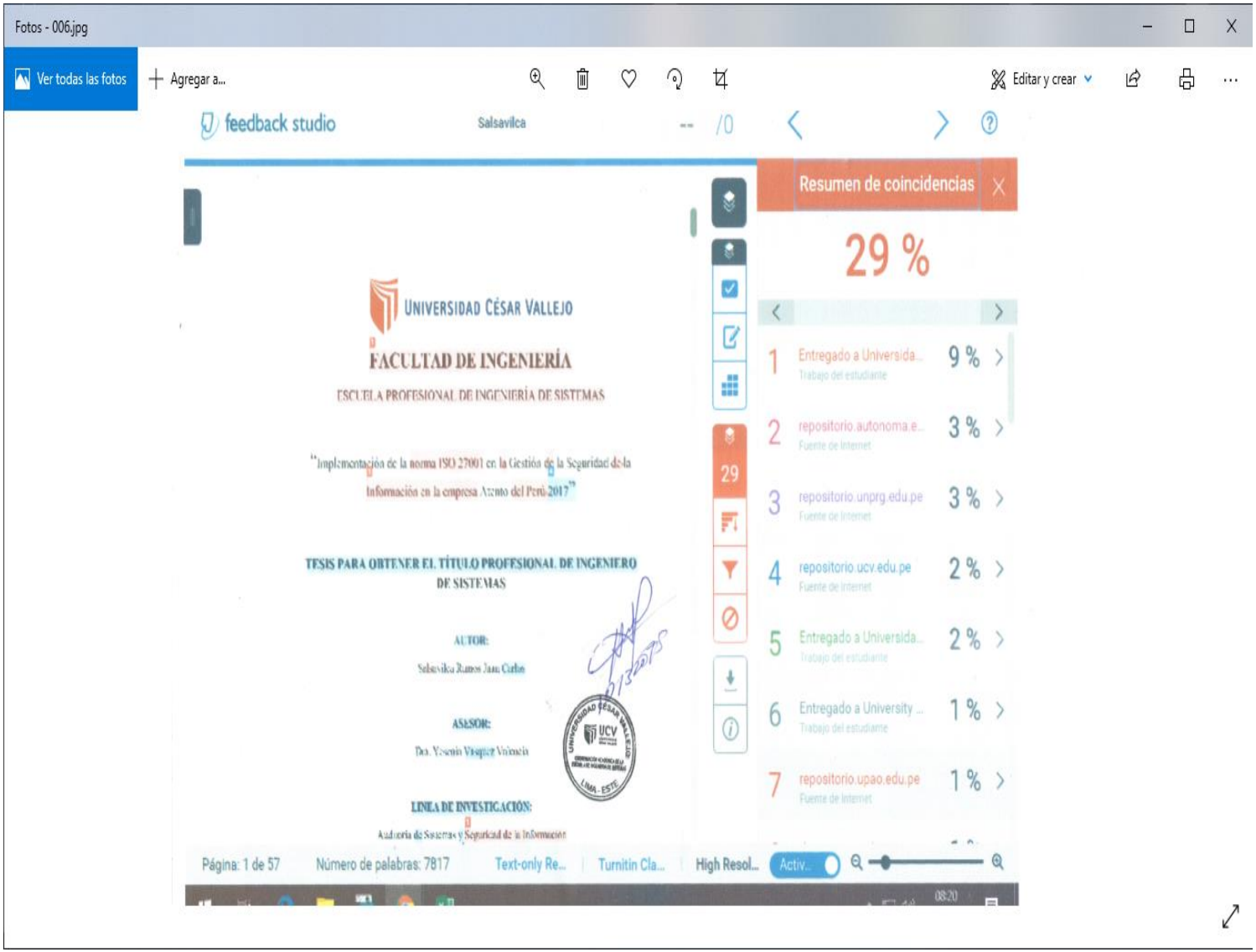
Yo, Dr. Hilario Falcón Francisco Manuel
docente de la Facultad Ingeniería y Escuela Profesional Ingeniería de Sistemas de la Universidad César Vallejo S.J. Lurigancho (precisar filial o sede), revisor (a) de la tesis titulada
"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la Empresa Atento del Perú 2017"
del (de la) estudiante Salsavilca Ramos Juan Carlos
constato que la investigación tiene un índice de similitud de 29 % verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lugar y fecha. Lima, San Juan de Lurigancho 16 Diciembre 2017

Firma
Dr. Francisco Manuel Hilario Falcón
DNI: 10132075

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado


Fotos - 006.jpg
Ver todas las fotos
Agregar a...
Editar y crear
feedback studio
Salsavilca
Resumen de coincidencias
29 %
UNIVERSIDAD CÉSAR VALLEJO
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017"
TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS
AUTOR:
Salsavilca Ramos Juan Carlos
ASESOR:
Dra. Yesenia Vásquez Valencia
LINEA DE INVESTIGACIÓN:
Auditoría de Sistemas y Seguridad de la Información
1 Entregado a Universida... 9 %
2 repositorio.autonoma.e... 3 %
3 repositorio.unprg.edu.pe 3 %
4 repositorio.ucv.edu.pe 2 %
5 Entregado a Universida... 2 %
6 Entregado a University ... 1 %
7 repositorio.upao.edu.pe 1 %
Página: 1 de 57
Número de palabras: 7817
Text-only Re...
Turnitin Cla...
High Resol...
Activ...

	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 07 Fecha : 31-03-2017 Página : 1 de 1

Yo Salsavilca Ramos Juan Carlos, identificado con DNI Nº 10721292, egresado de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, autorizo (X) , No autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado "Implementación de la Norma ISO 27001 en la Gestión de la Seguridad de la Información en la Empresa Atento del Perú 2017"; en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

FIRMA

DNI: 10721292

FECHA: 03 de Junio del 2019

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

La Escuela de Ingeniería de Sistemas
Dra Vasquez Valencia Yesenia

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

Salsavilca Ramos Juan Carlos

INFORME TÍTULADO:

" Implementación de la Norma ISO 27001 en la Gestión de la Seguridad de la Información en la Empresa Atento del Perú 2017

PARA OBTENER EL TÍTULO O GRADO DE:

Ingeniero de Sistemas

SUSTENTADO EN FECHA: 16 de Diciembre 2017

NOTA O MENCIÓN: 14

UNIVERSIDAD CESAR VALLEJO
UCV
COORDINACION ACADEMICA DE LA ESCUELA DE INGENIERIA DE SISTEMAS
LIMA NORTE

FIRMA DEL ENCARGADO DE INVESTIGACIÓN