VICERRECTORADO ACADÉMICO

ESCUELA DE POST GRADO

TESIS

LA NORMA ISO 27001 COMO SOPORTE AL PROCESO DE LA SEGURIDAD DE LA INFORMACIÓN Y SU INFLUENCIA EN LA GESTIÓN DE SERVICIOS EN EL CENTRO DE ADMINISTRACIÓN DE SERVICIOS EDUCATIVOS DE LA FUERZA AÉREA DEL PERÚ.

PRESENTADO POR:

Bach. CARLOS MUCHOTRIGO TALLA

PARA OBTENER EL GRADO DE

MAESTRO EN DOCENCIA UNIVERSITARIA Y GESTIÓN EDUCATIVA

LIMA - PERÚ

2016

DEDICATORIA

El trabajo está dedicado a mi esposa, mi hijo y mis padres, quienes con esfuerzo brindaron el apoyo incondicional, la confianza y sus palabras alentadoras para conseguir mis objetivos.

AGRADECIMIENTO

Mis agradecimientos al Centro de Administración de Servicios Educativos FAP, por facilitarme la información necesaria, a mis asesores por el apoyo brindado en mi proyecto de tesis.

RECONOCIMIENTO

Agradezco especialmente al Sr. Director del Centro de Administración de Centros Educativos FAP CORONEL FAP Augusto García Calderón.

A mis profesores quienes expandieron mi percepción y mi entendimiento.

A las autoridades y comité de Tesis de la UAP quienes brindaron la oportunidad de desarrollarme académicamente y profesionalmente.

Finalmente a todos los alumnos y administrativos de la I.E FAP “Manuel Polo Jiménez” quienes prestaron su desinteresada colaboración para la concreción de la presente investigación.

INDICE

RESUMEN

La investigación tuvo como objetivo principal, determina la influencia que existe entre la norma ISO 27001:2013 y el soporte al proceso de la seguridad de la información en la gestión de servicios del centro de administración de Servicios Educativos FAP. iniciando desde el entendimiento de la organización desde la óptica de los procesos críticos, ejecución del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para el Centro de Administración de Servicios Educativos.

Se utilizó el diseño correspondiente a la investigación descriptiva correlacional con un método hipotético deductivo. Se trabajó con una muestra de 80 personas a los cuales se les aplicó una encuesta que permitió recoger información y medir la variable norma ISO 27001:2013 como soporte de al proceso de seguridad de la información en un momento oportuno y para medir la gestión de servicios se utilizó los instrumentos de los usuarios de los servicios de los CASE-FAP.

Los resultados fueron según la tabla 3 y figura 1 que el 69% de los encuestados presentan un nivel regular con respecto a la variable norma ISO 27001:2013 como soporte de al proceso de seguridad de la información, un 28.17% un nivel alto y un 2.82% un nivel bajo y según los resultados brindados por los usuarios de la gestión de servicios, se obtuvo que el 43.33% presenta un logro previsto, el 36.62% un logro en el proceso, 16.20% un logro destacado y un mínimo del 32.52% en un nivel inicial. Según la comprobación de hipótesis la norma ISO 27001:2013 esté relacionada directa y positivamente con la variable gestión de servicios, según el estadístico “T” de Student de 0.742 representando este resultado como fuerte con una significancia estadística de p=0.000 siendo este menor que el 0.01.

Palabras clave: Proyecto, norma iso, gestión del riesgo, análisis de Riesgos.

ABSTRACT

The main objective of the research was to determine the influence that exists between the ISO 27001: 2013 standard and the support for the process of information security in the service management of the FAP Educational Services administration center. Starting from the understanding of the organization from the perspective of critical processes, execution of the information security diagnosis, identification of the main vulnerabilities and threats, applying a methodology of risk management for the management of information security risks, Planning of risk management plans and generation of the documentary framework of the information security management system for the Educational Services Administration Center.

We used the design corresponding to correlational descriptive research with a hypothetical deductive method. We worked with a sample of 80 people who were given a survey to collect information and measure the variable ISO 27001: 2013 as a support for the process of information security in a timely manner and to measure the management of services The instruments of the users of the CASE-FAP services were used.

The results were according to Table 3 and Figure 1 that 69% of the respondents present a regular level with respect to the ISO 27001: 2013 variable as a support for the information security process, 28.17% a high level and a 2.82% a low level and according to the results provided by users of the service management, it was obtained that 43.33% has an expected accomplishment, 36.62% an achievement in the process, 16.20% a remarkable achievement and a minimum of 32.52% At an initial level. According to the hypothesis test, the ISO 27001: 2013 standard is directly and positively related to the service management variable, according to the Student "T" statistic of 0.742, representing this result as strong with a statistical significance of p = 0.000 being less than 0.01.

Keywords: Project, ISO standard, risk management, risk analysis

INTRODUCCIÓN

La presente investigación, titulada: La norma ISO 27001 como soporte al proceso de la seguridad de la información y su influencia en la gestión de servicios en el centro de administración de servicios educativos de la Fuerza Aérea del Perú, se desarrolla con la finalidad de determinar la influencia que existe entre la norma ISO 27001 como soporte al proceso de la seguridad de la información y el gestión de servicios en el centro de administración de servicios educativos de la FAP.

La investigación implementa una estrategia, de proteger la confidencialidad, la integridad y la disponibilidad de los recursos de información, dichas estrategias se elaboran en base a la identificación de los riesgos tanto internos como externos de toda la infraestructura de la organización. La mayoría de las empresas ha invertido tiempo y dinero en la construcción de una infraestructura de la tecnología de la información que soporte la compañía, esa infraestructura de Tecnología de la Información podrá resultar ser una debilidad si se está comprometida.

Dicha investigación permite establecer todos los mecanismos y acciones salvaguardando los activos de la información de la organización, esto permitirá garantizar la administración de información, la operatividad del negocio, con lo cual se cumplirán los requerimientos regulatorios asociados a la seguridad de información.
Las organizaciones funcionan en la era de la informática interconectadas y con comunicación electrónica, las políticas de información documentadas se comunican, entienden e implementan en toda la empresa, son herramientas comerciales esenciales en el entorno actual para minimizar los riesgos de seguridad. Con la planificación integral, anticipada, efectiva, es posible responder rápida y apropiadamente a cualquier tipo de ataque lo cual atente contra los sistemas de información.

De esta manera la investigación, propone soluciones como una herramienta, lo cual concientiza a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos le permiten desarrollarse y mantenerse en su sector de negocios. Este proceso debe comprometer a todo el personal aportando agudeza, destreza y experiencia técnica para detectar debilidades, y constancia donde renueva y actualiza el plan en función del dinámico ambiente el cual rodean las organizaciones modernas.

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Los estudios realizados a gestores de Tecnología de la Información y grandes empresas en Europa el cual se encuentran en el campo de la Seguridad de la Información y como principales problemas el precario presupuesto que se dedica a la Tecnología de la Información y la carencia de apoyo para ocuparse de las necesidades en seguridad los cuales representan las mayores amenazas en la red, siguiéndole de cerca las fallas en los sistemas operativos y aplicaciones.

Los estudios realizados dan como insuficiente los presupuestos destinados a esta área, y los encargados de la gestión empresarial no le dan la importancia debida.

Las encuestas realizadas por IBM manifiestan los ataques informáticos han aumentado en Latinoamérica. Los dos principales problemas son las limitaciones en el presupuesto así como las contradicciones entre conciencia y acción de las empresas. Ese problema se explica en un contexto donde las inversiones de Seguridad en Latinoamérica bordean el 14.5% en comparación con las de Europa y EE.UU.[1]

[1] Encuesta IBM 2013. Recuperado de: http://www.ibm.com/encuest07

En América del Sur compañías Brasileñas y Chilenas fueron las mas afectadas con el 45% y 40% respectivamente, donde los riesgos en Seguridad Informática han experimentado un "aumento espectacular", siendo los hackers la principal amenaza a la red.[2]

En el Perú el 52% de los entrevistados en una encuesta realizada, consideró a la competencia como una amenaza a la seguridad.[3]

El Centro de Administración de Servicios Educativos FAP - CASED no cuenta con un Plan de Seguridad Informático y no establece una cultura de la seguridad en la organización.
Bajo el contexto descrito, existe diversidad de información de carácter secreto y/o confidencial donde no se aplica ninguna medida de seguridad para la protección de la información.

Otra deficiencia es el envío de información documentada entre las diferentes oficinas de la unidad, esta documentación es recepcionada pero en la mayoría de casos no es archivada, el documento queda libre a ser sustraído o manipulado por personas ajenas a la unidad. De igual manera resulta una deficiencia grave que los Sistemas de Información que actualmente maneja el Centro de Administración de Servicios Educativos FAP no cuenta con la seguridad necesaria al momento de ingresar al sistema.

Finalmente, debido a la constante pérdida de información y la falta de seguridad en la gestión de servicios, es afectada generando llamadas de atención por el ente superior.

1.2. DELIMITACIÓN DE LA INVESTIGACIÓN

1.2.1. Delimitación Espacial

El presente trabajo de investigación, a nivel de prototipo, se realizó en el Centro de Administración de Servicios Educativos FAP (CASED), ubicado en la Av. Higuereta 685 Las Gardenias – Surco, de Lima, Perú

[2] Encuesta IBM 2013. Recuperado de: http://www.ibm.com/encuest09
[3] Encuesta Cisco. Recuperado de: http://www.cisco.com/datos.htm

1.2.2. Delimitación Temporal

El desarrollo de la presente investigación, tendrá tuvo un horizonte temporal comprendido entre Enero – Setiembre del 2015.

1.2.3. Delimitación Social

De acuerdo a la naturaleza de las variables que intervienen en el tema desarrollado, los siguientes roles sociales son involucrados:

- Dirección del Centro de Administración
- Jefatura de Informática
- Jefatura de Personal
- Jefatura de Mesa de Partes

1.2.4 Delimitación Conceptual

Se presenta el principal descriptor temático usado para delimitar el aspecto conceptual sobre el cual se apoya este trabajo de investigación.

A.- Sistemas de Gestión de Seguridad de la Información SGSI - ISO 27001

El nuevo Estándar Internacional, ISO 27001:2013 está orientado a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas, además de reducir costes a través de la optimización de sus procesos, mejorar la comunicación entre sus departamentos y obtener el prestigio de conseguir una certificación internacionalmente reconocida [4] .

B.- Gestión de servicios

La gestión del servicio se encuentra integrada en la gestión de la cadena de suministro como el punto de unión entre las ventas y el cliente. El objetivo de lograr un alto rendimiento en la gestión del servicio es optimizar las cadenas de suministros centradas en el servicio, que son más complejas que aquellas centradas en los productos. Aceituno (2004).

[4] El Portal del ISO 27001. Recuperado de: http://www.iso27000.es

1.3 PROBLEMAS DE INVESTIGACIÓN

1.3.1 Problema Principal

¿De qué manera la Norma ISO 27001:2013 como soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios del Centro de Administración de Servicios Educativos FAP?

1.3.2 Problemas Secundarios

- ¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la gestión de Servicios en la productividad del Centro de Administración de Servicios Educativos FAP.?

- ¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la gestión de Servicios en la eficiencia del Centro de Administración de Servicios Educativos FAP.?

- ¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la gestión de Servicios en la eficacia del Centro de Administración de Servicios Educativos FAP.?

1.4 OBJETIVO DE LA INVESTIGACIÓN

1.4.1 Objetivo General

Determinar como la norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios del Centro de Administración de Servicios Educativos de la Fuerza Aérea del Perú.

1.4.2 Objetivos Específicos

- Determinar como la norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la productividad del Centro de Administración de Servicios Educativos de la FAP.
- Determinar como la norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la eficiencia del Centro de Administración de Servicios Educativos de la FAP.

- Determinar como la norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la eficacia del Centro de Administración de Servicios Educativos de la FAP.

1.5 HIPÓTESIS Y VARIABLES DE LA INVESTIGACIÓN

1.5.1 HIPÓTESIS GENERAL

La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en el Centro de Administración de Centros Educativos de la FAP.

1.5.2 HIPÓTESIS SECUNDARIAS

- La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la productividad del Centro de Administración de Centros Educativos de la FAP.

- La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la eficiencia del Centro de Administración de Centros Educativos de la FAP.

- La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la eficacia del Centro de Administración de Centros Educativos de la FAP.

1.5.3 IDENTIFICACIÓN Y CLASIFICACIÓN DE VARIABLES E INDICADORES

1.5.3.1 VARIABLE X:

Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información.

Dimensiones:

- Fiabilidad
- Seguridad
- Usabilidad

Indicadores:

- Funciones adecuadas
- Niveles de acceso
- Comprensibilidad

1.5.3.2 VARIABLE Y:

Gestión de Servicios.

Dimensiones:

- Productividad.
- Eficiencia.
- Eficacia.

Indicadores:

- Promedio mensual de documentos emitidos.
- Promedio mensual de documentos recibidos.
- Tiempo de respuesta promedio ante un requerimiento.

1.6 METODOLOGÍA DE LA INVESTIGACIÓN

1.6.1 TIPO Y NIVEL DE LA INVESTIGACIÓN

a) TIPO DE INVESTIGACIÓN

La Naturaleza de esta investigación es de enfoque cuantitativo, y de tipo sustantiva y básica.

Es sustantiva y básica, por que busca describir cada una de las variables en sus aspectos teóricos y caracterizaciones para luego establecer la relación existente entre las variables dentro de un contexto social y temporal. (Hernández, Fernández & Baptista, 2010, pág.286)

Es cuantitativa por que utilizó la recolección y el análisis de datos para contestar preguntas de investigación y probar las hipótesis establecidas previamente y confía en la medición numérica, la tabulación y el uso de la estadística para establecer asertivamente patrones de comportamiento en la población. (Hernández, Fernández & Baptista, 2010, pág.266)

b) NIVEL DE INVESTIGACIÓN

La Investigación corresponde a una investigación de nivel descriptivo correlacional. Según Bernal y otros (2000, pág. 1113) considera como una investigación descriptiva aquella en la que se reseñan las características y rasgos de una situación fenomenológica u objeto de estudio y correlacional porque se va determinar los niveles de relación que se establecen en la concurrencia de dos variables en un contexto situacional. (Hernández, Fernández & Baptista, 2010, pág.326)

1.6.2 MÉTODO Y DISEÑO DE LA INVESTIGACIÓN

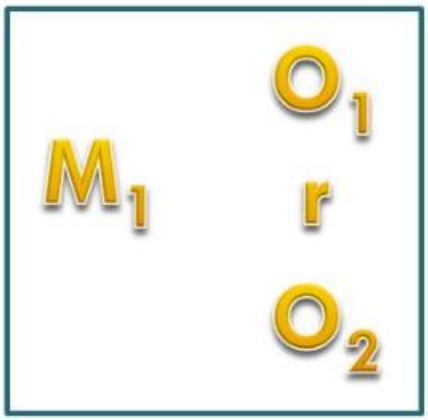
a) MÉTODOS DE INVESTIGACIÓN

El desarrollo de esta investigación se ha utilizado el método hipotético deductivo (deductivo - explicativo) por proporcionar un planteamiento ordenado y un nivel de rigurosidad alto en el tratamiento de los datos y análisis de resultados. En forma complementaria se ha utilizado el concepto sistémico. El trabajo de investigación sigue un método comprobado de recopilación y análisis de los antecedentes que se han obtenido y comprobado directamente en el campo el cual se ha presentado el hecho materia de investigación. (Hernández, Fernández & Baptista, 2010, pág.300)

b) DISEÑO DE INVESTIGACIÓN

El diseño de la investigación es no experimental de tipo transeccional debido al análisis de la relación de hechos y fenómenos de la realidad para conocer su nivel de influencia buscando determinar su nivel de relación entre variables.

La Variable independiente se considera como supuesta causa en la relación entre variables y el efecto provocado por dicha causa se le denomina variable dependiente.



Dónde:

M1: Población Muestral

O1: Observaciones de la 1era variable

O2: Observaciones de la 2da variable

R : Niveles de influencia que se dan entre las variables concurrentes.

1.6.3 POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

a) POBLACIÓN

La población es un conjunto de individuos de la misma clase, limitadas por el estudio. Según (Hernández, Fernández & Baptista, 2010), "La población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación" (Pág. 425).

La Unidad de análisis que sirve de base para la definición de la población que está conformada por 80 usuarios que tramitan la información confidencial (mensajes).

b) MUESTRA: NO PROBABILÍSTICOS

La muestra se determinó teniendo en cuenta la población de personas el cual laboran en el área de Mesa de Partes e Informática, encargados del envío y/o tramitar mensajes a otras unidades. La muestra se refleja en la siguiente tabla:

Tabla 01: *Mensajes enviados por áreas*

ÁREAS	# DE MENSAJES ENVIADOS/TRAMITADOS
INFORMÁTICA	10
MESA DE PARTES	20
TOTAL	**30**

Fuente: Elaboración Propia, 2016

1.6.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

a) TÉCNICAS

Las principales técnicas que se han utilizado para el levantamiento de información son:

- Entrevistas: Es una conversación entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados) basándose en una guía de preguntas específicas.
- Revisiones Bibliográficas: Identificar las fuentes arbitradas e indizadas que le dan un carácter de validez y rigor a la información que se busca.
- Cuestionario: Consiste en una series de preguntas, redactas de forma coherente, con una secuenciación lógica y estructuradas con unos objetivos claramente delimitados anteriormente y a los cuales estas preguntas deben dar respuesta.

b) INSTRUMENTOS

Los instrumentos utilizados fueron los siguientes:

- Guía Cuestionario: instrumento de investigación en una series de preguntas.
- Guía de entrevistas: Es una guía de preguntas específicas.
- Fichas Bibliográficas: Ficha pequeña, destinada a anotar meramente los datos de un libro o artículo.

1.6.5 JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

a) JUSTIFICACIÓN DE LA INVESTIGACIÓN

La justificación de esta investigación se basa en aplicar se contribuye a reducir la pérdida o robo de información confidencial existente. También se justifica porque lleva una adecuada administración de los sucesos que puedan ocurrir dentro del sistema de Seguridad de la Información.

En la primera década del siglo XXI ha surgido la aparición de nuevas amenazas en los sistemas informáticos, teniendo el riesgo de la información sea revelada o no sea utilizada apropiadamente, el correcto manejo de la información es trascendental para el éxito de CASED.

Debido a la importancia de este recurso, su aseguramiento debe ser un objetivo primordial y con el fin de suplir dichas necesidades de seguridad.

En el último lustro, se cuenta con estándares internacionales aceptados, proporcionan mecanismos de seguridad, con resultados ideales y deberían ser implementados por todas las organizaciones. En este sentido, sobresale la norma ISO 27001:2013, la cuales proveen los requisitos necesarios gestionando la Seguridad de la Información, minimizando los riesgos a los que está expuesta.

Mediante el diseño e implementación de un Sistema de Gestión de Seguridad de la Información, el Centro de Administración de Servicios Educativos consigue minimizar el riesgo de que su información se vea afectada por la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información. En la actualidad han surgido nuevas amenazas en la seguridad de la información, teniendo el riesgo de la información sea revelada o no sea utilizada apropiadamente, el correcto manejo de la información es trascendental para el éxito del CASED FAP.

b) IMPORTANCIA

El proceso de Seguridad de la Información es uno de los puntos más críticos en la institución. Por tanto, es importante contar con un soporte donde permita brindar seguridad a la información en general, donde se puedan manejar en la institución. Lamentablemente no existe en la actualidad una herramienta donde permita lograr sus objetivos; de allí se desprende la importancia de demostrar que el Sistema de Gestión de Seguridad mejora el rendimiento.

El diseño de un sistema de gestión de seguridad de la información para el CASED basado en la ISO 27001:2013, aportará substancialmente a una gestión eficaz de la seguridad de la información permitiendo:

- Asegurar el acceso a la información, previniendo la divulgación de la misma a personas o sistemas no autorizados.
- Asegurar la información con métodos de procesos exactos y completos, buscando mantener los datos libres de modificaciones no autorizadas.
- Asegurar que usuarios autorizados tengan acceso a la información cuando lo requieran, es decir que puedan estar a disposición de quienes deben acceder a ellas.

c) LIMITACIONES DE LA INVESTIGACIÓN

Las únicas limitaciones que se tuvo fueron la falta de tiempo para hacer mis investigaciones por motivo de estudios, por lo cual recurrimos a contar con ayuda de profesionales que me ayudaron y asesoraron con mi investigación.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Con relación a la temática estudiada se revisaron publicaciones existentes, consultando fuentes de informaciones primarias, secundarias y terciarias. Al respecto, se han encontrado algunas investigaciones relacionadas, proyecto donde aborde bajo el mismo enfoque la relación de las dos variables involucradas; en consecuencia, se da testimonio de la autenticidad de este trabajo.

Internacionales:

- Según Cerini M. (2010)**.** En su investigación denominada **"***Plan de Seguridad Informática"*. …. las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

- Según Universidad Católica de Chile. (2009). En su investigación *"Sistema de Gestión de Seguridad de Información (SGSI)"*. Los riesgos comerciales a los que una organización está sometida son interminables. Los activos de información que se manejan en la empresa moderna son importantísimos para su desempeño estratégico. Imaginémonos los virus que se proliferan en la red, los hackers siempre al acecho, intrusos que penetran a nuestro sistema informático y se llevan la información de los clientes, estados financieros que llegan fácilmente a manos de terceros y bases de datos que son usurpadas. Si las empresas no establecen sistemas que aseguren la integridad, confidencialidad y disponibilidad de su información jamás podrán mantenerse compitiendo en el mundo globalizado. La idea para minimizar la posibilidad de riesgo en el manejo de la información, consiste en establecer un Sistema de Gestión de Seguridad de Información (SGSI) en la empresa que permita llevar a sus niveles mínimos el riesgo y permita asegurarle a terceros que se tiene un sistema confiable de información.

- Según Areitio J, & Areitio B. (2008). *"Seguridad de la Información. Redes, Informática y sistemas de información"*. La seguridad ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por internet. Por ello, se hace imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.

  Este desplazamiento del enfoque de las cuestiones de seguridad, desde el nivel gubernamental al resto de la sociedad, ha elevado la importancia de la seguridad, que ha pasado a ser una disciplina cada vez más crítica, necesaria y obligatoria y un componente clave en todo tipo de proyectos de sistemas de información.

- Según Díaz O., Mur F. y San Cristóbal E. (2008). *"Seguridad en las Comunicaciones y en la Información"*. La seguridad informática de hoy en día suele tener muy en cuenta la prevención (cortafuegos, criptografía, etc.) pero está evolucionando en cuanto. Empiezan, poco a poco, a verse herramientas de detección (como los sistemas de detección de intrusos) y herramientas y sistemas (muchas veces humanos) de auditoria de vulnerabilidades.

- Según Villena M. (2008). *"SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA UNA INSTITUCION FINANCIERA"*. (Maestría). Universidad Autónoma de Nuevo León. México. En la actualidad, las inversiones en seguridad que realizan las empresas se destinan cada vez menos a la compra de productos, destinando más bien parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad ha variado, acuñándose uno nuevo, el de seguridad gestionada, que va desplazando poco a poco al de "seguridad informática". Las medidas que comienzan a tomar las empresas giran en torno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directivas, procedimientos y criterios que permiten desde la administración de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de información, la organización afín y sus infraestructuras. Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando lo anterior como punto de partida, una entidad puede adoptar algunas de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información.

Nacionales

- Según Barrantes C. (2007). *"Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos".* …en la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgo al igual que sus activos.

  Se centra en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usa como referencia las normas ISO 27001:2005 e ISO 17799:2005.

- Según Gutiérrez E. (2007). *"Calidad y seguridad de la información y auditoría informática"*. (Maestría). Universidad Autónoma. Lama. Perú. La seguridad de la información tiene como fin la protección de la información y de los sistemas de información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Los términos Seguridad de Información, Seguridad Informática y garantía de la información son usadas con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la confidencialidad integridad y disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas y las zonas de concentración.

Los gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan gran cantidad de información confidencial sobre sus empleados, clientes, productos, la investigación y la situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en ordenadores y transmitida a través de las redes a otros ordenadores.

- Según Jiménez J. (2000). *"Evaluación Seguridad de un Sistema de Información en la Organización"*. (Tesis pregrado). Universidad de Lima. Perú. La información vertida en esta evaluación está orientada a analizar la importancia de la información, los riesgos a los que se encuentran sujeto. se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información. Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable.

2.2 BASES TEÓRICAS

2.2.1 TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

La "Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella".

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC).

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or fight), para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.

Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales.

La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de la Res Publica (estado) de Roma Imperial y Republicana. El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas.

La Seguridad Moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayol en 1919 identifica la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la Seguridad Fayol dice: “... salvaguardar propiedades y personas contra el robo, fuego, inundaciones y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio”.

Las medidas de seguridad a las que se refiere Fayol, solo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los “cerebros electrónicos”, esta mentalidad se mantuvo, porque ¿quién seria capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Desde el punto de vista técnico, la seguridad esta en manos de la dirección de las organizaciones y, en ultima instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

2.2.2.1 TECNOLOGÍA COMPUTER TELEPHONY INTEGRATION (TECNOLOGÍA CTI)

a) DEFINICIÓN

Llamada también Integración Telefónica Computarizada o Integración Telefonía-Cómputo, es el producto de la integración y convergencia de la informática, la

microelectrónica, las telecomunicaciones y las técnicas para el procesamiento de datos[5].

El desarrollo de las TIC constituyen el motor de la nueva economía, denominada "Economía Digital" por los EEUU y "Sociedad de la Información" por la Unión Europea, esta última concepción es adoptada por la Naciones Unidas como una calificación más evolucionada de un modelo económico, que incluye conceptos sociales y políticos, que es apoyado por la convergencia de múltiples tecnologías[6].

Las herramientas que hacen posible esta nueva tendencia empresarial son dos: un canal de telecomunicaciones y un sistema de conmutación y distribución de llamadas.

El sistema informático parte de un equipo dotado de elementos físicos y lógicos capaces de gestionar la recepción de llamadas y distribuirlas adecuadamente, de manera prefijada, según los criterios que resulten más convenientes y provechosos para el servicio y la unidad. Concebido como una herramienta muy avanzada de automatización de procesos telefónicos, es capaz de ejecutar la mayoría de las funciones rutinarias de una centralita telefónica: atender las llamadas, encaminadas a sus correspondientes receptores, retenerlas, guardar y transmitir mensajes, ofrecer información típica básica, etc. Y hacerlo de manera automática y natural, en varios idiomas y con un timbre de voz agradable y una dicción perfecta, propios de locutores profesionales, ya que crea diálogos en lenguaje natural.

Además, esta tecnología es compatible con la marcación telefónica por tonos (multifrecuencia) y por pulsos (decádica), lo que permite rápido acceso a través del teclado del aparato telefónico a cualquier extensión de la empresa, e incluso identificación previa del llamante, y por tanto la detección automática de cualquier llamada desde el extranjero y la selección automática del idioma de respuesta en función del origen de la llamada. En cualquier caso, no se trata de una simple operadora telefónica automática, sino de mucho más, ya que es capaz también de integrar llamadas con las de procesamientos de datos y desarrollar así aplicaciones avanzadas.

b) BENEFICIOS

Las nuevas tecnologías de información y comunicaciones están creando o apoyando redes y sistemas innovadores que afectan cada vez más a las sociedades, gobiernos,

[5] CTI(Computer-Telephony-Integration). (2009). Recuperado de: http://www.idg.es/dealerworld
[6] Edagard, B. (1997). "PC Telephony". Parity Corporation, USA. 122-123

industrias, comunidades e individuos. La integración de las redes de telefonía y de cómputo permite que los directivos e integrantes de la organización puedan tener acceso a la información desde cualquier sitio, ya que permite que los usuarios tengan acceso y manejen todos sus mensajes (E-mail, voz y fax) sin importar que se encuentren en la oficina o en movimiento. Los usuarios pueden recuperar los mensajes ya sea desde la PC en el escritorio, desde cualquier teléfono o cualquier computadora con acceso a Internet en el mundo, obteniéndose las siguientes ventajas:

- Mejora del acceso a la información y mayor rapidez en la respuesta
- Posibilidad de compartir la información nueva y la ya existente
- Mejora de la eficacia en la comunicación y la presentación de información
- Reducción del tiempo de espera necesario para tener acceso a la información del cliente
- La llamada se transfiere de forma prioritaria a los agentes que tienen la formación adecuada para responder a las distintas necesidades del cliente
- Funciones de seguimiento y creación de informes.

Las políticas, estándares y procedimientos para la seguridad de la Información son una serie de múltiples documentos interrelacionados que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones actuales y futuras. Desafortunadamente, las discusiones acerca de las "políticas", "estándares" y "procedimientos" para la seguridad de la información son con frecuencia confusas; están llenas de malos entendidos, información errada y definiciones contradictorias[7].

c) DIFERENCIAN ENTRE LAS POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

Un aprendizaje es la mejor forma de imaginar este grupo importante de documentos de protección a la información:

- Una política de seguridad explica con documentación el por qué una organización protege su información.
- Los estándares de la organización explican con documentación lo que la organización quiere hacer para implementar y administrar la seguridad de su información.

[7] Huidobro J. (2002). *"Seguridad Aplicada a la Información"*. España. Editorial Paraninfo.

- Los procedimientos explican con documentación exactamente cómo la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior.

d) DOCUMENTO DE LA POLÍTICA DE SEGURIDAD

Es importante anotar que la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentación el enfoque del medio ambiente, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

e) PROCEDIMIENTOS

Los procedimientos de seguridad de la información establecen de manera detallada las operaciones que necesitan realizarse para satisfacer los requerimientos especificados en el Estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información.

f) DETERMINE EL VALOR DE LA INFORMACIÓN VALIOSA

Las organizaciones abordan la seguridad de la información con un enfoque aislado y asumen implícitamente que toda la información debe ser protegida. Usted debe preguntarse si éste es realmente el caso y si su organización sobreprotege alguna información y subprotege otra.

A fin de proteger adecuadamente los recursos de información de la organización es importante entender las clases de recursos de información y sus valores respectivos. A continuación se presentan otras dos definiciones cortas:

- Recurso de la información: Todo equipo, proceso o información que se asocia con la información y se considera debe ser protegida por la compañía.

- Valor de la información: El valor o costo relacionado con lo siguiente:
  - El valor intrínseco de la información.
  - La creación de la información.
  - El almacenaje de la información.
  - La retención y administración de la información.

ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Una Política de Seguridad de la Información es la base para un Programa de Seguridad de la Información[8]. Aunque la Política de Seguridad de la organización establece la necesidad de la seguridad de la información, no especifica lo que se debe hacer para implementarla. Ésta es la función de los Estándares de Seguridad de la Información, y establecen lo siguiente:

- Lo que se debe hacer.
- Los controles de seguridad que se requieren.
- Controles de seguridad adecuados que se apliquen a cada elemento del entorno de protección de la información.

Ayudarle a las organizaciones a desarrollar estándares de seguridad de la información, dos organismos de estándares han definido lo que deben considerar las organizaciones para definirlos. El estándar para la seguridad de la información **ISO/IEC 27001** (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electro technical Commission[9].

La ISO también desarrollo la norma ISO-15408 en 1999, que define estándares de medidas de seguridad TI que se implementan en el hardware, firmware o software. La norma ISO-15408 ignora toda medida de seguridad, que esté fuera del dispositivo, para el cual se ha aplicado, aunque reconoce que se puede aplicar seguridad significativa a través del uso de medidas administrativas, como los controles a las organizaciones, al personal, controles de tipo físico y de procedimiento.

[8] Pallavicini, C. (2008). *"Seguridad Informática"*. Recuperado de: http://www.seguridadinformatica.cl/empresa.php

[9] Bernal R. (2003). *"La Información y la Auditoria de Sistemas"*. México: Editorial Trillas.

2.2.2.2 TÉCNICAS, HERRAMIENTAS Y ESTRUCTURA PARA LOS ESTÁNDARES DE SEGURIDAD

La estructura de los estándares define lo que se debe hacer para proteger la información y respaldar los requerimientos de la política de seguridad de la información. Las normas ISO-27001 y BS-7799 soportan la misma estructura de estándares así:

- Política de Seguridad de la Información
  - Seguridad organizacional.
  - Infraestructura.
  - Acceso externo.
  - Outsourcing.
- Clasificación y control de activos
  - Clasificación de la información.
  - Responsabilidad de acceso.
- Seguridad del personal
  - Funciones y responsabilidades de la seguridad de la información.
  - Capacitación al usuario.
  - Respuesta a incidentes.
- Seguridad física y del entorno
  - Áreas protegidas.
  - Seguridad del equipo.
  - Controles generales.
- Comunicaciones y administración de operaciones
  - Procedimientos operativos y responsabilidades.
  - Planeación y aceptación de sistemas.
  - Protección contra software malicioso.
  - Tareas de reorganización - organización y administración de sistemas.
  - Administración de redes.
  - Manejo de los medios y la seguridad.
  - Intercambio de información y software.
- Control de acceso
  - Requerimientos de la empresa.
  - Administración de acceso al usuario.
  - Responsabilidades del usuario.
  - Control de acceso a la red.
  - Control de acceso al sistema operativo.
  - Control de acceso a las aplicaciones.

- Acceso al sistema de monitoreo y su uso.
- Computación móvil y teletrabajo.

- Desarrollo y mantenimientos de los sistemas
  - Requerimientos de seguridad de los sistemas.
  - Seguridad de las aplicaciones.
  - Controles criptográficos.
  - Seguridad de los archivos de sistemas.
  - Seguridad en los procesos de desarrollo y soporte.
- Administración de la continuidad de la empresa
  - Sistemas, redes, aplicaciones, personal, instalaciones y comunicaciones.
- Cumplimiento
  - Cumplimiento con los requerimientos jurídicos.
  - Cumplimiento de la seguridad e informes de cumplimiento técnico.
  - Aspectos de la auditoría de sistemas.

La creación de esta cantidad de documentación no es una tarea trivial. Afortunadamente, la tarea inicial mayor de poblar la estructura se debe hacer solamente una vez. Después, la documentación sólo debe cambiarse si se introduce un sistema, red, aplicación, ley o reglamentación nuevos o se cambian.
La estructura de los estándares suministrada puede aplicarse a cualquier organización. Algunos elementos de la estructura podrían no aplicar a su organización y otros requerirían documentación extensiva.

2.2.2.3 SEGURIDAD FÍSICA

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos que se encuentran distribuidos por toda la empresa. La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

2.2.2.4 TIPOS DE ATENTADOS DE SEGURIDAD

Este tipo de seguridad esta enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra.
Las principales amenazas previstas en seguridad física son:

- Desastres naturales, incendios, tormentas e inundaciones.
- Amenazas del hombre.
- Disturbios, sabotajes internos y externos.

A. Incendios.- Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

   El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

B. Inundaciones.- Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

   Es causa de mayores desastres en centros de cómputo. Además de las causas naturales de inundaciones, existe la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

C. Condiciones Climatológicas.- Normalmente se recibe de manera anticipada los avisos de tormentas, tempestades. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

D. Terremotos.- Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

E. Picos y Ruidos Electromagnéticos.- Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes eléctricos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

2.2.2.5 ACCIONES HOSTILES

A. Robo.- Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

La información importante o confidencial puede ser fácilmente copiada. El software, es una propiedad fácilmente sustraíble y los discos son fácilmente copiados sin dejar ningún rastro.

B. Fraude.- Millones de dólares son sustraídos de empresas y en muchas ocasiones las computadoras han sido utilizadas como instrumento para dichos fines.
   Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores) tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

C. Sabotaje.- El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.
   Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

D. El control de acceso.- No sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. Utilización de guardias, detectores de metales, sistemas biométricos, verificación automática de firmas (VAF).

2.2.2.5 SEGURIDAD LÓGICA

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra la información. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica[10].

[10] Alberto G. Ph.D. (2009). *Técnicas de la Seguridad Lógica*. México: Editorial Trillas.

Los pasos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas.

La Seguridad Informática se basa, en la efectiva administración de los permisos de accesos a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:

Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no.

a) Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema.

b) Transacciones

También pueden implementar controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

c) Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

d) Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y la información. Esta modalidad puede ser:

Lectura: El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.

Escritura: Este tipo de acceso permite agregar datos, modificar o borrar información.

Ejecución: Este acceso otorga al usuario el privilegio de ejecutar programas.

Borrado: Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Además existen otras modalidades de acceso especial, que generalmente se incluyen en las aplicaciones.

Creación: Permite al usuario crear nuevos archivos, registros o campos.

Búsqueda: Permite listar los archivos de un directorio determinado.

e) Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

f) Control de Acceso Interno

i. Palabras Claves (Password).
ii. Encriptación.
iii. Lista de Control de Acceso.
iv. Límites de la interfaz de usuario.
v. Etiquetas de seguridad.

g) Control de Acceso Externo

i. Dispositivos de control de puertos.
ii. Firewalls o puertas de seguridad.
iii. Acceso de personal contratado o consultores.
iv. Accesos públicos.

h) Administración

Una vez establecidos los controles de acceso sobre los sistemas y aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

2.2.2 NIVELES DE SEGURIDAD INFORMÁTICA

Los niveles describen diferentes tipos de seguridad del sistema operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC)[11].

a. Nivel D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplan con ninguna especificación de seguridad.

Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autotentificación con respecto a los usuarios y sus derechos en el acceso a la información

b. Nivel C1: Protección Discrecional

Se requiere identificación de usuarios al acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario", quien tiene responsabilidad en la seguridad de este. Con la actual descentralización de los sistemas de cómputo, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

c. Nivel C2: Protección de Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

d. Nivel B1: Seguridad Etiquetada

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

e. Nivel B2: Protección Estructurada

Requiere a la etiqueta de cada objeto de nivel superior por ser padre de un objeto inferior.

[11] Ribagorda A. (2010). *Estándares Internacionales de Seguridad en Sistemas de Información*. España: Editorial Stallings.-. Prentice Hall.

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior.

f. Nivel B3: Dominios de Seguridad

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

g. Nivel A: Protección Verificada

Es el nivel mas elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales para asegurar todos los procesos que realiza un usuario sobre el sistema.

2.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

- Acción preventiva**:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. Aceituno, V. (2003)
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. Gaspar, J. (2012)
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Aceituno, V. (2003)
- Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia. Gaspar, J. (2012)
- Auditoría: Es un término que puede hacer referencia a tres cosas diferentes pero ligadas entre sí: puede referirse al trabajo que realiza un auditor, a la tarea de estudiar la economía de una empresa, o a la oficina donde se realizan estas tareas. Pérez, J. (2009)
- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Pérez, J. (2009)
- Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa. Aceituno, V. (2003)

- ENAC: Entidad Nacional de Acreditación. Es el organismo español de acreditación, auspiciado por la Administración, que acredita organismos que realizan actividades de evaluación de la conformidad, sea cual sea el sector en que desarrollen su actividad. Además de laboratorios, entidades de inspección, etc., también acredita a las entidades de certificación, que son las que a su vez certificarán a las empresas en las diversas normas. Gaspar, J. (2012)
- Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos. Aceituno, V. (2003)
- Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. Pérez, J. (2009)
- Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales. Aceituno, V. (2003)
- Integridad: Propiedad de la información relativa a su exactitud y completitud.
- Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. Gaspar, J. (2012)
- ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas). Aceituno, V. (2003)
- ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial. Pérez, J. (2009)
- ITIL: Un marco de gestión de los servicios de tecnologías de la información. Gaspar, J. (2012)
- PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él. Pérez, J. (2009)
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse

como una combinación de la probabilidad de un evento y sus consecuencias. Gaspar, J. (2012)

- SGSI: Sistema de Gestión de la Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. Aceituno, V. (2003)
- Vulnerabilidad: Debilidad de un activo o control suceptible de ser explotada por una o más amenazas. Gaspar, J. (2012)

CAPÍTULO III

PRESENTACIÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

3.1 VALIDEZ Y CONFIABILIDAD DE INSTRUMENTOS

Para recopilar la información se aplicó la Técnica de Encuesta, con sus correspondientes Instrumentos. Todo instrumento de recolección de datos debe asumir dos propiedades esenciales: validez y confiabilidad.

Con la **validez** se determina la revisión de la presentación del Contenido, el contraste de los indicadores con los ítems que miden las variables correspondientes. Hernández, S. (2006) expresó la validez como el grado de precisión con el que el test utilizado mide realmente lo que está destinado medir. Lo expresado anteriormente define la validación de los instrumentos, como la determinación de la capacidad de los instrumentos para medir las cualidades para lo cual fueron construidos.

Los instrumentos de medición utilizados (cuestionario, pruebas escritas) fueron validados mediante el procedimiento conocido como juicio de expertos.

A los expertos se les suministró los instrumentos (matriz) de validación donde se evaluó la coherencia entre los reactivos, las variables, las dimensiones y los indicadores, presentadas en la matriz de operacionalización de las variables, así

como los aspectos relacionados con la calidad técnica del lenguaje (claridad de las preguntas y la redacción).

La validación del instrumento se realizó en base al marco teórico, considerándose la categoría de "validez de contenido". Se utilizó el procedimiento de juicio de expertos calificados quienes determinaron el coeficiente de confiabilidad a partir del análisis y evaluación de los ítems del respectivo instrumento.
A los expertos se les entregó un formato solicitando que evaluaran los instrumentos en su totalidad. De los resultados procesados podemos concluir que el cuestionario es válido, sobre la Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información, y sobre la gestión de servicios en el CASE de la FAP.

Confiabilidad

Con respecto a la **Confiabilidad** se estima que un instrumento de medición es confiable cuando permite determinar que el mismo, mide lo que el investigador quiere medir, y que, aplicado varias veces, replique el mismo resultado.
Por medio del método test retest calculamos la confiabilidad de cada instrumento:
Cálculos de la confiabilidad de los instrumentos:

Cuestionario Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información:

Tabla 2 Norma ISO 27001:2013

		Item1a	Item1b
Item1a	Correlación de Pearson	1	,820**
	Sig. (bilateral)		,004
	N	30	30
Item1b	Correlación de Pearson	,820**	1
	Sig. (bilateral)	,004	
	N	30	30

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

Cuestionario gestión de servicios:

Tabla 3
Gestión de Servicios

		Item2a	Item2b
Item2a	Correlación de Pearson	1	,724*
	Sig. (bilateral)		,018
	N	30	30
Item2b	Correlación de Pearson	,724*	1
	Sig. (bilateral)	,018	
	N	30	30

*. * La correlación es significante al nivel 0,05 (bilateral).

Criterio de confiabilidad valores

0,81 a 1,00 Muy Alta confiabilidad
0,61 a 0,80 Alta confiabilidad
0,41 a 0,60 Moderada confiabilidad
0,21 a 0,40 Baja confiabilidad
0,01 a 0,20 Muy Baja

Como observamos los tres instrumentos tienen una muy alta confiabilidad.

3.1.1 NIVEL DE CONFIANZA Y GRADO DE SIGNIFICANCIA

La ficha técnica sobre la cual es probados los datos recolectados para la prueba de hipótesis, esta diseñada de la siguiente manera:

Nivel de confianza: **95%**

Significancia: **5%**

3.1.2 TAMAÑO DE LA MUESTRA REPRESENTATIVA

Teniendo en consideración las características de la población, de la muestra, del nivel de confianza y la significancia, con el propósito de que los resultados estén respaldados estadísticamente, esto es, que sean representativos, se ha seleccionado la fórmula de garantía de tamaño de muestra óptima:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Esta expresión, es una síntesis de garantía según tamaño de la muestra, para un nivel de aceptación del 95% y un limite de error de ±5 [12], teniendo en consideración que, la unidad de análisis del trabajo de investigación, son transacciones que tiene mucha afinidad de comportamiento con las técnicas de medición del trabajo.

3.2 ANÁLISIS DE TABLAS Y GRÁFICOS - INTERPRETACIONES

A continuación se despliegan los resultados obtenidos de la prueba de campo realizada, tanto para la variable independiente como para los grupos de control y experimental de la variable dependiente, aplicando las métricas correspondientes a los indicadores seleccionados. Dichos resultados son sometidos a un minucioso análisis para extraer los principales rasgos de su comportamiento y, de este modo tener elementos de juicio para interpretar de manera global el comportamiento de las dos variables involucradas.

3.2.1 PARA LA VARIABLE INDEPENDIENTE

X= Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información.

Índices:

- Funciones adecuadas
- Niveles de acceso
- Comprensibilidad

A. Para el indicador Productividad.

1. Índice: Promedio mensual de documentos emitidos

Para la población infinita, tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Dónde:

N = Número de observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

[12] Arriaza B. (2006). *Guía Práctica de Análisis de Datos.* Argentina: Editorial IFAPA.

De la hoja de muestreo (Ver anexo Nº 2), para 30 muestras tenemos:

Tabla 04

Promedio mensual documentos emitidos

N	30
Suma X	2760
Suma x^2	258300

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{664} \sqrt{\frac{15978 - \frac{(664)^2}{30}}{30-1}} \right]^2$$

N= 28,55094192034 42 ≈ 29

Para N = 30, observamos que N' es 29, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Realizando un análisis más exhaustivo de los datos obtenidos de las muestras, tomando aleatoriamente 30 observaciones con respecto al comportamiento del promedio mensual de documentos emitidos, obtenemos los siguientes resultados:

Tabla 05

Estadística Descriptiva

Promedio mensual de documentos emitidos	
Media	90
Error típico	1.889822
Mediana	90
Moda	90
Desviación estándar	10
Varianza de la muestra	100
Curtosis	5.06769
Coeficiente de asimetría	0
Rango	60
Mínimo	60
Máximo	120
Suma	2520
Nivel de confianza (95%)	3.877595

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 03 el número de observaciones es de 30, el tiempo máximo es de 120, mientras que el tiempo mínimo es de 60. El promedio es de 90 min. Se considera cinco clases, teniendo un rango de 10 minutos.

Tabla 06

Rango de clases del índice "Promedio mensual de documentos emitidos"

Observaciones	30
Máximo	120
Mínimo	60
Media	90
Nro de Clases	5

Fuente: Elaboración Propia, 2016

En la tabla 04 se presenta la tabla de distribución de frecuencias.

Tabla 07

Frecuencias de clases del índice "Promedio mensual de documentos emitidos"

Clases	f	fr	F	Fr
60 – 70	1	1	3.33	3.33
70 – 80	2	3	6.67	10.00
80 – 90	22	25	73.33	83.33
90 – 100	0	25	0.00	83.33
100 – 120	5	30	16.67	100.00
Total	30		100.00	

Fuente: Elaboración Propia, 2016

B. Para el Indicador Eficiencia

1. Índice: Promedio mensual de documentos recibidos

Para la población infinita tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Dónde:

N = Número de Observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

De la hoja de muestreo, para 30 muestras tenemos:

Tabla 08

N	30
Suma X	507
Suma x^2	8717

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{507} \sqrt{\frac{8717 - \frac{(507)^2}{30}}{30-1}} \right]^2$$

$$N = 28{,}7249673717115 \approx 29$$

Para N = 30, observamos que N' es 29, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Realizando un análisis más exhaustivo de los datos obtenidos de las muestras, tomando aleatoriamente 30 observaciones con respecto al comportamiento del Promedio mensual de documentos recibidos, obtenemos los siguientes resultados:

En la tabla 09, observamos que el promedio del índice "Promedio mensual de documentos recibidos" es de 16.9 (17 documentos no atendidos), la mediana es de 17, el tiempo con mayor frecuencia o moda es de 17 min. Con una desviación estándar de 2.26.

Tabla 09

ESTADÍSTICAS DESCRIPTIVAS

Promedio mensual de documentos recibidos	
Media	16.9
Error típico	0.413424
Mediana	17
Moda	17
Desviación estándar	2.26441
Varianza de la muestra	5.12758
Curtosis	9.40701
Coeficiente de asimetría	-2.99855
Rango	11
Mínimo	9
Máximo	20
Suma	507
Nivel de confianza (95%)	0.84554

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 09 el número de observaciones es de 30, el número de accesos no atendidos es un máximo de 20, mientras que el mínimo es de 9. El promedio es de 16.9 accesos no atendidos no atendidos. Se considera cinco clases, teniendo un rango de 11.

Tabla 10

Rango de clases del índice "Promedio mensual de documentos recibidos"

Observaciones	30
Máximo	20
Mínimo	9
Media	16.9
Nro de Clases	5

Fuente: Elaboración Propia, 2016

En la tabla 11 se presenta la tabla de distribución de frecuencias.

Tabla 11

Frecuencias de clases del índice "Promedio mensual de documentos recibidos"

Clases	f	fr	F	Fr
9 – 11.75	2	2	6.67	6.67
11.75 – 14.5	0	2	0.00	6.67
14.5 – 17.25	16	18	53.33	60.00
17.25 – 20	12	30	40.00	100.00
Total	30		100.00	

Fuente: Elaboración Propia, 2016

C. Para el indicador Eficacia

1. Índice: Tiempo de respuesta promedio ante un requerimiento

Para la población infinita tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Dónde:

N = Número de Observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

De la hoja de muestreo, para 30 muestras tenemos:

Tabla 12

N	30
Suma X	2090
Suma x^2	147700

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{2090} \sqrt{\frac{147700 - \frac{(2090)^2}{30}}{30-1}} \right]^2$$

N= 23,834240248068 ≈ 24

Para N = 30, observamos que N' es 24, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Realizando un análisis más exhaustivo de los datos obtenidos de las muestras, tomando aleatoriamente 30 observaciones con respecto al comportamiento del Promedio mensual de documentos recibidos, obtenemos los siguientes resultados:

En la tabla 13 observamos que el promedio del índice "Tiempo de respuesta promedio ante un requerimiento" es de 70, la mediana es de 70, el tiempo con mayor frecuencia o moda es de 70, con una desviación estándar de 8.5.

Tabla 13

ESTADÍSTICAS DESCRIPTIVAS

Tiempo de respuesta promedio ante un requerimiento	
Media	69.66667
Error típico	1.552405
Mediana	70
Moda	70
Desviación estándar	8.50287
Varianza de la muestra	72.2988
Curtosis	0.90343
Coeficiente de asimetría	-1.06088
Rango	30
Mínimo	50
Máximo	80
Suma	2090
Nivel de confianza (95%)	3.175024

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 13 el número de observaciones es de 30, el tiempo de respuesta promedio ante un requerimiento máximo es de 20, mientras que el mínimo es de 50. El promedio es de 70 al tiempo de respuesta ante un requerimiento. Se considera cinco clases, teniendo un rango de 10 minutos.

Tabla 14

Rango de clases del índice "Tiempo de respuesta promedio ante un requerimiento"

Observaciones	30
Máximo	80
Mínimo	50
Media	69.66667
Nro de Clases	5

Fuente: Elaboración Propia, 2016

En la tabla 15 se presenta la tabla de distribución de frecuencias.

Tabla 15

Frecuencias de clases del índice "Promedio mensual de documentos recibidos"

Clases	f	fr	F	Fr
50 – 60	4	4	13.33	13.33
60 – 70	13	17	43.33	56.67
70 – 80	12	29	40.00	96.67
80 – 90	0	29	0.00	96.67
90 - 100	1	30	3.33	100.00
	30		100.00	

Fuente: Elaboración Propia, 2016

3.2.2 VARIABLE DEPENDIENTE

A. Para el indicador Productividad.

1. Índice: Tiempo empleado para elaboración de documentos

Para la población infinita, tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Dónde:

N = Número de Observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

De la hoja de muestreo (Ver Anexo Nº 4), para 30 muestras tenemos:

Tabla 16

N	30
Suma X	131
Suma x^2	581

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{581} \sqrt{\frac{581 - \frac{(131)^2}{30}}{30-1}} \right]^2$$

$$N = 25{,}9449553819909 \approx 26$$

Para N = 30, observamos que N' es 26, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Después de tomar aleatoriamente 30 observaciones con respecto al comportamiento de los tiempos empleado en hacer una tarea, obtenemos los siguientes resultados:

En la tabla 17, observamos que el promedio del índice "Tiempo empleado para elaboración de documentos" es de 7.57 minutos, la mediana es de 4min., el tiempo con mayor frecuencia o moda es de 4 min., con una desviación estándar de 0.56.

Tabla 17

ESTADISTICAS DESCRIPTIVAS

Tiempo empleado para elaboración de documentos	
Media	4.366667
Error típico	0.101521
Mediana	4
Moda	4
Desviación estándar	0.556053
Varianza de la muestra	0.309195
Curtosis	-0.796384
Coeficiente de asimetría	-0.073540
Rango	2
Mínimo	3
Máximo	5
Suma	131
Nivel de confianza (95%)	0.207633

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 18 el número de observaciones es de 30, el tiempo máximo es de 5, mientras que el mínimo es de 3. El promedio es de 4.366667. Se considera cinco clases, teniendo un rango de 10 minutos.

Tabla 18

Rango de clases del índice "Tiempo empleado para elaboración de documentos"

Observaciones	30
Máximo	5
Mínimo	3
Media	4.366667
Nro de Clases	5

Fuente: Elaboración Propia, 2016

En la tabla Nª 19 se presenta la tabla de distribución de frecuencias.

Tabla 19

Frecuencias de clases del índice "Tiempo empleado para elaboración de documentos"

Clases	f	fr	F	Fr
3 – 3.67	1	1	3.33	3.33
3.67 – 4.34	17	18	56.67	60.00
4.34 – 5.01	12	30	40.00	100.00
Total	30		100.00	

Fuente: Elaboración Propia, 2016

B Para el Indicador Eficiencia

1. Índice: Promedio mensual de documentos recibidos

Para la población infinita tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Donde:

N = Número de Observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

De la hoja de muestreo (Ver Anexo Nº 5), para 30 muestras tenemos:

Tabla 20

N	30
Suma X	147
Suma x^2	729

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{664} \sqrt{\frac{15978 - \frac{(664)^2}{30}}{30-1}} \right]^2$$

$$N = 19{,}9916701374428 \approx 20$$

Para N = 30, observamos que N' es 20, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Después de tomar aleatoriamente 30 observaciones con respecto al promedio mensual de documentos recibidos, obtenemos los siguientes resultados:

En la tabla Nª 21, observamos que el promedio del índice "Promedio mensual de documentos recibidos" es de 4.9, la media es de 5, el tiempo con mayor frecuencia o moda es de 5, con una desviación estándar de 0.55.

Tabla 21

ESTADÍSTICAS DESCRIPTIVAS

Promedio mensual de documentos recibidos	
Media	4.9
Error típico	0.1
Mediana	5
Moda	5
Desviación estándar	0.54772
Varianza de la muestra	0.3
Curtosis	0.58930
Coeficiente de asimetría	-0.08094
Rango	2
Mínimo	4
Máximo	6
Suma	147
Nivel de confianza (95%)	0.20452

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 22 el número de observaciones es de 30, el número de accesos no atendidos es un máximo de 6, mientras que el mínimo es de 4. El promedio es de 4.9 accesos no atendidos no atendidos. Se considera cinco clases, teniendo un rango de 2.

Tabla 22

Rango de clases del índice "Promedio mensual de documentos recibidos"

Observaciones	30
Máximo	6
Mínimo	4
Media	4.9
Nro de Clases	5

Fuente: Elaboración Propia, 2016

En la tabla 23 se presenta la tabla de distribución de frecuencias.

Tabla 23

Frecuencias de clases del índice "Promedio mensual de documentos recibidos"

Clases	f	fr	F	Fr
4 – 4.67	6	6	20.00	20.00
4.67 – 5.34	21	27	70.00	90.00
5.34 – 6.01	3	30	10.00	100.00
Total	30		100.00	

Fuente: Elaboración Propia, 2016

C Para el indicador Eficacia

1. Índice: Tiempo de respuesta promedio ante un requerimiento

Para la población infinita tenemos:

$$N' = \left[\frac{40N}{\sum x} \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N-1}} \right]^2$$

Dónde:

N = Número de Observaciones (30)

X = Tiempos tomados de referencia (748 min.)

Nivel de confianza = 95%

Error estándar = ±5

De la hoja de muestreo (Ver Anexo Nº 3), para 30 muestras tenemos:

Tabla 24

N	30
Suma X	695
Suma x^2	16275

Fuente: Elaboración Propia, 2016

Aplicando la fórmula descrita, se obtiene el siguiente resultado:

$$N' = \left[\frac{40(30)}{16275} \sqrt{\frac{16275 - \frac{(695)^2}{30}}{30-1}} \right]^2$$

$$N = 17{,}90440631865\,62 \approx 18$$

Para N = 30, observamos que N' es 18, lo cual significa que el tamaño de muestra es significativo, y suficiente para poder inferir algo acerca de la población.

Estadísticas Descriptivas

Después de tomar aleatoriamente 30 observaciones con respecto al comportamiento del promedio mensual de documentos recibidos, obtenemos los siguientes resultados:

En la tabla 25, observamos que el promedio del índice "Tiempo de respuesta promedio ante un requerimiento" es de 23, la mediana es de 25, el tiempo con mayor frecuencia o moda es de 25, con una desviación estándar de 2.45.

Tabla 25

ESTADÍSTICAS DESCRIPTIVAS

Tiempo de respuesta promedio ante un requerimiento	
Media	23.166667
Error típico	0.447427
Mediana	25
Moda	25
Desviación estándar	2.45066
Varianza de la muestra	6.00574
Curtosis	-1.78400
Coeficiente de asimetría	-0.58293
Rango	5
Mínimo	20
Máximo	25
Suma	695
Nivel de confianza (95%)	0.91509

Fuente: Elaboración Propia, 2016

Rango de clases y frecuencias

En la tabla 26 el número de observaciones es de

Frecuencias de clases del índice "Promedio mensual de documentos recibidos"

Clases	f	fr	F	Fr
20 – 21.67	11	11	36.67	36.67
21.67 – 23.34	0	11	0.00	36.67
23.34 – 25.01	19	30	63.33	100.00
Total	30		100.00	

Fuente: Elaboración Propia, 2016

3.3 PRUEBA DE HIPÓTESIS

Una hipótesis en el contexto de la estadística inferencial es una proposición respecto a uno o varios parámetros, y lo que el investigador hace a través de la prueba de hipótesis, es determinar si la hipótesis es consistente con los datos obtenidos en la muestra [[13]], para ello, a continuación se formula la hipótesis de investigación, la hipótesis nula y las correspondientes hipótesis estadísticas.

Las hipótesis científicas se someten a prueba o escrutinio empírico si son apoyadas o refutadas de acuerdo a lo que el investigador observa. En consecuencia, se procede a formular la hipótesis de investigación y la correspondiente hipótesis estadística.

3.3.1 HIPÓTESIS DE INVESTIGACIÓN

H_i = La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en el Centro de Administración de Servicios Educativos FAP.

3.3.2 HIPÓTESIS NULA

H_0 = La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información no influirá significativamente en la Gestión de Servicios en el Centro de Administración de Servicios Educativos FAP.

3.3.3 HIPÓTESIS ESTADÍSTICA

$H_i : r\ X\ Y \neq 0$

[13] Como nos dicen Hernández R., Fernández C., Baptista P. (2010) *Metodología de la Investigación***.** México: Mc Graw Hill.

Existe correlación (r) entre la variable independiente (X) (Norma ISO 27001:2013 como soporte al proceso de seguridad de la información) y la variable dependiente (Y) (Gestión de servicios en el CASED)

H_i : r X Y = 0

No existe correlación (r) entre la variable independiente (X) (Norma ISO 27001:2013 como soporte al proceso de seguridad de la información) y la variable dependiente (Y) (Gestión de servicios en el CASED)

3.4 PRUEBAS ESTADÍSTICAS UTILIZADAS

Para compatibilizar el tipo de investigación y el diseño seleccionado, se ha utilizado como método de prueba estadística de la hipótesis, la denominada prueba de "t" de Student, cuya formula es:

$$t = \frac{X_1 - X_2}{\sqrt{\frac{\delta_1^{\,2}}{N_1} + \frac{\delta_2^{\,2}}{N_2}}}$$

Dónde:

X_1 = Media de la variable dependiente

X_2 = Media de la variable dependiente

S_1^2 = Desviación estándar de la variable dependiente

S_2^2 = Desviación estándar de la variable dependiente

N_1 = Número de observaciones de la variable dependiente

N_2 = Número de observaciones de la variable independiente

3.4.1 PRUEBA DE HIPÓTESIS PARA EL INDICADOR DE PRODUCTIVIDAD

1. **Índice: Promedio mensual de documentos emitidos**

   Aplicando la formula T de Student:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_1^2}{N_1} + \frac{S_2^2}{N_2}}}$$

Teniendo en cuenta las estadísticas descriptivas para ambas variables tenemos: (con N = 30)

Tabla 28

Estadística Descriptiva	Variable Independiente	Variable Dependiente
Media	90	4.3666667
Desv. Estándar	10	0.5560534
Varianza Muestra	100	0.3091954
Observaciones	30	30

Fuente: Elaboración Propia, 2016

Aplicando la fórmula de T-Student obtenemos:

$$t = \frac{90 - 4.366666667}{\sqrt{\frac{100}{30} + \frac{0.309195402}{30}}}$$

$$t = 46{,}5414297791027$$

Calculando los grados de libertad:

GL = (N1 + N2) – 2

GL = 58

Ubicándolo en la tabla T-Student al 95% de confianza obtenemos:

Al comparar 46.54 con el valor obtenido por la tabla 28, a un nivel de confianza del 95% se aprecia que es mayor por lo tanto no existe diferencias entre las medias, lo cual significa que se acepta la hipótesis de investigación para este índice, rechazándose la hipótesis nula.

3.4.2 PRUEBA DE HIPÓTESIS PARA LA EFICIENCIA

1. Índice: Promedio mensual de documentos recibidos

Aplicando la formula T de Student:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_1^2}{N_1} + \frac{S_2^2}{N_2}}}$$

Teniendo en cuenta las estadísticas descriptivas para ambas variables tenemos: (con N = 30)

Tabla 29

Estadística Descriptiva	Variable Independiente	Variable Dependiente
Media	16.9	4.9
Desv. Estándar	2.2644	0.5477
Varianza Muestra	5.1275	0.3
Observaciones	30	30

Fuente: Elaboración Propia, 2016

Aplicando la fórmula de T-Student obtenemos:

$$t = \frac{16.9 - 4.9}{\sqrt{\frac{5.12758621}{30} + \frac{0.3}{30}}}$$

t= 28,2123009678692

Calculando los grados de libertad:

GL = (N1+N2) – 2

GL = 58

Ubicándolo en la tabla T-Student al 95% de confianza obtenemos:

Al comparar 28.21 con el valor obtenido por la tabla 29, a un nivel de confianza del 95% se aprecia que es mayor por lo tanto no existe diferencias entre las medias, lo cual significa que se acepta la hipótesis de investigación para este índice, rechazándose la hipótesis nula.

3.4.3 PRUEBA DE HIPÓTESIS PARA EL INDICADOR EFICACIA

1. Índice: Tiempo de respuesta promedio ante un requerimiento

Aplicando la formula T de Student:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_1^2}{N_1} + \frac{S_2^2}{N_2}}}$$

Teniendo en cuenta las estadísticas descriptivas para ambas variables tenemos: (con N = 30)

Tabla 30

Estadística Descriptiva	Variable Independiente	Variable Dependiente
Media	69.6667	23.1667
Desv. Estándar	8.5028	2.4506
Varianza Muestra	72.2988	6.0057
Observaciones	30	30

Fuente: Elaboración Propia, 2016

Aplicando la fórmula de T-Student obtenemos:

$$t = \frac{69.6666667 - 23.16666667}{\sqrt{\frac{72.2988506}{30} + \frac{6.005747126}{30}}}$$

t= 28,781932406069

Calculando los grados de libertad:

GL = (N1+N2) – 2

GL = 58

Ubicándolo en la tabla T-Student al 95% de confianza obtenemos:

Al comparar 28.78 con el valor obtenido por la tabla 30, a un nivel de confianza del 95% se aprecia es mayor por lo tanto no existe diferencias entre las medias, lo cual significa que se acepta la hipótesis de investigación para este índice, rechazándose la hipótesis nula.

3.5 DISCUSIÓN

A la luz de los resultados obtenidos en los diversos aspectos investigados sobre los indicadores: productividad, eficiencia y eficacia de la variable "Gestión de servicios", se ha comprobado, mediante un 82%, que la hipótesis general es validada, y ratifica una relación significativa sobre la norma ISO 27001:2013 como soporte al proceso de seguridad de la información, asimismo, al converger tales generalizaciones empíricas con la Teoría de Gestión de servicios de Toranzos y las teorías de Milicic y Fernández se hace más consistente este resultado; estas demostraciones empíricas son corroboradas con los antecedentes de las investigaciones de Milian y Vega (2009), quienes en su investigación concluyen que existe relación significativa entre ambas variables.

Hace más sólido los resultados, lo que manifiesta Lafourcade (1988), en su obra "Calidad de la Educación" cuando dice que "una educación de calidad puede significar la que posibilite el dominio de un saber desinteresado que se manifiesta en la adquisición de una cultura científica o literaria, la que desarrolla la máxima capacidad para generar riquezas o convertir a alguien en un recurso humano idóneo para contribuir al aparato productivo…"

Respecto del indicador 'productividad', en contraste con la hipótesis " La productividad de la gestión de servicios se relaciona significativamente con la norma ISO 27001:2013 como soporte al proceso de seguridad de la información en los CASED de la FAP, según los resultados obtenidos producto de la contratación de la hipótesis, se relaciona satisfactoriamente, corroborado con lo que manifiesta Layomi (2009): es muy importante la serie de valores, normas, pautas ideológicas, objetivos e ideas de la institución, es decir cómo se relaciona con la sociedad y como participa en la problemática educativa.

Respecto del indicador 'eficiencia´, en contraste con la hipótesis " La eficiencia de la calidad educativa se relaciona significativamente con el gestión de servicios en la norma ISO 27001:2013 como soporte al proceso de seguridad de la información en los CASED de la FAP según los resultados obtenidos se establece un grado de

relación significativa, respaldado con lo manifestado por Ruiz y Arévalo (1989), una persona que es aceptado cordialmente en un grupo de gestión de servicios, que forma parte de un clima estudiantil adecuado, eleva su nivel de seguridad.

Respecto del indicador ‘eficacia’, en contraste con la hipótesis " La eficacia de la gestión de servicios se relaciona significativamente con la norma ISO 27001:2013 como soporte al proceso de seguridad de la información en los CASED de la FAP según los resultados obtenidos se ratifica una relación significativa sobre la calidad educativa, particularmente cuando los cadetes manifiestan que participan activamente en las clases y comunican a sus profesores de sus logros.

CONCLUSIONES

1. El diseño de un Sistema de Gestión de la Seguridad de la Información como solución garantiza el cumplimiento de los objetivos de la organización, estableciendo una metodología de gestión de la seguridad clara y estructurada, manteniendo los niveles de competitividad, conformidad legal e imagen institucional.

2. La seguridad de la información es tema crítico dentro de las organizaciones, y por tanto deben establecerse requisitos de seguridad en la parte legal como normativas, estatutos, regulaciones y contratos los cuales satisfagan a las organizaciones, los contratistas y los proveedores de servicios, de tal forma garantizan la seguridad de los activos, la exactitud y confiabilidad de sus registros y la aceptación de las normas.

3. La información, junto a los procesos y sistemas hacen uso de ella son activos importantes de una organización los cuales identificados permiten realizar un análisis de riesgo reduciendo los riesgos de perdida, robo o corrupción de información y así garantizar la confianza de los clientes.

4. En una organización existen recursos humanos, recursos técnicos e infraestructura expuestos a diferentes tipos de riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, virus informáticos, espionajes, sabotaje, vandalismo y otros. La dependencia de los sistemas y servicios de información implica la vulnerabilidad de ante amenazas de seguridad, y al compartir sus recursos de información e interconectar las redes públicas (Internet) con las privadas.

RECOMENDACIONES

1. Al Centro de Administración de Servicios Educativos FAP, compromiso y apoyo estableciendo políticas de seguridad, responsabilidades legales y necesidad de mejora continua desarrollando las buenas prácticas. Reconociendo como proceso, la seguridad no es un proyecto es una actividad continua.

2. La implementación mediante la Presidencia del Consejo de Ministros (PCM) a través de la Oficina Nacional de Gobierno Electrónico, dispone del uso obligatorio de la Norma Técnica Peruana ISO 17799:2004 para ser implementada en Entidades Públicas. Esta norma se ha basado en la norma internacional ISO/IEC 17799:2000.

3. El reconocimiento de todo el personal estar en conocimiento de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI y las consecuencias de no seguir los lineamientos de seguridad.

4. Los problemas son minimizados por medio del análisis de riesgos y responder a tres cuestiones básicas sobre nuestra seguridad:

    - ¿Qué queremos proteger?
    - ¿Contra quién o qué lo queremos proteger?
    - ¿Cómo lo queremos proteger?

    Debemos planificar no sólo la prevención ante un problema sino también la recuperación si el mismo se produce, y recuperarnos de ese incidente en el menor tiempo posible y el menor costo, por ello es necesaria que las instituciones cuenten con un plan de continuidad del negocio cuando se han producido desastres o fallas de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Aceituno, V. (2004). *Definición de seguridad de la información y sus limitaciones*. Recuperado de: http://www.fistconference.org/data/presentaciones/queesseguridad.pdf.

Asensio, G. (2006). *Seguridad en Internet*. Ediciones Nowtilus S.L. Madrid, España.

Arévalo, E. (1990). *Estudio acerca de los rasgos de personalidad en la clasificación grupal de aceptados, rechazados y aislados en estudiantes secundarios de ambos sexos*. Lima, Perú: CONCYTEC.

Arévalo, E. (2002).*Clima escolar y niveles de interacción social en estudiantes de secundaria del Colegio Claretiano de Trujillo*. Tesis de maestría. UNMSM, Lima, Perú.

Berman, D. (1997). *El hombre y la paz*. Paris, Francia: UNESCO

Bernstein, B. (2007) Hacia una Teoría del Discurso Pedagógico. *Revista colombiana de Educación* No.233. U.P.N. Bogotá, Colombia.

Bowen, J. & Hobson, P. (1995). *Teorías de la Educación* (Innovaciones Importantes en el Pensamiento Educativo Occidental). Buenos Aires, Argentina: Limusa.

Carrasco A. (2004). Covariación del consumo del alcohol con otras conductas de salud en adolescentes y factores psicosociales asociados. *Revista Psicología y salud*, 12(2):203:212.

Casassus, J. & Arancibia, V. (1997). *Claves para una Educación de Calidad*. Buenos Aires, Argentina: Kapelusz.

Chiavenato, I. (2006) *Introducción a la teoría general de la administración.* México: Séptima Edición. McGRAW-HILL.

Córdova, N. (8 de Junio de 2006). *Plan de seguridad informática para una entidad financiera*. Recuperado de: http://sisbib.unmsm.edu.pe/bibvirtual/Tesis/Basic/cordova_rn/cordova_rn.htm

Portal de ISO 27000. (20 de octubre 2011). Recuperado de: http://www.iso27000.es/iso27000.html.

Gaspar, J. (2008). *Planes de Contingencia*. España: Díaz de Santos.

Huidobro J. (2002). *"Seguridad Aplicada a la Información"*. España. Editorial Paraninfo.

Hernández, Fernández & Baptista (2014). *Metodología de la investigación científica*. DF, México. Mc Graw-Hill 6ta Ed.

Lafourcade, P. (1988) *Calidad de la Educación*, Buenos Aires, Argentina: Dirección Nacional de Información, difusión estadística y tecnología educativa del Ministerio de Educación y Justicia.

López, F. (1994). *La gestión de la calidad en la educación*. Madrid, España: Editorial La Muralla.

Lafout, E. (1999). *La convivencia como criterio de enseñanza en los colegios*, Madrid, España: Universidad Autónoma de Madrid.

Laudon K. y Laudon J. (2012). *Sistemas de Información Gerencial*. Decimosegunda edición, México: Pearson Educación.

MCleod, R. (2009). *Sistemas de información gerencial*. Séptima Edición. México: Prentice May Hispanoamericana.

Molina, J. (2010). *Seguridad de la información*. *Criptología*. España: El Cid Editor.

Pérez, J. (2009). *La Biblia del Hacker*. España: Anaya Multimedia.

Peso, E. (2008). *Servicios de la sociedad de la información.* España: Díaz de Santos.

Rutty, M. (2007) *Evaluación de impacto en la capacitación de recursos humanos*, en su tesis. para obtener el grado académico de magister en la universidad inca Garcilaso de la vega. Lima, Perú.

Schmelkes, S. (1997) *Programa de evaluación de la calidad de la educación*. DF, México: Cumbre Iberoamericana.

Toranzos (Enero/abril 1996). Evaluación y calidad. Revista Iberoamericana de Educación. 63-78.

Rodríguez, J. (2008). *Administración I.* México: Thomson Learning Ibero.

SYMANTEC CORPORATION. "Universidades abordan el problema del robo de identidad". (03 de Marzo 2010). Recuperado de: http://www.symantec.com/region/mx/enterprisesecurity/content/government/LAM_3583.html

Universidad Carlos III de Madrid**.** (12 de Junio 2011). La innovación al servicio del alumno. Recuperado de: http://www.microsoft.com/spain/enterprise/casestudies/cs_uni_carlosiii01.aspx

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

LA NORMA ISO 27001 COMO SOPORTE AL PROCESO DE LA SEGURIDAD DE LA INFORMACIÓN Y SU INFLUENCIA EN LA GESTIÓN DE SERVICIOS EN EL CENTRO DE ADMINISTRACIÓN DE SERVICIOS EDUCATIVOS DE LA FUERZA AÉREA DEL PERÚ

PROBLEMA PRINCIPAL	OBJETIVO PRINCIPAL	HIPÓTESIS PRINCIPAL	VARIABLES	INDICADORES	METODOLOGÍA
¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios del Centro de Administración de Servicios Educativos FAP?	Determinar como la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios del Centro de Administración de Servicios Educativos FAP.	La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios del Centro de Administración de Servicios Educativos FAP.	Independiente:(X) **Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información**. DIMENSIONES • Fiabilidad • Seguridad • Usabilidad Dependiente:(Y) **Gestión de Servicios.** DIMENSIONES • Productividad • Eficiencia • Eficacia	**Dimensiones e Indicadores Variable Independiente.** FIABILIDAD • Funciones adecuadas. SEGURIDAD • Niveles de acceso. USABILIDAD • Comprensibilidad **Dimensiones e indicadores Variable Dependiente.** PRODUCTIVIDAD • Promedio mensual de documentos emitidos. EFICIENCIA • Promedio mensual de documentos recibidos. EFICACIA • Tiempo de repuesta promedio ante un requerimiento.	**Tipo de Investigación:** Básica. **Nivel de Investigación:** Descriptiva Correlacional, Transeccional. **Método de Investigación:** Hipotético deductivo. **Técnicas de recolección de datos:** Encuesta estructurada. **Instrumento:** Cuestionario. Tipo Likert **Población:** Todos los 80 **Muestra:** No probabilística
ESPECIFICOS	**ESPECIFICOS**	**ESPECIFICOS**			
¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Productividad del Centro de Administración de Servicios Educativos FAP?	Determinar como la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Productividad del Centro de Administración de Servicios Educativos FAP	La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la Productividad del Centro de Administración de Servicios Educativos FAP.			
¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Eficiencia del Centro de Administración de Servicios Educativos FAP?	Determinar como la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Eficiencia del Centro de Administración de Servicios Educativos FAP	La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la Eficiencia del Centro de Administración de Servicios Educativos FAP.			
¿De qué manera la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Eficacia del Centro de Administración de Servicios Educativos FAP?	Determinar como la Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influye en la Gestión de Servicios en la Eficacia del Centro de Administración de Servicios Educativos FAP	La Norma ISO 27001:2013 como Soporte al proceso de la Seguridad de la Información influirá significativamente en la Gestión de Servicios en la Eficacia del Centro de Administración de Servicios Educativos FAP.			

CUESTIONARIO

El presente cuestionario tiene como finalidad conocer cuál es la percepción de los trabajadores de la seguridad de los activos de información, sobre el conocimiento de los trabajadores de políticas de seguridad, acciones para salvaguardar los activos de información y acciones de reducción de las vulnerabilidades.

TÍTULO DE LA INVESTIGACIÓN: "LA NORMA ISO 27001 COMO SOPORTE AL PROCESO DE LA SEGURIDAD DE LA INFORMACIÓN Y SU INFLUENCIA EN LA GESTIÓN DE SERVICIOS EN EL CENTRO DE ADMINISTRACIÓN DE SERVICIOS EDUCATIVOS DE LA FUERZA AÉREA DEL PERÚ"

INSTRUCCIONES: Estimado(a) trabajador(a) del Centro de Administración de Servicios Educativos de la FAP, se le solicita responder con sinceridad cada pregunta planteada, debiendo colocar tu respuesta en los cuadros en blanco o rellenar los espacios, según sea el caso. Evite en lo posible enmendadura. Gracias.

I. CARACTERÍSTICAS SOCIODEMOGRÁFICAS

¿A qué género perteneces?

Masculino ☐ Femenino ☐

¿Cuántos años tienes? ☐

¿Cuál es su grado de instrucción?

Primaria ☐ Técnico ☐ Militar ☐

Secundaria ☐ Superior ☐

II. PREGUNTAS RESPECTO A LOS INDICADORES DE LA VARIABLE INDEPENDIENTE: **Norma ISO 27001:2013 como Soporte al Proceso de Seguridad de la Información.**

1. ¿Las políticas de seguridad deben ser publicadas y comunicadas a todos los usuarios?
   - ☐ Totalmente de acuerdo
   - ☐ De acuerdo
   - ☐ Ni de acuerdo ni en desacuerdo
   - ☐ En desacuerdo
   - ☐ Totalmente en desacuerdo
2. ¿Las políticas de seguridad deben ser revisadas regularmente o a intervalos planeados?
   - ☐ Totalmente de acuerdo
   - ☐ De acuerdo
   - ☐ Ni de acuerdo ni en desacuerdo
   - ☐ En desacuerdo
   - ☐ Totalmente en desacuerdo

3. ¿La Dirección debe de establecer, documentar y revisar las políticas de control de acceso?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
4. ¿Se debe asegurar la protección y privacidad del personal según las normas internas de la institución?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
5. ¿El Jefe de Área, debe asegurar que los procedimientos de seguridad deban cumplir con las políticas y estándares de seguridad?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo

- **Mapeo de Procesos**

1. ¿La Dirección debe apoyar la seguridad dentro de la organización?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
2. ¿La Dirección debe implementar un proceso de autorización para los nuevos medios de procesamiento de información?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
3. ¿La información debe ser clasificada en términos de su valor, requerimientos legales y confidencialidad?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo

4. ¿Los empleados deben tener roles y responsabilidades de seguridad de la información?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
5. ¿Los empleados deben aplicar la seguridad en concordancia con las políticas establecidas por la organización?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
6. ¿Debe existir procedimientos de operación documentado?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
7. ¿Debe existir procedimientos y controles de intercambio de información?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
8. ¿Debe existir procedimientos a nivel de Dirección para una respuesta rápida a los incidentes de seguridad?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo

- **Activos de la Información**

1. ¿Debe existir controles de entrada para permitir solo el acceso al personal autorizado?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
2. ¿Debe existir protección contra amenazas externas y ambientales?
    - Totalmente de acuerdo
    - De acuerdo

- Ni de acuerdo ni en desacuerdo
- En desacuerdo
- Totalmente en desacuerdo

3. ¿Los equipos deben tener un mantenimiento preventivo para su correcto funcionamiento?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
4. ¿Los equipos, información, software no deben salir de la institución sin la autorización respectiva?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
5. ¿La información que contiene los diversos sistemas deben ser protegidos de accesos no autorizados?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
6. ¿Los medios de procesamiento debe ser monitoreado mediante procedimientos establecidos?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo

PREGUNTAS RESPECTO A LOS INDICADORES DE LA VARIABLE DEPENDIENTE:

Gestión de Servicios

1. ¿Está de acuerdo que el Director apoye la seguridad de la información dentro del área?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
2. ¿Al seleccionar al personal se realizaran verificación de antecedentes?
    - Totalmente de acuerdo
    - De acuerdo

- Ni de acuerdo ni en desacuerdo
- En desacuerdo
- Totalmente en desacuerdo

3. ¿Para el manejo y almacenamiento de la información se debe establecer procedimientos?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
4. ¿Los usuarios solo deben tener acceso a los servicios para lo cual ha sido autorizado, según su perfil?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
5. ¿Se debe restringir la conexión de los usuarios en las redes compartidas?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
6. ¿Los usuarios deben de informar de manera oportuna las vulnerabilidades encontradas?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
7. ¿Se debe tener en cuenta los incidentes ocurridos, así poder implementar mecanismos de monitoreo?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
8. ¿Está de acuerdo en proteger los registros organizacionales de pérdida, destrucción y falsificación?
   - Totalmente de acuerdo
   - De acuerdo
   - Ni de acuerdo ni en desacuerdo
   - En desacuerdo
   - Totalmente en desacuerdo

- **Análisis de la Valoración del Riesgo en la Gestión de servicios.**

1. ¿Los empleados deben ser capacitados en seguridad de la información para su función laboral?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
2. ¿Debe existir un proceso disciplinario para los empleados que han cometido una violación en la seguridad?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
3. ¿Todos los empleados deben devolver todos los activos que estén en su posesión al término de su empleo o contrato?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo
4. ¿Los derechos de acceso a la información de los empleados debe ser eliminado al término de su empleo o contrato?
    - Totalmente de acuerdo
    - De acuerdo
    - Ni de acuerdo ni en desacuerdo
    - En desacuerdo
    - Totalmente en desacuerdo

ANEXO 3

INDICADOR PRODUCTIVIDAD

Muestra de "Tiempo empleado en hacer las funciones adecuadas"

TAREAS	TIEMPO DE ATENCION (MINUTOS)	X^2
1	60	3600
2	90	8100
3	75	5625
4	90	8100
5	90	8100
6	90	8100
7	90	8100
8	90	8100
9	90	8100
10	90	8100
11	90	8100
12	90	8100
13	120	14400
14	90	8100
15	90	8100
16	75	5625
17	90	8100
18	90	8100
19	105	11025
20	90	8100
21	90	8100
22	90	8100
23	90	8100
24	105	11025
25	90	8100
26	90	8100
27	90	8100
28	90	8100
29	120	14400
30	120	14400
	2760	**258300**

Fuente: Elaboración Propia, 2016

ANEXO 4

INDICADOR EFICACIA

Muestra de "Tiempo de respuesta promedio ante un requerimiento"

Obs.	Tiempo elaboración Documentos	X^2
1	20	400
2	25	625
3	25	625
4	25	625
5	20	400
6	25	625
7	25	625
8	25	625
9	25	625
10	25	625
11	25	625
12	25	625
13	25	625
14	20	400
15	20	400
16	25	625
17	25	625
18	25	625
19	20	400
20	20	400
21	20	400
22	25	625
23	25	625
24	20	400
25	25	625
26	20	400
27	20	400
28	25	625
29	25	625
30	20	400
	695	**16275**

Fuente: Elaboración Propia, 2016

ANEXO 5

INDICADOR PRODUCTIVIDAD

Muestra de "Tiempo empleado para elaboración de documentos"

Tareas	Tiempo elaboración Documentos	X^2
1	4	16
2	4	16
3	4	16
4	5	25
5	5	25
6	5	25
7	5	25
8	4	16
9	4	16
10	5	25
11	4	16
12	4	16
13	5	25
14	5	25
15	5	25
16	5	25
17	5	25
18	4	16
19	4	16
20	4	16
21	5	25
22	4	16
23	5	25
24	4	16
25	4	16
26	4	16
27	3	9
28	4	16
29	4	16
30	4	16
	131	**581**

Fuente: Elaboración Propia, 2016

ANEXO 6

INDICADOR EFICIENCIA

Muestra de "Promedio mensual de documentos recibidos"

Dia	Documentos a presentar	Documentos atendidos	Documentos no atendidos	X^2
1	10	5	5	25
2	10	6	4	16
3	20	16	4	16
4	20	16	4	16
5	20	16	4	16
6	20	15	5	25
7	20	15	5	25
8	20	15	5	25
9	20	15	5	25
10	30	24	6	36
11	20	15	5	25
12	35	30	5	25
13	35	30	5	25
14	20	15	5	25
15	20	15	5	25
16	20	16	4	16
17	20	16	4	16
18	30	25	5	25
19	25	20	5	25
20	25	20	5	25
21	25	20	5	25
22	35	30	5	25
23	20	14	6	36
24	30	25	5	25
25	30	25	5	25
26	20	15	5	25
27	20	14	6	36
28	35	30	5	25
29	35	30	5	25
30	30	25	5	25
			147	**729**

Fuente: Elaboración Propia, 2016

ANEXO 7: **VALIDACIÓN DE LAS ENCUESTAS**

I. DATOS GENERALES

1.1 NOMBRES Y APELLIDOS DEL EXPERTO
Mg. José Collao Arce
1.2 CARGO E INSTITUCIÓN QUE LABORA
Gestor de evaluación - UPIG
1.3 INSTRUMENTO MOTIVO DE LA INVESTIGACIÓN
Cuestionario de Preguntas
1.4 AUTOR DEL INSTRUMENTO:
Carlos Muchotrigo Talla
1.5 TESIS:
La norma ISO 27001 como soporte al proceso de la seguridad de la información y su influencia en la gestión de servicios educativos de la Fuerza Aérea del Perú.

II. ASPECTOS DE VALIDACIÓN:

INDICADORES	CRITERIOS	DEFICIENTE 0-20 %	BAJA 21-40%	REGULAR 41-60%	BUENA 61-80%	EXCELENTE 81-100%
Intencionalidad	**El instrumento responde a los objetivos de la investigación planteada.**					
Objetividad	**El instrumento esta expresado en comportamientos observables.**					
Organización	**El orden de los Ítems y áreas es adecuado.**					
Claridad	**El vocabulario empleado es adecuado**					
Suficiencia	**El número de Ítems propuesto es suficiente para medir las variables**					
Consistencia	**Tiene una base teórica y científica que la respalda**					
Coherencia	**Entre el objetivo, problema, hipótesis existe coherencia**					
Aplicabilidad	**Los procedimientos para su aplicación y corrección son sencillos.**					

III. Opinión de Aplicabilidad:

IV. PROMEDIO DE VALORACIÓN AL 100%

Cañete, 02 de Marzo 2016
