

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



Presentado por

EBER JESÚS APAHUASCO SACCACO

**“EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA
INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC
APLICANDO LINEAMIENTOS ISO 27001”**

Asesor:

Dra. Cecilia Edith García Rivas Plata

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

ANDAHUAYLAS - APURÍMAC - PERÚ

2019

APROBACIÓN DEL ASESOR



APROBACIÓN DEL ASESOR

Quién suscribe:

Dra. Cecilia Edith García Rivas Plata, por la presente:

CERTIFICA,

Que, el Bachiller en Ingeniería de Sistemas, EBER JESÚS APAHUASCO SACCACO ha culminado satisfactoriamente el Proyecto de Tesis intitulado: "EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001" para optar el Título Profesional de Ingeniero de Sistemas.

Andahuaylas, 13 de Setiembre del 2019.

Dra. Cecilia Edith García Rivas Plata
Asesor

Bach. Eber Jesús Apahuasco Saccaco
Tesista

APROBACIÓN DEL JURADO DICTAMINADOR



APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS: "EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001"; para optar el Título Profesional de INGENIERO DE SISTEMAS, ha sido evaluada por el Jurado Dictaminador conformado por:

PRESIDENTE: DR. YALMAR TEMISTOCLES PONCE ATENCIO
PRIMER MIEMBRO: DR. JULIO CÉSAR HUANCA MARÍN
SEGUNDO MIEMBRO: MTR. JUAN JOSÉ ORÉ CERRÓN

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 04 del mes de setiembre de 2019.

Andahuaylas, 13 de setiembre de 2019.

DR. YALMAR TEMISTOCLES PONCE ATENCIO
PRESIDENTE DEL JURADO DICTAMINADOR

DR. JULIO CÉSAR HUANCA MARÍN
PRIMER MIEMBRO DEL JURADO DICTAMINADOR

MTR. JUAN JOSÉ ORÉ CERRÓN
SEGUNDO MIEMBRO DEL JURADO DICTAMINADOR

DECLARACIÓN JURADA DE AUTENTICIDAD



DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, **EBER JESÚS APAHUASCO SACCACO**, identificado (a) con DNI N° **45822700** de la Escuela Profesional de Ingeniería de Sistemas.

Declaro bajo juramento que el Informe Final de Tesis Titulado: EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001

Es auténtico y no vulnera los derechos de autor. Además, su contenido es de entera responsabilidad del autor (es) del proyecto, quedando la UNAJMA exenta de toda responsabilidad en caso de atentar contra la Ley de propiedad intelectual y derechos de autor.

Andahuaylas, 13 de setiembre de 2019

Firma

N° DNI: 45822700

E-mail: eber.jesus582@gmail.com

N° Celular: 983608542

ACTA DE SUSTENTACIÓN DE TESIS



Universidad Nacional José María Arguedas

Identidad y Excelencia para el Trabajo Productivo y el Desarrollo



FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

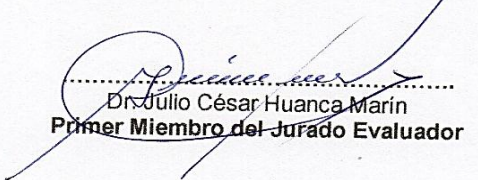
En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 12:00 horas del día 04 de setiembre del año 2019, se reunieron los docentes: Dr. Yalmar Temístocles Ponce Atencio, Dr. Julio César Huanca Marín, Mtr. Juan José Oré Cerrón, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001", cuyo autor es el Bachiller en Ingeniería de Sistemas **EBER JESÚS APAHUASCO SACCACO**, la asesora Dra. Cecilia Edith García Rivas Plata, con el propósito de proceder a la sustentación y defensa de dicha tesis.

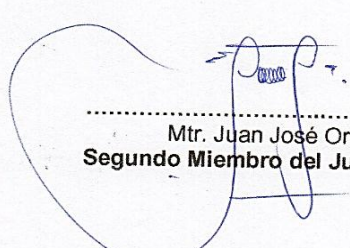
Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ**: aprobar por unanimidad al Bachiller en Ingeniería de Sistemas **EBER JESÚS APAHUASCO SACCACO**, obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
15	quince	bueno

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.


.....
Dr. Yalmar Temístocles Ponce Atencio
Presidente del Jurado Evaluador


.....
Dr. Julio César Huanca Marín
Primer Miembro del Jurado Evaluador


.....
Mtr. Juan José Oré Cerrón
Segundo Miembro del Jurado Evaluador

DEDICATORIA

Con mucho cariño y amor a mi Madre Daria Saccaco Galindo, quien ha estado conmigo siempre, por su sacrificio, por enseñarme a crecer y a que si caigo debo levantarme para ser mejor cada día, por apoyarme y guiarme, por ser la base que me ayudo a llegar hasta aquí.

A mi papá y a mis hermanos que son ellos quienes sobrellevaron mi tan cambiante estado de ánimo y fueron mi soporte ante todas las adversidades que tuve en este difícil camino; a mi amada esposa y a mi hija que son mi motor y motivo de superarme cada día y ser mejor de lo que fui ayer y por ultimo a mis compañeros y amigos, quienes sin esperar nada a cambio compartieron su conocimiento, alegrías y tristezas y a todas aquellas personas que durante mi etapa universitaria estuvieron a mi lado apoyándome y lograron que este sueño se haga realidad. Gracias.

AGRADECIMIENTO

En primer lugar, quiero agradecer a la Universidad Nacional José María Arguedas, por albergarme estos 5 años y hacer de mí un profesional competitivo, del mismo modo a todos mis docentes que me brindaron sus conocimientos para sobresalir día a día, y en especial al Ingeniero Edwin Octavio Ramos Velásquez, quien hoy no se encuentra entre nosotros, pero a quien llevamos siempre presente, por su incansable labor en lograr el éxito profesional en sus estudiantes.

A mi Madre por darme la vida y cuidarme.

A mis Hermanos, Esposa e Hija por su apoyo incondicional.

Agradezco también a mi asesora de tesis la Dr. Cecilia Edith García Rivas Plata, por brindarme la oportunidad de recurrir a su capacidad y conocimiento, así como también haberme tenido toda la paciencia del mundo para guiarme durante todo el desarrollo de la tesis.

ÍNDICE

APROBACIÓN DEL ASESOR.....	ii
APROBACIÓN DEL JURADO DICTAMINADOR.....	iii
DECLARACIÓN JURADA DE AUTENTICIDAD	iv
ACTA DE SUSTENTACIÓN DE TESIS	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
RESUMEN.....	xiv
ABSTRACT	xv
CHUMASQA.....	xvi
CAPÍTULO I: INTRODUCCIÓN	1
1.1. PROBLEMA DE LA INVESTIGACIÓN	2
1.1.1. REALIDAD PROBLEMÁTICA.....	2
1.2. FORMULACIÓN DEL PROBLEMA	6
1.3. OBJETIVOS.....	6
1.3.1. Objetivo General.....	6
1.3.2. Objetivos Específicos	6
1.4. JUSTIFICACIÓN	6
CAPÍTULO II: ANTECEDENTES.....	8
CAPÍTULO III: MARCO TEÓRICO	12
3.1. SEGURIDAD DE LA INFORMACIÓN	12
3.1.1. Objetivos de la Seguridad de Información	14
3.1.2. Sistema de gestión de la seguridad de la información	15
3.2. ISO 27001.....	17
CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN	21

4.1.	HIPÓTESIS DE LA INVESTIGACIÓN	21
4.1.1.	Hipótesis General	21
4.1.2.	Hipótesis Específicas.....	21
4.2.	OPERACIÓN DE VARIABLES	21
4.3.	MÉTODO DE LA INVESTIGACIÓN	22
4.4.	DISEÑO DE LA INVESTIGACIÓN	22
4.5.	TIPO Y NIVEL DE INVESTIGACIÓN	23
4.6.	POBLACIÓN Y MUESTRA	23
4.7.	TÉCNICAS DE ANÁLISIS DE DATOS.....	24
4.8.	ANÁLISIS A LA ORGANIZACIÓN DISAV SAC	25
4.9.	LISTA DE COTEJO PARA VERIFICACIÓN BASADAS EN LA ISO/IEC 27001	25
4.10.	PLANIFICACIÓN DE ENCUESTA PRE TEST Y POST TEST	26
4.11.	EVALUACIÓN DE LOS LINEAMIENTOS DE LA ISO 27001	27
	CAPÍTULO V: RESULTADOS.....	36
5.1.	INTERPRETACIÓN DE DATOS	36
	CAPITULO VI: DISCUSIÓN	44
	CONCLUSIONES	45
	RECOMENDACIONES.....	46
	REFERENCIA BIBLIOGRAFICA.....	47
	ANEXOS:	49
	ANEXO 01: Matriz de Consistencia	49
	ANEXO 02: Encuesta	50
	ANEXO 3: Solicitud de permiso para realizar trabajos de investigación.....	52
	ANEXO 4: Memorándum Informativo sobre la EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001	53

ANEXO 5: Acta de Conformidad de la capacitación realizada sobre EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001	54
ANEXO 6: Capacitación al personal que labora en Organización Disav SAC .	55
ANEXO 7: Fotografías de la encuesta realizada de la PRE y POST evaluación del sistema de seguridad	56

ÍNDICE DE TABLAS

Tabla 1. Operación de variables	21
Tabla 2. Cantidad de equipos tecnológicos	23
Tabla 3. Planificación de la encuesta de pre test y post test	26
Tabla 4. Prioridad de control elegido para su implementación	27
Tabla 5. Prioridad de control elegido para su implementación	28
Tabla 6. Calificación de las respuestas.....	36
Tabla 7. Calificación de las respuestas pre test	37
Tabla 8. Calificación de las respuestas post test	39
Tabla 9. Verificación de porcentaje de la minimización de la vulnerabilidad de la información	43

ÍNDICE DE GRÁFICOS

Gráfico 1. Índice de procesos y controles de la información antes y después de la aplicación	40
Gráfico 2. Índice de alteración de la información antes y después de la aplicación.....	41
Gráfico 3. Índice de costo de pérdida de la información antes y después de la aplicación.....	42

ÍNDICE DE FIGURAS

Figura 1. Implementación de Controles	3
Figura 2. Aceptación del IRTM	4
Figura 3. MIPYMES 2012.....	5
Figura 4. Etapas del SGSI.....	17
Figura 5. UNE-ISO/IEC 27001	18
Figura 6. Beneficios de las ISO	20
Figura 7. Nivel de seguridad de la información andes de la aplicación	38
Figura 8. Nivel de seguridad de la información después de la aplicación	40

RESUMEN

Durante estos últimos años la información se ha convertido en un activo muy importante y sensible dentro de las empresas y organizaciones, ya sea para gestionar la información y su seguridad o el adecuado uso de la misma, empleando normas y buenas prácticas existentes en el mercado.

Entonces para el caso de una empresa del rubro de distribución de bebidas, también aplica esta necesidad de proteger la información. Por ejemplo, uno de sus principales procesos es la Venta, está implicada información de gran importancia para la empresa, como clientes, productos, precios, etc., la cual debe estar protegida correctamente para evitar que dicha información se pierda o caiga en manos indebidas o de la competencia y así garantizar que se logren los objetivos del negocio.

La presente investigación tiene como objetivo evaluar la gestión de seguridad de la información basada en el estándar ISO 27001 en la Organización Disav Sac, pues tiene valiosa información que está expuesta por falta de aplicación de los controles de la seguridad de la información basadas en las buenas prácticas de la norma ISO/IEC 27001. Para poder llegar al objetivo se realizó análisis de la seguridad de la información en los terminales tecnológicos y personal que labora en la empresa a través de preguntas referidas al tema, luego se implementó todos los controles seleccionados a través de capacitación al personal y trabajos en terminales informáticos para garantizar buen manejo de información importante que todo trabajador almacena en su terminal, luego con los datos obtenidos se evaluaron con el software SPSS v.24 y los resultados obtenidos dan a conocer que el análisis fue adecuado ya que la vulnerabilidad de la información en la organización se minimizó satisfactoriamente; El presente trabajo es de tipo cuantitativo ya que se hizo una encuesta en la empresa para para conocer la necesidad de seguridad.

Palabras claves: Seguridad de la Información, ISO/IEC 27001, Análisis, Vulnerabilidad.

ABSTRACT

In recent years, information has become a very important and sensitive assets within companies and organizations, either to manage information and safety or the proper use of it using standards and best practices in the market.

So in the case of a company for the category beverage distribution, also applies this need to protect information. For example, one of its main processes is selling, is involved information of great importance for the company, such as customers, products, prices, etc., which must be protected properly to prevent such information from being lost or fall into the wrong hands or competition and so ensure that business objectives are achieved.

This research aimsevaluate the management of information security based on ISO 27001 standard in Disav Sac Organization, it has valuable informationwhich it is exposed for lack of implementation of security controls based information on best practices of ISO / IEC 27001. To reach the objective analysis of information security took place in the technological terminals and staff working in the company through questions regarding the issue, then all selected through staff training and work on computer terminals to ensure good management of important information that every worker stored in the terminal, then with the data controls implemented they were evaluated using SPSS v.24 software and results disclose that the analysis was appropriate because the vulnerability of information in the organization successfully downplayed;This paper is quantitative since a survey in the company to meet the need for security was made.

Keywords: Information Security, ISO / IEC 27001, Analysis, Vulnerability.

CHUMASQA

Kunan qina punchaw watakunapiqa kay willarikuykunaqa kay allí allin yacharikuykunamantaqa, suma sumaqtam recurirparin ancha niraq sumaqta kay empresa nisqan ukupiqa, chaynallataq kay organizaciones nisqankunapitaq qinallataq huk qawariyllawan kay gestionar nisqan willarikuykunamantapas, alli allintam waqaychasqa kanam, chaynallataq llankaqkunamanpas churarinachikmi kay normas nisqankunatapas allin puririnampaq kay mercado nisqankuna.

Chaynallataq kay empresa nisqan ukupiqa kay rubro nisqan yaku upyay aypurikuykunapiqa, anchatan waqaychanku sumaqllawan kay sumaq yachay willarikuykunataqa, qawarisqanman qina willakamun.

Kay huk allí allimnin sumaq ruwariynin venta nisqanta allintan waqaychanku.

Chaynallataq kay yachay willarikuykunaqa, sumaqtan puririchkan kay empresa nisqan ukupiqa, kay llapan rantiqninkunapaq, qinallataq kay productos nisqan lluksirinampaq qawarichkanku, precio nisqanta allinta rantinankupaq chaymi kay sumaq willarikuy yacharikuykunaqa, allin waqaychasqa kanan mana pipas qapirispayachanankupaq kay sumaq yachayninkuta, chayman qinan sumaq wiñayman kay negocio nisqan puririnampaq.

Chaymi kay sumaq investigación nisqamqa sumaqlлата huk qawariyllawan ruwakuchkan kay gestión seguridad nisqanta, kay sumaq willakuykunamanta kay estándar ISO 27001 nisqampi, chaynallataq kay Organización Disav Sac nisqapipas. Chaymi kay yachay willakuykunaqa munay waqaychasqa kanan mana wikapasqa kanampaq, kay control seguridad nisqan willakuykuna qawka kanampaq kay ISO/IEC 27001 nisqampi.

Chaymi allin chayarinampaq ruwarikurqa kay qillqapi huk qawarikuyllawan kay análisis nisqanqa, kay willakuykuna sumaq waqaychasqa kanampaq kay terminales tecnológicos ukupi, chaynallataq kay empresa nisqanpi, chaymi llankaqkunapas churarikuchkanku allin yuyaymanaykunata, chaymi akllarispachurarichkanku allin yachaykunata kay llankaqkunaman allinta llankanamkupaq chayman qina sumaqta wiñarichinampaq kay empresa nisqanta allinta willakuykunata qapirispanku.

Chaymi kay llapan yachay urqurisqakunawan ruwarikurqa churarispa kay Software SPSS v.24 nisqanta qinallataq kayqa willakamuckan llapan yachaykuna lluksirimusqanta chaynataqmi kay willakuykunaqa allinta lluksiriramun sumaqta puririnampaq.

Qinallataq kay sumaq qillqa llankasqayqa cuantitativo nisqanwanmi ruwarikurqa, chaymi puririmurqani empresa nisqan ukupi, qapirispay kay qillqana rapi encuesta nisqanwan, allinta riksirinaypaq imaynatan llankarinku kay seguridad nisqanta.

Musuq Sutikuna: Seguridad de la Información ISO/IEC27001, Analisis, vulnerabilidad nisqankuna

CAPÍTULO I: INTRODUCCIÓN

La información es un activo importante para cualquier empresa pública o privada, por lo que es necesario protegerla, para ello se han creado diferentes normas y leyes, las cuales permiten bajo un lineamiento protegerlo de cualquier ataque o amenaza.

Organización DISAV SAC es reconocida a nivel de la Región Apurímac por lo que es de gran importancia proteger su información, pero al igual que muchas empresas de nuestra región no saben cómo hacerlo, por lo que en esta tesis analizaremos y minimizaremos la vulnerabilidad de la información, mediante la norma ISO/IEC 27001.

La ISO/IEC 27001 es un estándar conocido que especifica los requisitos para establecer, implementar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI), extendida a las infraestructuras físicas, lógicas y organizativas donde se gestiona la información.

En esta tesis se evaluará el sistema de seguridad de la información en la Organización DISAV SAC, aplicando lineamientos ISO 27001, con el fin de minimizar la vulnerabilidad de la Información.

1.1. PROBLEMA DE LA INVESTIGACIÓN

1.1.1. REALIDAD PROBLEMÁTICA

Al transcurrir los años, los seres humanos continuamente encontramos la forma de guardar información, ya sea esta de una simple actividad o por querer tener siempre el recuerdo de algún hecho o suceso importante. Por todas las partes del mundo podemos encontrar información que pasa de generación en generación distorsionándose hasta a veces que se pierde con el tiempo, pero no toda la información se considera como un simple recuerdo, podemos encontrar información de nuestros pasados que nos dice cómo eran aquellos tiempos o hasta información de gran impacto para todo aquel que viva en este planeta. Sin duda alguna la información nos ha hecho desarrollarnos como personas a toda la humanidad entera, gracias a ella sabemos de dónde venimos y como hemos estado creciendo, siempre apoyándonos de información que nos dice lo que podemos o no hacer para lograr el éxito que buscamos, de igual forma, toda organización por más pequeña que sea, necesita saber su pasado, presente y la situación actual en la que se encuentra todo esto para poder afrontar el futuro en el campo sea cual sea en el que se desempeñe.

(Martinez, 2005) En el artículo “Importancia de los sistemas de información para las pequeñas empresas” nos dice que “la información es un recurso muy importante para toda organización, y el buen manejo de esta puede significar la diferencia entre el éxito o el fracaso para todos los proyectos que se emprendan dentro de un organismo que busca el crecimiento, el desarrollo y el éxito”.

(Fonceca, 2012) En el artículo “La información es el activo más importante de cualquier organización”, indica que primero se debe tener en cuenta el valor del activo más importante de toda empresa, institución u organización que en este caso es la información, se debe tener conciencia de la importancia que tiene la información en una empresa, muchas veces esta puede ser medida imaginariamente, suponiendo el impacto que

tendría esta, si llegara a desaparecer o lo que es peor, que llegara a caer en manos de la competencia o personas malintencionadas.

En general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.



Figura 1. Implementación de Controles

Fuente: 13ª Encuesta Global de Seguridad de la Información (EGSI) y comparativo en México.

(Información, 2012) Se investigó y se encontró que la tercera parte de las empresas tenía un programa (proyecto) bien establecido y que casi una cuarta parte había implementado un programa de ITRM (Gestión de riesgos en tecnologías de información) recientemente. El 30% de los encuestados se encontraba implementando o estaba considerando esta opción. Así mismo, es muy probable que las grandes empresas (700 o más empleados) hayan implementado un programa establecido de ITRM que las compañías con menos empleados, a continuación, se muestra de una manera más grafica lo indicado con respecto del IRTM.

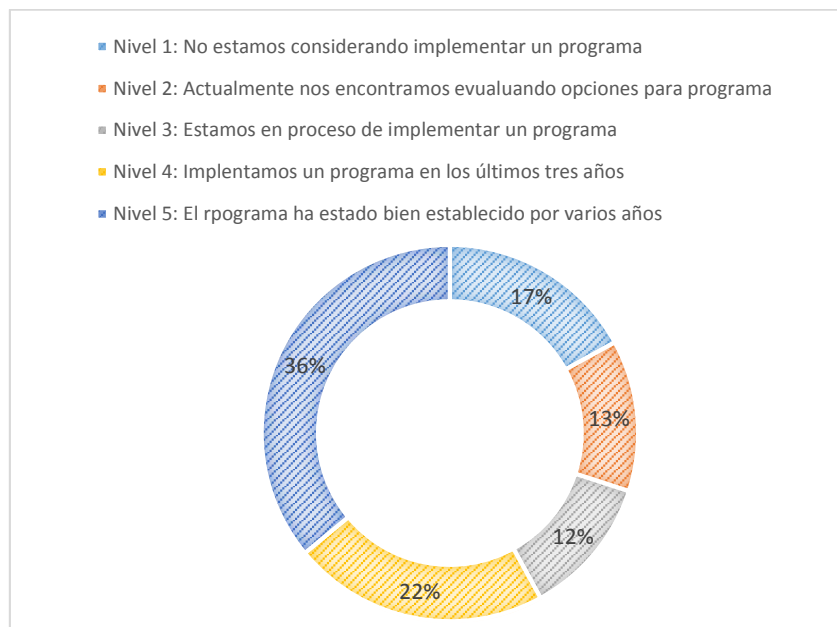


Figura 2. Aceptación del IRTM

Fuente: Encuesta de Agenda de Riesgo de TI

En España existe la Ley Orgánica de Protección de Datos, ley que desde su punto de vista es muy importante para las medidas de seguridad que van destinadas a todas las Organizaciones, empresas e instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información, siendo su finalidad principal proteger los datos de carácter personal evaluados de posibles incidencias que puedan provocar su pérdida, alteración u acceso no autorizado.

Por ello, la adopción de medidas técnicas y organizativas tendentes a garantizar la seguridad de los datos de carácter personal es una obligación básica que debe ser cumplida por todas las empresas que traten, almacenen y accedan a datos de carácter personal y empresarial.

En Perú, según el Registro Único de Contribuyente (RUC) de la Superintendencia Nacional de Administración Tributaria (SUNAT), en el 2012 se han identificado 1,345.390 micro, pequeñas y medianas empresas (MIPYMES) formales. Por distribución geográfica, el 72,4% de las MIPYMES se ubica en las regiones de la costa (el 52,0%se localiza en

Lima y el callao). La sierra concentra el 21,4% de las MIPYMES y solo el 6,2% se ubica en las regiones de la selva.

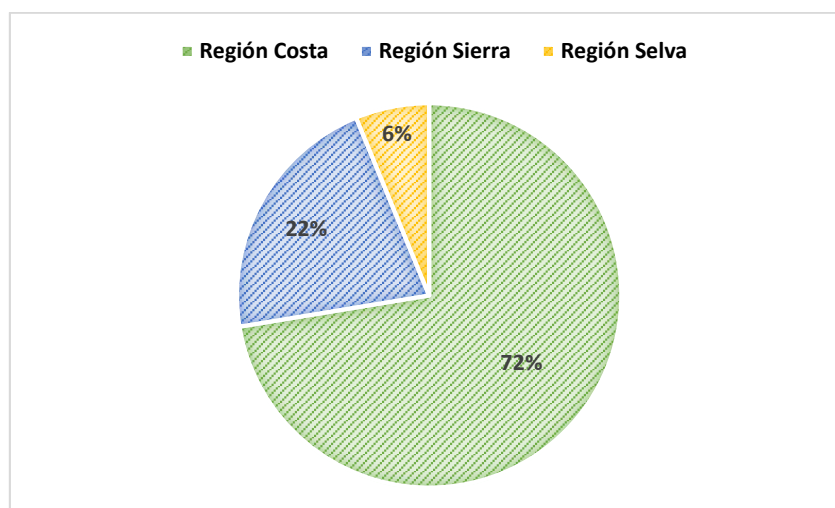


Figura 3. MIPYMES 2012

Fuente: Superintendencia Nacional de Administración Tributaria

Organización Disav SAC es una empresa dedicada a la venta y comercialización de bebidas no alcohólicas con más de 25 años en el mercado local, actualmente está ubicado en Curibamba – Andahuaylas, en esta empresa laboran 15 personas tanto en las áreas administrativas como en las áreas comerciales el número de terminales usados en Disav es el mismo ya que cada trabajador maneja un terminal tecnológico; lo que se necesita ahora es información oportuna y confiable, para tomar decisiones, para ello cuenta con un sistema de información no muy confiable, Pero a diferencia de otras organizaciones privadas no le da mucho interés al tema de seguridad informática.

A continuación, se describirá algunas deficiencias en la Organización Disav SAC:

- 1) Ausencia de una política de seguridad de la Información.
- 2) Ausencia de un plan de Gestión de Riesgo.
- 3) Inadecuado plan de la seguridad de la información.
- 4) Inapropiada administración de recursos informáticos.

- 5) Ausencia de la seguridad física de todo entorno tecnológico.
- 6) Inadecuada administración de las comunicaciones y operaciones.
- 7) Inadecuado control de acceso a la Información.
- 8) Inadecuada adquisición de sistemas de información, desarrollo y mantenimiento.
- 9) Inadecuada administración de los incidentes de seguridad de la Información.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo mejorar la seguridad de la información en la Organización Disav SAC?

1.3. OBJETIVOS

1.3.1. Objetivo General

Evaluar la gestión de seguridad de la información basada en el estándar ISO 27001 en la Organización Disav SAC.

1.3.2. Objetivos Específicos

- 1) Evaluar los procesos y controles de gestión de la seguridad de la información en la Organización Disav SAC.
- 2) Minimizar la alteración de la información en la Organización Disav SAC.
- 3) Reducir los costos originado por la pérdida de información.

1.4. JUSTIFICACIÓN

Con el pasar de los años hemos podido percibir el crecimiento acelerado de la tecnología y a su vez esto ha generado grandes problemas de vulnerabilidad en todo tipo de organizaciones, ya sea con inseguridad o riesgo de fraudes informáticos, virus informático, intrusión en la información hasta espionaje.

Este tipo de vulnerabilidades ha sido detonante para que las instituciones dedicadas a la venta de productos o ventas en general tomen medidas preventivas de seguridad para poder evitar que su información sea robada o modificada de manera tal que dañe la toma de decisiones en la parte administrativa.

El diseño de un sistema de seguridad de la información contribuirá y establecerá nuevas políticas de seguridad, normas y acciones para asegurar la información y mejorar la gestión, transmitiendo en los miembros de la institución la importancia y sensibilidad de la información y la seguridad.

Las instituciones que se dedican a venta de productos hoy en día necesitan sistemas de gestión de seguridad de la información para que estos a su vez ayuden en la obtención, procesamiento, almacenamiento y transmisión de la información segura.

Organización Disav SAC, cree que implementar un sistema de seguridad de la Información es demasiado esfuerzo, y está solo destinado a grandes empresas o mega corporaciones sin embargo es posible que en algunos casos aplicar unos pocos principios, en lugar de un Sistema de seguridad de la información completo, para conseguir mejoras significativas en la institución. Para esto en este proyecto de tesis finalmente, se considerará la norma ISO 27001, que es la norma más usada para establecer una correcta evaluación, la cual describe un código de buenas prácticas para la gestión de la seguridad de la información y su vez estos ayudaran en la correcta toma de decisiones en la parte administrativa con datos correctos, oportunos y seguros, logrando minimizar la alteración de información y reducir los costos originados en los mismos.

CAPÍTULO II: ANTECEDENTES

De acuerdo a lo mencionado por (Bermúdez Molina & Bailón Sanchez, 2015), en el análisis en seguridad informática y seguridad de la información basada en la norma ISO/IEC 27001 dirigido a una empresa de servicios financieros se realizó un análisis de las debilidades de seguridad para identificar los posibles riesgos que estaba afecto a la empresa, de esta manera conocer la situación actual referente a su seguridad y promover lineamientos que garanticen la confidencialidad, disponibilidad e integridad de información, las cuales están recomendadas en la norma; posterior a la evaluación se logró identificar que no poseía un manual de políticas de seguridad, que había áreas de sistemas, caja, crédito y cobranzas que tenían instructivos que la mayoría de transacciones se hacían de manera manual sin una adecuada normativa o compromiso formal indicando como, cuando y donde se podían realizar, entonces con la finalidad de obtener resultados reales de la situación de la empresa referente a temas de seguridad de la información se elaboró un cuadro de entrevistas a todo el personal directivo y estratégico que laboraba en la institución financiera de las áreas (Sistemas, Crédito, Cartera y Cobranzas) encontrándose un total de 13 entrevistados. Finalmente con la aplicación de la norma 27001 se elaboró un manual de políticas donde se detallaron los controles de seguridad acorde a la realidad y necesidades de la empresa permitiéndoles mejorar tres aspectos fundamentales como son confidencialidad, integridad y disponibilidad de la información y de esta forma mitigar riesgos existente así como reducir la posibilidad de ocurrencia de nuevos; todos estos controles de seguridad que se les recomendó empezaron a gestionar de una forma oportuna y adecuada, ya que por ser una norma ayuda en la gestión de la información, delineando cada paso a seguir para implementación de un sistema de gestión de seguridad de información que permite planear, implementar, monitorear y mejorar continuamente los procedimientos, métodos y proyectos.

De acuerdo a lo mencionado por (Guamán, 2015), en el diseño del sistema de gestión de seguridad de información para instituciones militares se encontró que el uso inadecuado de los recursos tecnológicos en estas instituciones hace que

tengan serios problemas de seguridad derivándoles un aumento desmesurado de delitos informáticos, para evitar todo ello el autor propuso analizar y evaluar los riesgos de seguridad en todos los ámbitos militares para de esta manera teniendo un conocimiento más amplio diseñar un sistema de gestión de seguridad de información militar; con la aplicación de esta norma se logró dar soporte a la gestión de seguridad de información de acuerdo a lo que pedía las instituciones militares pero para eso se debían realizar 2 documentos, el primero debía ser un manual de políticas de seguridad de información (elaborado por el área de tecnologías de información) y el segundo un plan de seguridad de información (El cómo se debía realizar las acciones o toma de decisiones); entonces se realizó una encuesta a 51 personas que laboraban en el área de TI para determinar cómo se encontraba la seguridad de la información en función a los riesgos, confiabilidad y la disponibilidad de la información y los datos; este levantamiento se realizó utilizando la norma ISO/IEC 27001:2005, en la cual se encuentran diferentes normas de control para mejorar en base al requerimiento de las instituciones militares. Determinándose la factibilidad operativa, técnica y económica para establecer un diseño de un sistema de gestión de seguridad de la información para la institución, verificándose que cumplían con todas las características logrando así que los usuarios estén en compromiso con la seguridad y el reconocimiento de las responsabilidades de la seguridad de la información.

Según (Espinoza Aguinaga, 2013), indica en el análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo que las compañías deben mejorar sus sistemas y capacitar a su equipo para encontrar y resolver problemas, ya que a veces no es nada barato y después del robo peor aún, las compañías deben indicar a sus clientes que la información está en riesgo, y deben gastar incluso más por no prevenir antes, entonces para que no ocurran estas acciones se inventarió los procesos del negocio y procesos de TI, se identificó y analizo los riesgos seguridad para luego elaborar un sistema de gestión de seguridad de información en base a la

norma 27001:2005; entonces luego de la adecuada evaluación se verificó la relación de procesos más importantes de la empresa cuyo propósito fue determinar y entender cada uno de ellos y calcular su impacto en tiempos que sean tolerables mientras se esté aplicando la norma 27001 y su obligatoria documentación según el sistema de gestión de seguridad de la información. Pero para todo esto se tuvo que realizar un levantamiento de información que permita documentar de forma adecuada al proceso de producción y sus subprocesos involucrados debido a que en el caso de las empresas de producción y comercialización de productos alimenticios de consumo masivo es ser el más importante; para ello se describió y presento a la empresa este proyecto para concientizar a los empleados que forman parte de la empresa sobre la adecuada gestión de la seguridad de información que es algo que debe estar ya incluido en la cultura organizacional de las empresas; y en todas ellas esta adecuada gestión no se lograría sin el apoyo de la alta gerencia como promotor activo de la seguridad en la empresa. Debe tenerse en cuenta que el diseño de SGSI que se presentó se adoptó a los objetivos planteados al proceso de producción, en el cual se basó el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de la empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán.

De acuerdo a lo mencionado por (Talavera Alvarez, 2015), en el diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013, nos dice que siempre se tiene presente el riesgo de fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información o por terceros que han accedido a ella mediante algún mecanismo de ataque, para poder contrarrestar estos problemas de intrusión se planteó elaborar documentación exigida por la norma 27001, elaborar metodologías de análisis, mapa de riesgos y declaración de aplicabilidad que a su vez ayuden al desarrollo de un sistema de gestión de seguridad de información en toda la institución basadas en dicha norma; luego de verificar estos puntos se logró desarrollar un sistema que fue acorde a esta institución denominado "HIS" que ayudo a proteger la información personal,

prevenir errores en la práctica de la salud y mantener funciones en todo el personal; Todo esto fue posible gracias a la aplicación de distintas normas como iso/dis 27799 extensión de la norma 27002, una serie de buenas prácticas y recomendaciones de la gestión de la seguridad de la información, entonces se pudo decir que es de vital importancia que se defina formalmente un comité de seguridad de la información tal que se encargue estrechamente de la gestión de riesgos de la institución presentando documentos de control tecnológicos que la institución pueda tener o requerir, siempre de la mano y aplicados por el SGSI.

CAPÍTULO III: MARCO TEÓRICO

Hay algunas definiciones importantes relacionadas al concepto de seguridad de información, que son útiles para una mejor comprensión de este proyecto de investigación.

3.1. SEGURIDAD DE LA INFORMACIÓN

Los términos de seguridad informática son usados continuamente por aquellas personas que siguen una misma finalidad de proteger la confidencialidad, integridad y disponibilidad de la información.

Según (Areitio, 2008), indica que la información con el pasar de los años ha pasado de utilizarse comunmente como cualquier dato en un activo muy fundamental para cualquier institución, por ello, se hace muy importante que las necesidades de seguridad sean potenciales, sean tenidas en cuenta y determinen todo tipo de desciones. Es decir los ambitos de de aplicación de seguridad de la información estan abarcados en el desarrollo, la integridad, la operación, la administración, el mantenimiento y la evolución de los sistemas; todos estos involucrados en el ciclo de vida de los productos o unidades de negocio.

Según (Paredes Fierro & Vega Noboa, 2011), nos dice que como resultado de la creciente inter conectividad en el ambiente de los negocios, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del

negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Según (Barrantes Porras & Hugo Barrera, 2012), nos explica que “La seguridad de información son aquellas medidas de prevención y reacción del hombre, de las instituciones y de todo sistema tecnológico que permitan salvaguardar y preservar la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.” En la seguridad de la información es importante puntar que su manejo esta establecido en la tecnología y debemos saber que es confidencial. Puede ser divulgada, robada, sabotada y mal utilizada, etc. La información ofrece acceso a ciertas etapas y se clasifica como:

- **Crítica:** Es indispensable para la operación de la empresa.
- **Valiosa:** Es un activo de la empresa muy valioso.
- **Sensible:** Debe ser conocida solo por personas autorizadas.

De acuerdo (Project Management Consultores de Proyectos, 2006), También nos indica que la defensa de la información de una clase amplia de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Entonces hoy en día toda etapa moderna se certifica por el mantenimiento de la seguridad, que exige una gestión global de la misma en todo el microsistema de información del mundo. Es decir en el desarrollo económico, social, estrategico, comercial, etc, no sera posible si no se ha implantado una completa gestión de la seguridad.

3.1.1. Objetivos de la Seguridad de Información

La seguridad en los sistemas de información es una disciplina en continua evolución, el fin principal de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión.

Objetivos principales de la seguridad

- a) **Disponibilidad:** Frecuentemente es uno de los objetivos de seguridad más importantes de toda organización o institución.
- b) **Integridad:** Se encarga de garantizar que la información contenga la consistencia deseada y no haya sido alterada de ninguna manera mientras se almacenan o transmiten.
- c) **Confidencialidad:** Continuamente esta después de la disponibilidad y la integridad, pues en términos de importancia esta es la clave ya que no todos están accesibles a esta.

Objetivos generales de la seguridad

- a) Conocer todos los riesgos asociados a una empresa u organización.
- b) Establecer un conjunto de requisitos de seguridad de acuerdo con los riesgos identificados, para satisfacer las necesidades del proceso.
- c) Transformar las necesidades de seguridad en guías o normas de seguridad, para integrarlas a los procesos.
- d) Establecer la confianza o garantía en la corrección y efectividad de los mecanismos de seguridad.

Finalmente, para poder garantizar que la seguridad de la información está gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial, ya que en el camino veremos cierto tipo de acontecimientos que dificultarán los mismos como pueden ser:

- **Evento de seguridad de información**

Sea cual sea el evento de seguridad de la información es una ocurrencia identificada del estado de sistema o servicio indicando una posible falla en la política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Incidente de seguridad de información**

Es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

3.1.2. Sistema de gestión de la seguridad de la información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el principal concepto sobre el que se conforma la norma ISO 27001. La gestión de la Seguridad de la Información se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa

Según (Gomez, 2012), es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

Según (Villena, 2006), la tarea de establecer y mantener las políticas de seguridad de información corresponde al administrador de seguridad de información, quien debe implementar procesos para lograr ello. La institución debe asegurar que estas políticas sean parte

integral de su administración. Se deben considerar como “documentos vivientes” que deben ser revisados con regularidad para asegurar se mantengan actualizados ante cualquier cambio (tecnológico, organizacional, de procesos, etc.) en la institución. Se debe formalizar la periodicidad de revisión de las políticas y los criterios para dicha revisión. A partir de acá, los estándares se revisan y modifican para direccionar los cambios en las políticas. Los procedimientos y guías se derivan de las políticas de seguridad. Las políticas de seguridad de información sirven a varios propósitos, estableciendo primariamente lo que está o no permitido. Además éstas deben alinearse apropiadamente a los objetivos de negocio. Algunos métodos para lograr este último propósito se citan a continuación:

- Determinar si las inversiones en seguridad de información son proporcionales o no con el perfil de riesgo de la institución y los objetivos de negocios.
- Determinar la clasificación de la información requerida para la institución, con la finalidad de implementar las políticas necesarias.
- Determinar si las políticas de seguridad han sido adecuadamente diseñadas, implementadas y reforzadas para proteger la información de la institución. Los enunciados de las políticas deben ser lo suficientemente genéricos de manera que no sea necesario cambiarlos con mucha frecuencia; ni se presten a interpretaciones ambiguas. No es apropiado tener políticas que sean tan específicas que tengan que ser reformuladas cada vez que cambia la tecnología.

Según (Barrantes Porras & Hugo Barrera, 2012), son conjunto de procedimientos, procesos y recursos que establecen las altas jerarquías con la consigna de monitorear, dirigir y controlar la seguridad de los activos de información y de esta manera asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007). Un sistema de Gestión de Seguridad de la información esta soportado

en cuatro grandes y continuas etapas para su mantención en el tiempo, las cuales son:

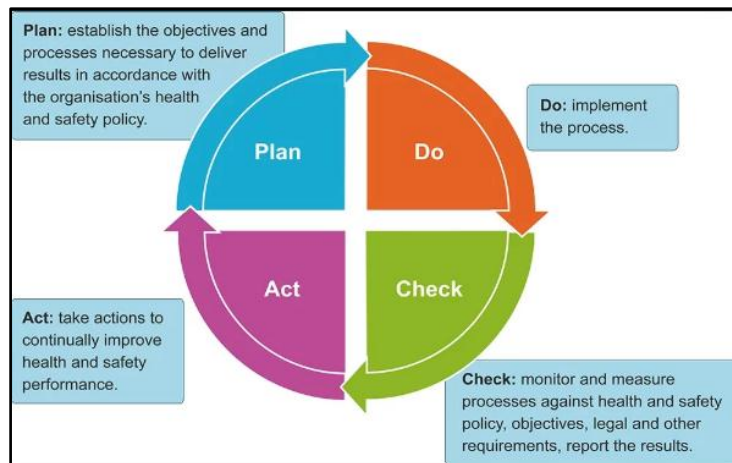


Figura 4. Etapas del SGSI

Fuente: Sistema de gestión de seguridad de la información

3.2. ISO 27001

Según (ISO, 2015), es el estándar más conocido en la familia que proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI). La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).

La Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel. En los entornos globalizados actuales, donde las transacciones de negocio (Empresas) llevan en su praxis el sufijo “electrónico”, esta prioridad se maximiza ante las especiales características del medio en que se desarrollan y sus riesgos asociados.

De acuerdo a lo mencionado por Poveda (2011), la norma fue publicada en el año 2007, En el año de 1995 el British Standard Institute (BSI) publica la norma BS7799 que es un código de buenas prácticas para la

gestión de la seguridad de la información. En vista de la gran aceptación de esta Norma, en 1998, el BSI publica la norma BS7799-2 que fue las especificaciones para los sistemas de gestión de la seguridad de la información. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en el año 2002 y denominada ISO/IEC 17799 en el año 2005.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27001 y en octubre del 2007 la norma ISO 27001 se adopta también por IEC. Con la publicación de la ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

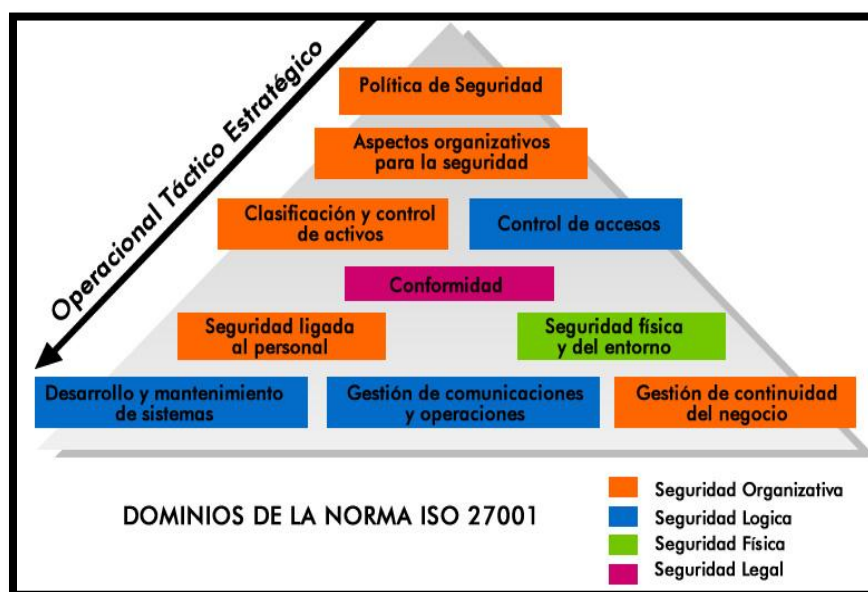


Figura 5. UNE-ISO/IEC 27001

Fuente: ISO

La norma ISO/IEC 27001 da a conocer las pautas para elaborar una metodología para un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del contexto de los riesgos identificados por la Organización.

Los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad. La norma ISO 27001 permite la elaboración de una metodología para:

- Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- Cómo se debe implantar el SGSI.
- Define los controles que deberán ser adaptados a la realidad de una organización para proceder a la implantación de la metodología que se estime conveniente.
- La ISO 27001 permite elaborar una metodología que adopte un proceso estructurado para implementar un SGSI.

Según (Sanchez, 2013), nos dice que ISO es el mayor desarrollador mundial de normas internacionales que nos garantizan que productos y servicios sean seguros, fiables y de buena calidad para todas aquellas empresas que desean reducir costos, disminuyendo los errores, aumentando la productividad e integrar nuevos mercados y facilitar el comercio mundial. Es decir una norma ISO es desarrollada por cierto grupo de expertos una vez que se haya establecido la necesidad de una norma en el mercado mundial, tan pronto sea necesario se llega a la votación si la aprobación o la desaprobación para convertirse en un estándar.

Principios fundamentales en la elaboración de las normas son:

1. Responden a una necesidad en el mercado.
2. Se basan en la opinión mundial de expertos.
3. Son desarrolladas a través de un proceso de múltiples partes.
4. Están basados en un consenso (ISO)

Normas Internacionales ISO		
Garantizan que los productos y servicios sean seguros, fiables y de buena calidad.	Reducen los costos, disminuyendo al mínimo los desechos y los errores, y aumentando la productividad.	Ayudan a las empresas a acceder a nuevos mercados, nivelar el campo de juego para los países en desarrollo y facilitar el comercio mundial libre y justo.

Figura 6. *Beneficios de las ISO*

Fuente: ISO

Según (Puma, 2017), explica aspectos organizativos para la seguridad, clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, gestión de incidentes de seguridad de la información, gestión de continuidad de negocio, conformidad y un conjunto de recomendaciones sobre qué medidas tomar en la empresa para asegurar los sistemas de información, el cual nos provee de una serie de dominios por medio de los cuales se logra la integración de las actividades y los objetivos que se deben considerar para lograr una correcta y exitosa implementación y mejora continua de los procesos. A diferencia de La ISO/IEC 27001 fundamenta en el modelo propuesto por W. Edwards Deming con el ciclo que lleva el mismo nombre, también conocido como PDCA (Plan-Do-Check-Act), ayuda a la organización no solo a obtener una certificación en materia de seguridad de la información para los procesos de negocio que conforman la organización.

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. HIPÓTESIS DE LA INVESTIGACIÓN

4.1.1. Hipótesis General

La evaluación del Sistema de Seguridad de la Información en la Organización Disav Sac Aplicando Lineamientos Iso 27001 minimizará la vulnerabilidad de la información.

4.1.2. Hipótesis Específicas

- El Sistema de Seguridad de la Información en la Organización DISAV SAC Aplicando Lineamientos ISO 27001 Evaluará los procesos y controles.
- El Sistema de Seguridad de la Información en la Organización DISAV SAC Aplicando Lineamientos ISO 27001 minimizará la alteración de la información en la Organización DISAV SAC.
- El Sistema de Seguridad de la Información en la Organización DISAV SAC Aplicando Lineamientos ISO 27001 Reducirá los costos originado por la pérdida de información.

4.2. OPERACIÓN DE VARIABLES

Tabla 1. Operación de variables

Variable independiente	Definición Conceptual	Dimensiones	Indicadores	Cuestionario	Tipo de variable
Lineamientos ISO 27001	Conceptos de lineamientos ISO 27001	Evaluar la seguridad de la información.	% de la evaluación de seguridad de la información	Ítems(1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7)	Ordinal

Variable dependiente	Definición Conceptual	Sub Dimensiones			
Evaluación del sistema de seguridad de la información	Concepto de sistema de seguridad de la información	Procesos y controles.	% de la evaluación de los procesos y controles	Ítems (1.1, 1.2, 1.3, 1.4, 1.5, 1.6)	Ordinal
		Alteración de la información.	% de la minimización de Alteración de la información.	Ítems (2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10)	Ordinal
		Costo de perdida de la información	% costo de perdida de la información	Ítems (3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7)	Ordinal

4.3. MÉTODO DE LA INVESTIGACIÓN

La investigación realizada pertenece al enfoque cuantitativo, se utilizó procesos estadísticos en este enfoque, para la estimación de los datos obtenidos se utilizó lista de cotejos que nos permitió examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo.

4.4. DISEÑO DE LA INVESTIGACIÓN

Una vez que se precisó el planteamiento del problema, se definió el alcance inicial de la investigación y se formuló las hipótesis, se visualizó de la manera práctica y concreta para contestar las preguntas de investigación, además se cumplió con los objetivos fijados. Esto implica seleccionar o desarrollar uno o más diseños de investigación y aplicarlos al contexto particular de su estudio.

Pre experimental: El pre experimentales es el diseño de un solo grupo para pre prueba y post prueba se caracterizan porque a un grupo se le aplica una prueba previa al estímulo o tratamiento experimental, después

se le administra el tratamiento y finalmente se le aplica una prueba posterior al estímulo.

Ge: O1 ----- X ----- O2

Donde:

Ge: Es el grupo experimental donde se hará la investigación.

O1: Pre test es la evaluación antes proyecto

O2: Post test es la evaluación después del proyecto.

X: Es el variable independiente del proyecto

4.5. TIPO Y NIVEL DE INVESTIGACIÓN

El presente trabajo está clasificado como un tipo de investigación aplicada, este tipo de investigación está encargado en resolver problemas

El nivel explicativo porque se evaluará el efecto de la variable independiente sobre la variable dependiente y probar hipótesis

4.6. POBLACIÓN Y MUESTRA

Son cada uno de los terminales informáticos (host) usados en la Organización DISAV SAC, a continuación, se detalla:

Tabla 2. Cantidad de equipos tecnológicos

EQUIPO	SO	CANTIDAD
PCs	Windows 7	2
Laptops	Windows 7	3
Celulares	Android	10
Total		15

Fuente: Elaboración propia

La población y la muestra es la misma ya que la Organización Disav Sac, es una empresa pequeña, tal como se observa en la tabla N° 2.

Se empleó el muestreo no probabilístico para el presente trabajo.

Técnicas e instrumentos de acopio de datos.

Observación: se evaluó aspectos cuantitativos y cualitativos, que junto a la lista de cotejos permitió a la recolección de datos estableciendo contacto con las unidades de observación

Se denomina lista de cotejos al conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población.

Lista de cotejo: se utilizó en la organización Disav Sac, debido a su versatilidad que permitió utilizarlo como instrumento de investigación.

4.7. TÉCNICAS DE ANÁLISIS DE DATOS

Se realizó visitas a la organización DISAV SAC ingresando a sus instalaciones para la recolección de datos y aplicación de un cuestionario el cual contiene 23 preguntas para medir la vulnerabilidad de la información.

Los datos recolectados a través de la encuesta se procesarán en el software estadístico SPSS V24, estos serán sometidos a diversas pruebas estadísticas de carácter descriptivo e inferencial, y serán aplicados para dar respuesta a los objetivos específicos e hipótesis planteadas en el presente trabajo de investigación

Prueba T-Student

La prueba de T-Student se utilizó para la validación de la hipótesis de la investigación con un nivel de confianza de 95%, con la finalidad de evaluar si los resultados obtenidos de la investigación el pre y post prueba se aceptan significativamente.

Formula de T-Student

$$T = \frac{\bar{X} - u}{\frac{S}{\sqrt{n}}}$$

Donde:

\bar{x} = Media del grupo experimental

s = Desviación estándar del grupo experimental

n = Tamaño de muestra del grupo experimental

μ = Media poblacional

Para procesamiento de los datos obtenidos de la encuesta en nuestro objeto de estudio se empleó el Software estadístico SPSS v.24 usando la prueba de T-student y también se utilizó el software Microsoft Excel 2013 para la realización de gráficos.

4.8. ANÁLISIS A LA ORGANIZACIÓN DISAV SAC

Los resultados obtenidos en la situación actual sobre la seguridad de la información ayudarán a la Organización Disav Sac en la implementación de la Norma ISO/IEC 27001 que mitigará las vulnerabilidades y pérdidas de la información importante que se ha ocurrido hasta el momento.

Con el fin de verificar la seguridad de la información, se realizó una primera encuesta a los todos los trabajadores y también se revisó todos los terminales tecnológicos donde se tiene información importante, fue de muy valiosa la ayuda del Líder de Operaciones para el análisis veras de la situación actual de la Organización Disav Sac.

La principal área analizada sobre la seguridad de la información fue el Área Comercial, por ser la oficina donde se almacenan la mayor cantidad de información que tiene la organización, también se analizó las áreas como Caja, Almacén, Recursos Humanos y Administración.

4.9. LISTA DE COTEJO PARA VERIFICACIÓN BASADAS EN LA ISO/IEC 27001

En esta etapa se usó los lineamientos de la norma ISO/IEC 27001 y se procedió a elaborar un cuestionario con preguntas seleccionadas según los indicadores que estaban orientadas a minimizar la vulnerabilidad de la información.

4.10. PLANIFICACIÓN DE ENCUESTA PRE TEST Y POST TEST

La revisión de los terminales se hizo previa coordinación con el personal de cada terminal, con la finalidad de obtener resultados reales de la situación actual de la seguridad de la información.

Con la colaboración del Líder Comercial y Logístico se programaron un total de 15 encuestas que a continuación se detallan por áreas y la fecha de primera encuesta realizada al personal que usa terminal tecnológico.

Tabla 3. Planificación de la encuesta de pre test y post test

Fecha de encuesta antes de la aplicación	Fecha de encuesta después de la aplicación	Áreas Encuestadas	Terminal que se usa	Cantidad de terminales
25/02/2019	05/07/2019	Administración, Área Comercial, Caja, Almacén, Recursos Humanos	Pcs, Laptops, Celulares	15
Total				15

Se observa que se tiene un total de 15 terminales tecnológicos, cantidad poblacional, cada terminal tecnológico es utilizado por un trabajador de la organización, el cual nos sirvió para realizar un análisis de pre test y post test del estudio.

Para esta evaluación se presentó una solicitud de permiso al líder comercial y logístico de la organización para proceder a evaluar cada terminal tecnológico con la ayuda del personal encargado utilizando como guía la lista de cotejo.

4.11. EVALUACIÓN DE LOS LINEAMIENTOS DE LA ISO 27001

En la tabla que se muestra a continuación, detalladamente todos los controles seleccionados del ISO/IEC 27001: 2015 para la Organización DISAV SAC que permitirá mejorar significativamente en la toma de decisiones, donde cada control es necesario implementar primero de acuerdo a su prioridad.

Tabla 4. Prioridad de control elegido para su implementación

Prioridades	Detalle
Primario	Son los lineamientos de la ISO 27001 que su implementación es de gran importancia en la organización.
Secundario	Son los lineamientos de la ISO 27001 que se puede implementar más adelante.

Tabla 5. Prioridad de control elegido para su implementación

5	Políticas de la seguridad de la información.		Prioridad
5.1	Dirección de la gerencia para la seguridad de la información.		
5.1.1	Políticas de la seguridad de la información.	<p>Organización Disav sac deberá tener las políticas de la seguridad de la información definido y aprobada por la alta gerencia, comunicando a los empleados.</p> <p>Las políticas de la seguridad de la información deberían ser revisadas por los encargados que conoce el tema para garantizar que sigue siendo adecuado, suficiente y eficaz.</p>	Primario
6	Aspectos organizativos de la seguridad de la información.		Prioridad
6.1	Organización interna.		
6.1.1	Asignación de responsabilidades para la seguridad de la información.	<p>Debería tener definidas y asignadas formalmente a un responsable de seguridad de la información capacitada.</p> <p>Capacitar al trabajador sobre sus tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.</p>	Secundario

		Es importante que todos el personal conozcan quien es el responsable de la seguridad de la información de tal forma que pueda saber a quién dirigirse oportunamente en casos de seguridad.	
6.1.2	Contacto con grupos de interés especial.	Es definitivamente muy importante y necesario tener contactos con grupos o empresas que aporten conocimientos referidos a la seguridad de la información. Todos los trabajadores en coordinación del responsable de la seguridad de la información deberán tener un compromiso de confidencialidad y no divulgación de la información que cuenta en su terminal informático.	Primario
6.2	Dispositivos para movilidad y teletrabajo.		
6.2.1	Política de uso de dispositivos para movilidad.	Debería tener medidas de la seguridad adecuadas para la protección de riesgos en uso de los recursos informática móvil y telecomunicaciones. Todos los terminales tecnológicos móviles deberían ser autorizados por el encargado de la seguridad de la información para el uso adecuado de la información con el fin de minimizar la divulgación de o la pérdida de la información vital que se pueda tener.	Primario
6.2.2	Teletrabajo.	Debería ingresar solo el personal autorizado al dispositivo móvil el cual es autorizado para realizar algún trabajo referido a la institución para evitar algún robo luego divulgación de la información vital, que contiene el dispositivo, debería ser uso específico del trabajador en bien de la institución, la implementación de las nuevas tecnologías de la información, ya que la institución que contrata personal que puede	Primario

		hacer trabajos a distancia (teletrabajo) está obligada a disponer de equipos adecuados para poder realizar un trabajo ágil.	
7	Seguridad de los recursos humanos.		Prioridad
7.1	Durante la contratación.		
7.1.1	Responsabilidades de gestión.	<p>La dirección debe exigir que los empleados contratistas y usuarios de terceras partes tener en cuenta la seguridad de la información.</p> <p>El personal que labora en la institución debe ser capacitado para mantener la reserva o confidencialidad de la información durante y después de su contrata.</p> <p>Todo trabajador debe tener compromiso y responsabilidad de no divulgar, ni copiar parcial o totalmente la información que se proporcione.</p>	Secundario
8	Gestión de activos.		Prioridad
8.2.3	Manipulación de los activos.	Se deberían tener en cuenta los procedimientos para la manipulación de los activos acorde con el esquema de clasificación de la información específicamente el uso de la información de cada trabajador en sus respectivas áreas, también cada trabajador debe ser responsable de su información evitando que sea manipulada por otro trabajador que podría ser perjudicial.	Primario
9	Control de accesos.		Prioridad

9.1	Requisitos de negocio para el control de acceso.		
9.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos de la institución y de la seguridad para el acceso de cada persona al área que no le corresponde. A las oficinas solo debe ingresar personal autorizado con el fin de evitar extracciones o modificación de la información confidencial	Primario
9.1.2	Control de acceso a las redes y servicios asociados.	Todos los accesos a cualquier equipo no designado debe ser autorizados por el encargado	Primario
9,2,5	Revisión de los derechos de acceso a la información.	Los propietarios de los activos principalmente equipos tecnológicos deberían revisar y verificar con regularidad la conformidad del activo más valioso que es la información.	Secundario
9.3.1	Uso de información confidencial para la autenticación.	Se debería exigir a los trabajadores la aplicación de las buenas prácticas de seguridad de la información y el uso de la información confidencial para la autenticación. El encargado de la cada una de las áreas de la institución deberá ser capacitado sobre la información confidencial para evitar la divulgación y tener mayor confianza en la toma de decisiones.	Primario
9.4	Control de acceso a sistemas y aplicaciones.		

9.4.3	Gestión de contraseñas de usuario.	<p>La asignación de contraseñas se debe controlar a través de un proceso formal de gestión por el encargado.</p> <p>Cada usuario de la computadora o dispositivo móvil de la institución deberá cambiar con frecuencia su contraseña para evitar ciertas alteraciones de la información confidencial almacenada.</p>	Primario
10	Cifrado.		Prioridad
10.1	Controles criptográficos.		
10.1.2	Gestión de claves.	<p>Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.</p> <p>Toda la clave designada a cada trabajador debería ser descifradas o difícil de comprender con el propósito de que los mensajes enviados lleguen sin alteraciones.</p>	Secundario
11	Seguridad física y ambiental.		Prioridad
11.1	Áreas seguras.		
11.1.1	Perímetro de seguridad física.	La Organización debería utilizar perímetros de seguridad tales como paredes, puertas de acceso, ventanas, y otros para proteger las áreas que contienen información.	Secundario

		Después de la finalización de día el trabajador debe estar 100% seguro que nadie más pueda ingresar a esa área.	
11.1.2	Controles físicos de entrada.	Las áreas de acceso deberían estar protegida para asegurarse que solo personal autorizado pueda ingresar.	Primario
11.1.4	Protección contra las amenazas externas y ambientales.	Se debería diseñar y aplicar protecciones físicas contra daño por inundación, terremoto, incendio, y otras formas de desastre natural o artificial que podría afectar la alteración o pérdida de la información. Los equipos donde se almacenan información deben estar ubicados o protegidos para reducir el riesgo debido a amenazas.	Primario
11.2	Seguridad de los equipos.		
11.2.3	Seguridad del cableado.	El cableado de energía y de telecomunicaciones en la Organización debe estar bien protegidos contra cualquier daño y en caso de alguna falla de internet el trabajador deberá comunicar al encargado para su pronta verificación y solución.	Secundario
11.2.4	Mantenimiento de los equipos.	Los equipos que están en utilización que contienen información vital deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	Primario
11.2.5	Salida de activos fuera de las dependencias de la empresa.	Los equipos tecnológicos, la información o el software no se deberían retirar del sitio sin previa autorización por el encargado de la seguridad de la información.	Primario

11.2.8	Equipo informático de usuario desatendido.	Un equipo informático desatendido primeramente debería ser autorizado por el encargado para ser utilizado, luego el usuario deberá asegurarse que cuenta con la protección adecuada.	Primario
12	Seguridad operativa.		Prioridad
12.2	Protección contra código malicioso.		
12.2.1	Controles contra el código malicioso.	<p>Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los trabajadores.</p> <p>El antivirus debería ser instalado solo por el personal autorizado de la institución</p> <p>Para garantizar la continuidad del trabajo es necesario realizar monitoreo de todas las PCs contra el ingreso de algún malicioso que puede perjudicar.</p>	Primario
12.3	Copias de seguridad.		
12.3.1	Copias de seguridad de la información.	<p>Como toda información es importante para una empresa se debería hacer copias de respaldo(backup)</p> <p>Cada trabajador es responsable de toda información que tiene en su terminal tecnológico que labora, por lo tanto el encargado de la institución deberá capacitar como hacer la copia de respaldo de la información, esta copia deberá realizar</p>	Primario

		frecuentemente para no perder alguna información en caso de que se dañe o se malogra el terminal tecnológico.	
12.4	Registro de actividad y supervisión.		
12.4.2	Protección de los registros de información.	Se debería proteger contra posibles alteraciones y accesos no autorizados a la información de los registros. En el intercambio de la información deber ser considerado en controles de seguridad que permitan garantizar la integridad y confidencialidad de los datos físicos o lógicos, pues si no se consideran los controles necesarios, este intercambio podría considerarse como un mecanismo de fuga o alteración de información.	Secundario
12.6	Gestión de la vulnerabilidad técnica.		
12.6.2	Restricciones en la instalación de software.	Cualquier software deberá ser instalado por el encargado de la organización o un trabajador autorizado.	Secundario
13	Seguridad en las telecomunicaciones.		Prioridad
13.2	Intercambio de información con partes externas.		
13.2.4	Acuerdos de confidencialidad y secreto.	se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información	Primario

CAPÍTULO V: RESULTADOS

5.1. INTERPRETACIÓN DE DATOS

En la encuesta realizada, por cada respuesta seleccionada se colocó un puntaje según la siguiente tabla.

Tabla 6. Calificación de las respuestas

Respuestas	Calificación	Detalle
No	0	Riesgo alto
Parcialmente	1	Está en riesgo
Si	2	No tiene riesgo

Fuente: Elaboración propia

a) Índice de la evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001, donde.

T = Terminal tecnológico

NP = Número de pregunta

C = Calificación

En la siguiente tabla se muestran los resultados del pre test:

Tabla 7. Calificación de las respuestas pre test

Resultados de la Evaluación de la seguridad de la Información en la Organización DISAV SAC																											
Dimensiones	Procesos y Controles						C	Alteración de la Información										C	Costo de Perdida de la información							C	Sub Total
Preg Terminal	1	2	3	4	5	6		1	2	3	4	5	6	7	8	9	10		1	2	3	4	5	6	7		
T01	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T02	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T03	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T04	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T05	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T06	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T07	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T08	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T09	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T10	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T11	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T12	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T13	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T14	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
T15	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	0	2	0	0	1	1	0	0	0	2	5
	Calificación de Pre Test						15	Calificación de Pre Test										30	Calificación de Pre Test							30	75

Fuente: Elaboración propia

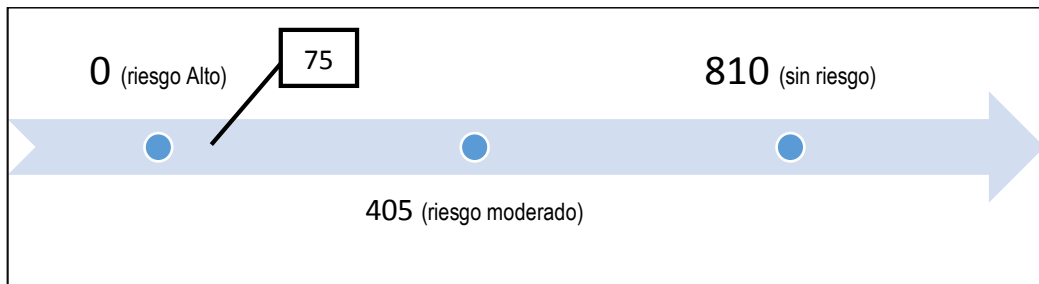


Figura 7. Nivel de seguridad de la información antes de la aplicación

Fuente: Elaboración propia

En la figura 7 se muestra la línea de riesgo en la que se encuentra la organización DISAV SAC, después de la evaluación del sistema de seguridad de la información aplicando lineamientos ISO 27001, donde 0 es la calificación mínima que significa que la organización no cuenta con ningún lineamiento para salvaguardar su información, 810 la calificación máxima que significa que la organización cumple con todos los lineamientos de la seguridad de la información y 405 es la calificación mediana que es el punto medio entre 0 y 810, podemos notar que la organización tiene una calificación de 75 por lo que se encuentra entre 0 y 405, lo que nos permite interpretar que la organización tiene conocimiento de algunos lineamientos para la seguridad de la información pero no es mínima, poniendo en riesgo la información de la organización.

Tabla 8. Calificación de las respuestas post test

Resultados de la Evaluación de la seguridad de la Información en la Organización DISAV SAC																												
Dimensiones	Procesos y Controles						C	Alteración de la Información										C	Costo de Perdida de la información							C	Sub Total	
	Terminal	Preg	1	2	3	4		5	6	1	2	3	4	5	6	7	8		9	10	1	2	3	4	5			6
T01		2	1	1	2	2	2	10	1	1	2	1	2	2	1	1	2	2	15	2	2	1	2	1	2	1	11	36
T02		2	1	1	2	2	2	10	1	1	2	1	2	2	1	1	2	2	15	2	2	1	2	1	2	1	11	36
T03		2	1	1	2	2	2	10	1	1	2	1	2	2	1	1	2	2	15	2	2	1	2	1	2	1	11	36
T04		2	1	1	2	2	2	10	1	1	2	1	1	1	1	1	2	12	2	2	1	2	1	2	1	11	33	
T05		2	1	1	2	2	1	9	1	1	2	1	1	2	1	1	2	13	2	2	1	2	1	2	1	11	33	
T06		2	1	1	1	2	2	9	1	0	2	0	1	2	1	1	2	12	2	2	1	2	1	2	1	11	32	
T07		2	1	1	1	1	2	8	1	1	2	0	1	2	1	1	2	13	2	2	2	2	1	2	1	12	33	
T08		2	1	1	2	1	2	9	1	1	2	1	2	2	1	1	1	14	2	2	1	2	2	2	1	12	35	
T09		2	1	1	2	2	2	10	1	0	2	1	2	1	1	1	2	13	2	2	1	2	1	1	1	10	33	
T10		2	1	1	1	2	2	9	1	1	2	1	1	2	1	1	1	13	2	2	2	2	2	2	1	13	35	
T11		2	1	1	2	2	2	10	1	0	2	1	2	2	1	1	1	13	2	2	1	2	1	1	1	10	33	
T12		2	1	1	2	2	1	9	1	0	2	1	2	2	1	1	2	14	2	2	2	2	1	2	1	12	35	
T13		2	1	1	1	1	2	8	1	1	2	0	2	2	1	1	1	13	2	2	2	2	1	2	1	12	33	
T14		2	1	1	2	2	2	10	1	1	2	1	2	1	1	1	2	14	2	2	1	2	2	2	1	12	36	
T15		2	1	1	2	2	2	10	1	1	2	1	1	1	1	1	2	12	2	2	1	2	1	2	1	11	33	
		Calificación de Post Test						141	Calificación de Post Test										201	Calificación de Post Test							170	512

Fuente: Elaboración propia

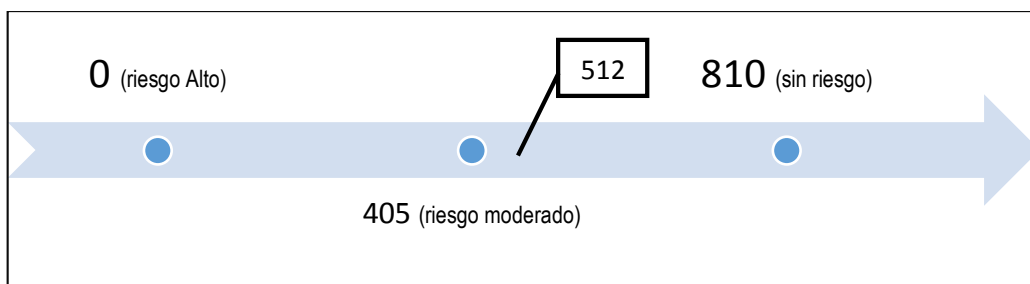


Figura 8. Nivel de seguridad de la información después de la aplicación

Fuente: Elaboración propia

Después de hacer el alcance de la evaluación y sensibilizar al personal de la organización se realizó otra evaluación de los terminales, consiguiendo que la Organización tenga la calificación de 512, logrando la minimización de riesgo de pérdida de información, siendo un logro ya que al aplicar algunos lineamientos de la ISO 27001, están salvaguardando un activo muy importante en la Organización.

a) Aplicación de los procesos y controles de la ISO 27001.

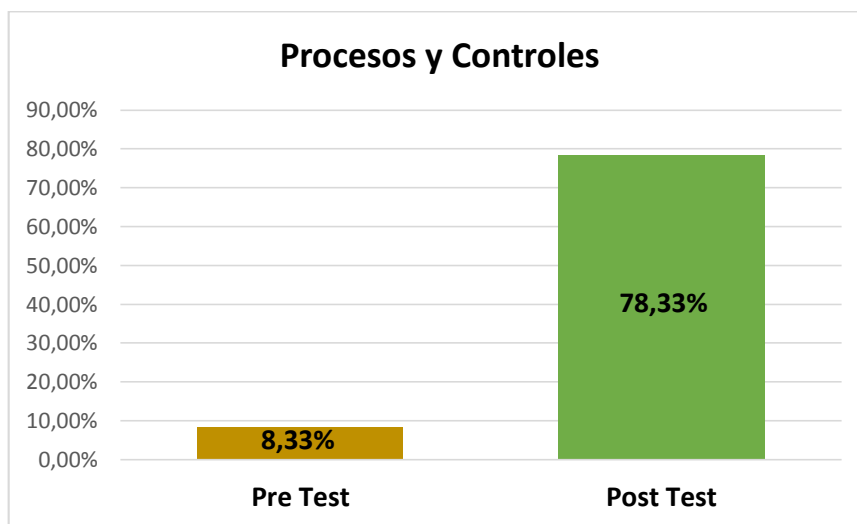


Gráfico 1. Índice de procesos y controles de la información antes y después de la aplicación

Fuente: Elaboración propia

Interpretación: En el gráfico N°1, se observa que la implementación de los procesos y controles en la Organización se encontraba en un 8.33% y

que después de la Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001, se implementaron los procesos y controles en un 78.33% mejorando un 70%.

b) Aplicación de la alteración de la información de la ISO 27001.

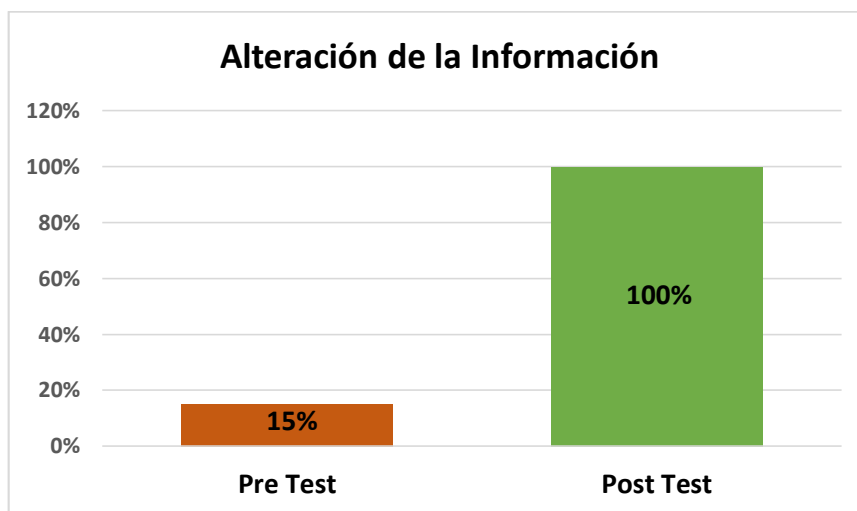


Gráfico 2. Índice de alteración de la información antes y después de la aplicación

Fuente: Elaboración propia

Interpretación: En el gráfico N°2, se puede observar que el estado de la alteración de la información se minimizó significativamente en un 85% después de la Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001.

c) Aplicación del costo de pérdida de la información de la ISO 27001.

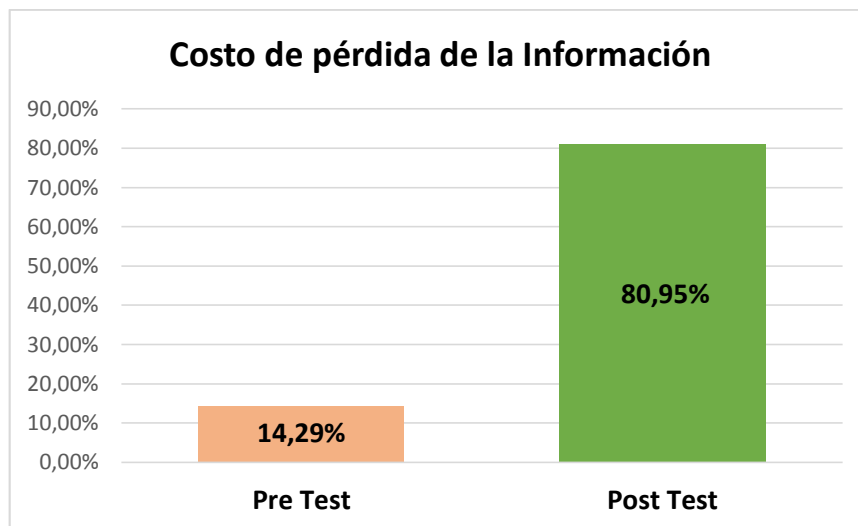


Gráfico 3. Índice de costo de pérdida de la información antes y después de la aplicación

Fuente: Elaboración propia

Interpretación: En el gráfico N°3, se observa que el costo por la pérdida de la información antes de la evaluación el estado de la amenazas de la información minimizó significativamente en un 66.66% después de la Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001.

Tabla 9. Verificación de porcentaje de la minimización de la vulnerabilidad de la información

Dimensión	Puntaje pre test	Pre test	Puntaje post test	Post test	Variación porcentaje de minimización
Minimización en Procesos y controles	15	8,33%	141	78,33%	70%
Minimización en alteración de la información	30	15,00%	201	100%	85%
Minimización en costos de perdida de la información	30	14,29%	170	80,95%	66,66%
Minimización de la vulnerabilidad de la información	75	10,87%	512	74,20%	63,33%

Fuente: elaboración propia

CAPITULO VI: DISCUSIÓN

Como se puede apreciar en este estudio se realizó la variación o comparación de la minimización de la vulnerabilidad de la información antes y después de la evaluación de la seguridad de información; Donde se obtuvo como resultado 23,95% antes de la aplicación de la evaluación el cual nos indica que la vulnerabilidad de la información es alta y posterior a la evaluación la vulnerabilidad de la información se minimizó en un 80,03% después de la Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001, quiere decir que los terminales tecnológicos de la organización fueron implementados satisfactoriamente sobre seguridad de la información, (Espinoza Aguinaga, 2013), la adecuada gestión de la seguridad de información es algo que debe estar ya incluido en la cultura organizacional de las empresas; y en todas ellas esta adecuada gestión no se lograría sin el apoyo de la alta gerencia como promotor activo de la seguridad en la empresa.

Debe tenerse en cuenta que el diseño de SGSI se adapta a los objetivos actuales de procesos de producción, los objetivos estratégicos y de gobierno de las empresas pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán. Entonces todas las empresas deben mayor importancia a la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades.

CONCLUSIONES

Se evaluó la gestión de la seguridad de la información basada en el estándar ISO 27001 en la Organización Disav SAC, obteniendo como resultado la minimización en un 63,33%. Por lo tanto se concluye que hay una minimización de la vulnerabilidad de la información de manera significativa.

- Se evaluó los procesos y controles de gestión de la seguridad de la información en la Organización Disav SAC, obteniendo que la implementación de estos procesos mejoro en un 70%.
- Se minimizó la alteración de la información en la Organización Disav SAC en un 85% positivo para la empresa.
- Se redujeron los costos originado por la pérdida de información en la Organización Disav SAC en un 66,66%.

RECOMENDACIONES

En primera instancia se recomienda a Organización Disav Sac que en base al diseño presentado en este proyecto, se dedique en concientizar a todos los trabajadores que forman parte de dicha empresa, sobre la seguridad de la información y su importancia, y realizar evaluaciones periódicas a los indicadores de seguridad de la empresa y de los riesgos encontrados.

Luego, se recomienda a todas las empresas ya sean privada o pública a que puedan implantar un Sistema de Gestión de la Seguridad de la Información con ISO/IEC 27001 basada en buenas practicas, lo cual garantizará que su activo más importante que es la información este más confiable para la toma decisiones de las altas gerencias.

En esta empresa solo se estableció algunos controles de la seguridad de la información que son de prioridad para los trabajadores por lo tanto se recomienda implementar todos los controles con lo cual sería mucho mejor el cuidado del activo más valioso de la institución, se recomienda formar y capacitar de manera periódica a todos los personales de la institución en temas de la seguridad de la información y así lograr que los activos más valiosos que tiene una institución esté integro, confiable y disponible.

Como trabajos futuros se pueden realizar diseños similares para los demás procesos de la empresa. De manera similar sería adecuado que se elabore un plan de continuidad de negocio, lo que permitirá reforzar la seguridad en la empresa y además de diseñar un plan de auditoría que se realice periódicamente para analizar cómo va variando el nivel de seguridad de la empresa tal como avanza el tiempo.

REFERENCIA BIBLIOGRAFICA

- Areitio. (2008). Redes, Informática y Sistemas de la Información. *Seguridad de la Información*. España: Ediciones Paraninfo S.A.
- Barrantes Porras, C. E., & Hugo Barrera, J. (2012). *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos*. Lima, Perú.
- Bermúdez Molina, K. G., & Bailón Sanchez, E. R. (Marzo de 2015). 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. guayaquil, ecuador.
- Espinoza Aguinaga, H. R. (Octubre de 2013). análisis y diseño de un sistema de gestión de seguridad de información basado en la norma iso/iec 27001:2005 para una empresa de producción y comercialización de productos masivos. lima, Perú.
- Fonceca. (2012). La información el activo más importante para cualquier organización. 18.
- Gomez. (2012). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. Barcelona, España: Aenor Ediciones.
- Guamán, J. A. (Abril de 2015). Diseño de un sistema de gestión de seguridad de la información para instituciones militares. Quito, Ecuador.
- Información, E. G. (2012). *Encuesta de Agenda de Riesgo de Tecnologías de la Información*. Mexico, Mexico: Culiacan.
- ISO. (2015). *Organización Internacional de Normalización*. Obtenido de <http://www.ISO.org>
- Martinez. (2005). Importancia de los sistemas de información para las pequeñas empresas. 25.

- Paredes Fierro, G., & Vega Noboa, M. (2011). Desarrollo de una metodología para la auditoria de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de pichincha del consejo de la judicatura. Chimborazo, Ecuador: Politecnica Chimborazo S.R.L.
- Project Management Consultores de Proyectos, S. (2006). Sistema de gestión de la seguridad de la información ISO 27001. *Project Management Consultores de Proyectos*, 1-2.
- Puma. (2017). Implantación de un proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002 en una entidad financiera de puno. Puno, Perú: Ayaviris .
- Sanchez. (2013). *Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de quito*. Quito, Ecuador.
- Talavera Alvarez, V. R. (Mayo de 2015). diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la iso/iec 27001:2013. lima, Perú.
- Villena. (2006). Sistema de gestión de seguridad de información para una institución financiera. 31.
- Poveda. (2011). Estándares de la gestión de la información. revista auditoria informática. pag. 04.
- Cabrera. (2018). diseño de un modelo de políticas basado en la norma iso 27001, para mejorar la gestión de la seguridad de la información en la municipalidad distrital de florida – bongará – amazonas. tarapoto.
- Sunat. (2012). superintendencia nacional de administración tributaria (sunat).
Obtenido de: www.sunat.gob.pe

ANEXOS:

ANEXO 01: Matriz de Consistencia

“ EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001”						
PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLE	DIMENSION	INDICADORES	METODOLOGÍA
¿Cómo mejorar la seguridad de la información en la Organización Disav SAC?	General Evaluar la gestión de seguridad de la información basada en el estándar ISO 27001 en la Organización Disav SAC.	General La evaluación del Sistema de Seguridad de la Información en la Organización Disav Sac Aplicando Lineamientos Iso 27001 minimizará la vulnerabilidad de la información.	V. Independiente Lineamientos ISO 27001	Evaluar la seguridad de la información.	% de la evaluación de seguridad de la información	Método (cuantitativo) Nivel (explicativo) Diseño (pre experimental).
	Específicos Evaluar los procesos y controles de gestión de la seguridad de la información en la Organización Disav SAC. Minimizar la alteración de la información en la Organización Disav SAC. Reducir los costos originado por la pérdida de información.	El Sistema de Seguridad de la Información en la Organización Disav Sac Aplicando Lineamientos Iso 27001 Evaluará los procesos y controles. El Sistema de Seguridad de la Información en la Organización Disav Sac Aplicando Lineamientos Iso 27001 minimizará la alteración de la información en la Organización Disav SAC. El Sistema de Seguridad de la Información en la Organización Disav Sac Aplicando Lineamientos Iso 27001 Reducirá los costos originado por la pérdida de información.	V. Dependiente Evaluación del sistema de seguridad de la información	Procesos y controles. Alteración de la información. Costo de perdida de la información	% de la evaluación de los procesos y controles % de la minimización de Alteración de la información. % costo de perdida de la información	Población: los 15 terminales tecnológicos de la Organización DISAV SAC. Muestra: los 15 terminales tecnológicos de la organización DISAV SAC

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Buenas tardes, Sr.(a) Mi nombre es Eber Jesús Apahuasco Saccaco, estoy realizando un estudio sobre la “**EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001.**”

Por tal motivo, me gustaría revisar su terminal tecnológico. La información que sea encontrada será estrictamente confidencial y permanecerá en absoluta reserva. Según Ley N° 29733 (Ley de Protección de Datos Personales).

Fecha: ___/___/2019 N° de Encuesta

1) PROCESOS Y CONTROLES

1.1. ¿Organización Disav le hizo conocer políticas de seguridad de la información?

SI () NO () EN PARTE ()

1.2. ¿Los terminales de Organización Disav cuenta con políticas de seguridad de la información?

SI () NO () EN PARTE ()

1.3. ¿Los encargados de los terminales tecnológicos fueron capacitados sobre la seguridad de la información por un conocedor o una empresa especializada?

SI () NO () EN PARTE ()

1.4. ¿La administración exige a tener en cuenta la Seguridad de la Información para el uso de los terminales?

SI () NO () EN PARTE ()

1.5. ¿La información utilizada es confidencial en los terminales tecnológicos?

SI () NO () EN PARTE ()

1.6. ¿La contraseña del terminal tecnológico es confidencial?

SI () NO () EN PARTE ()

2) ALTERACIÓN DE LA INFORMACIÓN

2.1. ¿La información es manipulada de acuerdo a dónde pertenece o corresponde?

SI () NO () EN PARTE ()

2.2. ¿Organización Disav cuenta con una política de control de accesos a las áreas donde hay equipos tecnológicos?

SI () NO () EN PARTE ()

2.3. ¿Las computadoras y dispositivos móviles cuenta con una contraseña seguro para permitir el acceso?

SI () NO () EN PARTE ()

2.4. ¿Se revisa toda la información que se tiene en su computadora y/o dispositivo móvil con frecuencia?

SI () NO () EN PARTE ()

2.5. ¿La contraseña de acceso de usuarios es cambiada frecuentemente?

SI () NO () EN PARTE ()

2.6. ¿Se utiliza mecanismos de bloqueo automático de su computadora personal cuando se deja de usar?

SI () NO () EN PARTE ()

2.7. ¿Se asegura que las computadoras donde trabaja cuenten con protección adecuada contra virus informático?

SI () NO () EN PARTE ()

2.8. ¿Las computadoras donde se labora tienen instalado antivirus?

SI () NO () EN PARTE ()

2.9. ¿La información está protegida contra posibles alteraciones?

SI () NO () EN PARTE ()

2.10. ¿Se restringen la instalación de otras aplicaciones o software que no sea de trabajo?

SI () NO () EN PARTE ()

3) COSTO DE PÉRDIDA DE LA INFORMACIÓN

3.1. ¿Las puertas y ventanas del área de sistemas se encuentran seguras?

SI () NO () EN PARTE ()

3.2. El área de sistemas está seguro y ubicado contra amenazas externas? Ejemplo incendios, inundaciones

SI () NO () EN PARTE ()

3.3. ¿Las computadoras y/o dispositivos móviles son utilizados solo por personal autorizado?

SI () NO () EN PARTE ()

3.4. ¿En caso de falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su ágil verificación?

SI () NO () EN PARTE ()

3.5. ¿Se realiza mantenimiento reiterado de hardware y software en la empresa?

SI () NO () EN PARTE ()

3.6. ¿Se realiza copias de la información que maneja en el equipo tecnológico de trabajo?

SI () NO () EN PARTE ()

3.7. ¿La empresa cuenta con un personal responsable en el área de seguridad de la información?

SI () NO () EN PARTE ()

ANEXO 3: Solicitud de permiso para realizar trabajos de investigación

“AÑO DE LA LUCHA CONTRA LA CORRUPCION E IMPUNIDAD”

SOLICITO: Permiso para realizar encuesta al personal de la Empresa

**Señor: NEANDER ORTIZ MEDINA
LIDER COMERCIAL Y LOGÍSTICO DE ORGANIZACIÓN DISAV**


Yo, Eber Jesús Apahuasco Saccaco, identificado con DNI N° 45822700, domiciliado en Jr. Los Cactus N°320 en el centro poblado de Pochccota, distrito de Andahuaylas, provincia de Andahuaylas, departamento de Apurímac, con el debido respeto me presento ante Ud. y expongo:

Que teniendo la oportunidad de saludarlo muy cordialmente y a la vez solicitarle permiso para poder ingresar a las áreas de la empresa y tomar un tiempo de cada personal para poder realizar una encuesta del proyecto que lleva como título **“EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001”**, aprobado por la Universidad Nacional José María Arguedas, esta encuesta será de vital importancia para vuestra empresa pues los resultados obtenidos ayudarán significativamente al área de administración en la toma de decisiones.

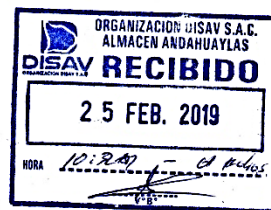
Por lo expuesto.

Agradezco anticipadamente la atención brindada ante la presente solicitud

Atentamente,



Eber Jesús Apahuasco Saccaco
45822700
Bach. Ingeniería de Sistemas



ANEXO 4: Memorandum Informativo sobre la EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001



ORGANIZACIÓN DISAV

"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN E IMPUNIDAD"

MEMORANDUM INFORMATIVO

Para: Westher (Líder Operaciones); Jackelyn (Caja, Almacén); Eber (Supervisor Comercial); Lesli, Moises, Antony (Agente Comercial); Emilio (Chofer Liquidador); Percy (Auxiliar Reparto)

De: Neander Ortiz Medina (Líder Comercial y Logístico)

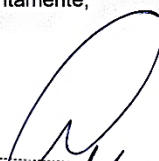
Fecha: 08/07/2019 (08:00:52am)

Tema: **APROBACIÓN DE LA EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC**

El que suscribe, Neander Ortiz Medina con documento de identidad N° 40961502, Líder Comercial y Logístico de Organización DISAV SAC en el Distrito de Andahuaylas, Provincia de Andahuaylas, Región de Apurímac.

Se hace constar el presente memorándum con fines de informar sobre la **APROBACIÓN** de la EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001; el cual fue desarrollada y aplicada en nuestra empresa para minimizar la vulnerabilidad de la información por una persona conocedora del tema. Todo el personal de la empresa deberá cumplir de manera urgente con las políticas aprobadas por la administración.

Atentamente,



Neander Ortiz Medina
LIDER COMERCIAL Y LOGISTICO
DISAV
ORGANIZACIÓN DISAV SAC

ORGANIZACION DISAV S.A.C.
Av. Sesquicentenario 751 - Andahuaylas - Apurímac
Av. Tamburco 180, Abancay - Abancay - Apurímac
Telf. (083) 421084 – RUC. 20603051654

ANEXO 5: Acta de Conformidad de la capacitación realizada sobre EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001



ORGANIZACIÓN DISAV

"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN E IMPUNIDAD"

HACE CONSTAR:

Se hace constar la siguiente **Acta de Conformidad** en favor de la **EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001**; realizado en nuestra empresa el 01 de julio por el sr. Eber Jesús Apahuasco Saccaco identificado con Dni: 45822700; la cual fue desarrollada y aplicada en nuestra empresa con el fin de minimizar la vulnerabilidad de la información.

La presente a expide a favor del involucrado y los fines que considere convenientes.

Andahuaylas, 08 de Julio del 2019

Atentamente,


DISTRIBUIDORA
ALARCÓN VALENZA S.R.L.
Rommel Reynaldo Alarcón Valenzuela
GERENTE DE VENTAS


ORGANIZACION DISAV S.A.C.
RUC. 20603051654
Westher Porfirio Gutiérrez
JEFE DE OPERACION
DNI: 48570516

ORGANIZACION DISAV S.A.C.
Av. Sesquicentenario 751 - Andahuaylas - Apurímac
Av. Tamburco 180, Abancay - Abancay - Apurímac
Telf. (083) 421084 – RUC. 20603051654

ANEXO 6: Capacitación al personal que labora en Organización Disav SAC



ANEXO 7: Fotografías de la encuesta realizada de la PRE y POST evaluación del sistema de seguridad

