UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERIA

ESCUELA DE INGENIERIA INFORMATICA Y DE SISTEMAS

Evaluación de la seguridad de información en el Instituto Nacional de Estadística e Informática, Huacho, 2019

Tesis para obtener el título de Ingeniera en Informática y de Sistemas

Autor

Laurente Carreño, Tania Estela

Asesor

Martínez Carrión, Javier

HUACHO – PERÚ

2019

INDICE

PALABRAS CLAVE i

TITULO ii

RESUMEN iii

ABSTRACT iv

INTRODUCCIÓN 1

RESULTADOS 13

ANALISIS Y DISCUSION 31

CONCLUSION Y RECOMENDACIÓN 32

AGRADECIMIENTO 34

REFERENCIA BIBLIOGRAFÍCAS 35

ANEXOS 37

PALABRAS CLAVE

Tema	Seguridad de la Información
Especialidad	Gestión

KEYWORDS

Topic	security of the information
Specialty	Management

LINEA DE INVESTIGACION

Línea	Sistema de Gestión
Área	Ciencias sociales
Sub Área	Economía y Negocio
Disciplina	Negocios y Management

TITULO

Evaluación de la seguridad de información en el Instituto Nacional de Estadística e Informática, Huacho, 2019

Information security assessment in the National Institute of Statistics and Informatics, Huacho, 2019

RESUMEN

En esta tesis, el objetivo fue el desarrollo de una evaluación de seguridad de la información en el Instituto Nacional de Estadística e Informática en Huacho, basada en los procedimientos de la Metodología MAIGTI, donde dentro de la metodología evaluaremos algunos de sus procedimientos. Definir y validar los procesos necesarios para La gestión de la seguridad de la información.

La tesis es un tipo de investigación descriptiva, en la que se aplicó la metodología MAIGIT y sus procedimientos, que ha permitido realizar la evaluación de toda la organización desde el punto de vista del sistema de información.

El resultado logrado fue la evaluación de la información, mediante la aplicación de las mejores prácticas de seguridad de la información empleando la metodología MAIGTI, se elaboró la documentación que permitirá una gestión segura de la información.

.

.

ABSTRACT

In this thesis, the objective was the development of an information security assessment at the National Institute of Statistics and Informatics in Huacho, based on the procedures of the MAIGTI Methodology, where within the methodology we will evaluate some of its procedures. Define and validate the processes necessary for the management of information security.

The thesis is a type of descriptive research, in which the MAIGIT methodology and its procedures were applied, which has allowed the evaluation of the entire organization from the point of view of the information system.

The result was the evaluation of the information, through the application of the best information security practices using the MAIGTI methodology, the documentation that will allow a secure information management was developed.

INTRODUCCIÓN

El presente tesis consideró a los siguientes Antecedentes.:

En Perú, Hans Ryan Espinoza Aguinaga (2013), en su tesis Titulada "Análisis y diseño de un sistema de gestión de seguridad de información basada en la norma ISO/IEC 27001:2005 para una empresa de producto de consumo masivo", Realizada en la Universidad Católica de Perú , Escuela de Ciencias e Ingeniería para obtener el título Ingeniero informático, Realizo el estudio con el objetivo de analizar y diseñar un sistema de gestión de seguridad de información ,basado en la norma ISO /IEC 27001:2015 para una empresa dedicada a la producción y comercialización de consumo masivo , lo cual permitió que esta cumpliera con las normas de regulación vigentes en lo que respecta a seguridad de información .para efecto del análisis de riesgo del proyecto de tesis, se decidió trabajar con el proceso de producción ya que se considero que era el proceso más importante dentro del funcionamiento de la empresa. Este proceso de producción a su vez se divido en 4 subprocesos que lo conforman. Los cuales fueron el proceso de planificación, manufactura, calidad y bodega e inventarios aplicando la metodología MAGERIT, obteniendo como resultado Documentación obligatoria exigida por la norma ISO 27001 para implantar un SGSI, Documento con la declaración de aplicabilidad de la norma ISO 27001 para el SGSI que se diseño. De lo cual nos ayudo a implantar medidas de seguridad a la información del Instituto Nacional de Estadística e Informática.

En Ecuador, Jorge Luis Valdivieso Troya y Roberto Josué Rodríguez Poveda (2015) en su Tesis titulada "Informe de evaluación de seguridad en la información Basada en la norma ISO 27001 en el departamento de TI de una Empresa de Lácteos", Realizada en la Universidad Politécnica Salesiana de Ecuador , Escuela de Ingeniería de Sistemas, para obtener el título de Ingeniero de Sistemas, Realizó un estudio con el objetivo de la elaboración de un informe de evaluación que permite detectar los errores o falencias que existen en la empresa con respecto a la seguridad de la información., para el caso de estudio propuesto, se usa la metodología de investigación de riesgo MAGERIT, la cual brindo las herramientas necesarias que ayudo a realizar una matriz de evaluación en la cual se identifico los activos,

amenazas, vulnerabilidades, y a través de niveles de valoración para cada elementos. Y como resultado de esta investigación fue hacer un informe basado en un análisis de riesgo que permitió detectar las amenazas y vulnerabilidades de los activos más críticos del departamento TI. En el mismo se propuso controles adecuados tomando como referencias la norma ISO 27001. Lo cual esta investigación nos ayudo a identificar las posibles amenazas que existen en una información de las organizaciones.

En Trujillo, Yan Carranza Freddy y Zavala Vásquez Cinthia Liliana (2013), en su tesis titula "Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT ", realizó en la Universidad Privada Antenor Orrego, en la escuela de Ingeniería de computación y sistema, para obtener el Título profesional de Ingeniero de computación y sistema, realizó el estudio con el objetivo que elaboraron un plan de mejora de seguridad de la información y continuidad del Centro de datos, utilizando la metodología MAIGTI. Y como resultaron mostraron el informe de la auditoria de sistema del centro de datos de la GRELL, Identificaron los riesgos de TI asociados al centro de datos, los controles de TI que base en COBIT y elaboraron el plan de mejora basándose en la NTP ISO/IEC 27001 y las buenas prácticas de COBIT. Esta tesis nos sirvió para identificar la metodología que utilizamos en nuestra tesis ya que la metodología MAIGTI nos ayuda a identificar las posibles amenazas.

En Piura Carmen Cynthia Elizabeth Ramos Arca (2015), en su Tesis titula "Propuesta de auditoría Informática para el Sistema de Información en Salud y el aplicativo para el registro de formatos SIS en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015", se realizo en la universidad Nacional de Perú ,en la escuela profesional de ingeniería informática, realizó el estudio con el objetivo de un plan de auditoría informática para los dos sistemas más importantes de cada establecimiento de salud, los cuales son el sistema de información en salud y el aplicativo para el Registro de formatos SIS, la propuesta del plan de auditoría se ha realizado en base a la guía de control interno de las

entidades del Estado Peruano para realizar un análisis de riesgo de ambos sistemas de información basadas en encuestas aplicadas a 10 establecimientos de salud, además se aplico la Norma Técnica Peruana ISO 27001:2008, como resultado se aplico y se estableció los objetivos y procedimientos de control adaptados a los establecimientos de salud para posteriormente plasmarlo en el programa detallado de auditoría informática y aplicarlo en un futuro mediante el papel de trabajo por cada procedimiento de control. Esta tesis nos ayudo a realizar a nuestra tesis analizar los riesgos que presentan en las distintas organizaciones.

Sangolqui, Sofía Montserrat Viteri Diaz, (2013), en su tesis titulada "Evaluación técnica de la seguridad informática del data center de la brigada de fuerzas especiales N°9 Patria", se realizo en la escuela Politécnica del ejercito, en el Dpto de ciencias de la computación, con el objetivo que realizó una evaluación técnica informática de las seguridades del datacenter de la brigada Patria en Latacunga, considerando como referencia ISO 27001 e ISO 27002, utilizo la metodología MAGERIT y la normas de ISO 27001, como resultado descubrieron las debilidades en el sistema informáticos ,y mediante las recomendaciones basadas en los estándares ISO 27001 e ISO 27002, se realizo el diagnostico de la seguridad informática Datacenter, este proyecto diseño un plan de seguridad informática , el mismo que servirá para que los usuarios Datacenter de la brigada "Patria", se encuentre en capacidad de aplicar medidas de seguridad para mantener la información disponible, confiable y oportuna. Esta tesis nos orientó y nos ayudó saber sobre el ISO 27001 y su gestión de seguridad de la información para aplicar medidas de seguridad.

En Ecuador, María Victoria Rivera Chávez y María Fernanda Zambrano Bravo (2015), en su tesis Titulada "Auditoria al control y mantenimiento de la infraestructura tecnológica del departamento tecnológico de la ESPAM MFL", se realizo en la Escuela Superior Politécnica Agropecuaria de Manuel Félix López en la carrera informática para obtener el título de Ingeniería Informática, realizó un estudio con el objetivo de aplicar una auditoria al control y mantenimiento de la infraestructura Tecnológica del Departamento Tecnológico de la ESPAM MFL, que evaluaron el nivel de cumplimiento de aplicaciones de buenas prácticas, estándares y

normas de control interno informático y tecnológico de la contraloría General del Estado Ecuatoriano, se empleó la metodología determinada en las Normas internacionales de auditoría, como resultado de este proyecto fue que emitieron el informe de auditoría de la infraestructura tecnológica tomando en cuenta todos los hallazgos recopilados. La tesis nos sirvió para poder orientarnos sobre las inseguridades de la infraestructura del área o lugar donde se encuentre la organización.

La investigación se justifica en la social por que el personales que laboran en el Instituto Nacional de Estadística e Informática podrán aprovechar en mejorar sus conocimiento sobre como prevenir, contrarrestar, mitigar las amenazas que pueden presentar la seguridad de la informaciones de la Institución por medios de las capacitaciones de seguridad de información, como también las constancia de certificados ayudara actualizar su currículum vitae de los personales que laboran en el Instituto Nacional de Estadística e Informática.

Así mismo se justifica científicamente porque se pretende contribuir a mejorar la seguridad de la información en el Instituto Nacional de Estadística e Informática, una seguridad plena que sea confiable, segura. De tal manera se pretende dar seguridad a la información y saber contrarrestar las amenas que puedan presentarse.

En el Instituto Nacional de Estadística e Informática, la información es considerada muy importante, por esa razón es necesario asegurar la confidencialidad, integridad de la misma. Estas características son factores importantes para tener la categoría o niveles de jurisdicción y lograr los objetivos de la organización. Asimismo, la investigación de la evaluación de seguridad de información en el Instituto nacional de estadística e informática busca obtener como resultado establecer los lineamientos de cambios para la mitigación de las amenazas.

Finalmente, la investigación se alega de manera práctica, porque busca dar una seguridad a la información desarrollando una Evaluación de seguridad de la Información y contribuir a la mejora y definir procedimientos alineados a una metodología MAIGTI.

Luego de realizar un análisis en el Instituto Nacional de Estadística e Informática siendo una organismo donde recopila demasiadas informaciones de diferentes estándares lo cual necesita confidencialidad e integridad se pudo determinar que no cuenta de manera formal solo con políticas pero no con procedimientos que puedan ayudar a evitar las pérdidas de información, eso hace que no se garantice la disponibilidad, integridad y confidencialidad de la información ya que no están estipulado bajo estándares definido y en consecuencia no existe una identificación de las amenazas y riesgos existente.

Es por ellos que se sugiere que sea necesario que se desarrolle procedimientos basados a la Metodología MAIGTI ya que el Instituto Nacional de Estadística e Informática tiene el acceso no controlado de la información que maneja, se requiere evaluar el funcionamiento de seguridad de la información en base de los estándares y es por ello que se propone una evaluación interna empleando la metodología MAIGTI, para analizar los procesos relativos de la seguridad de la información y poder establecer los lineamientos para la mitigación de las amenazas .

Después de realizar un análisis sobre los problemas del Instituto Nacional de Estadística e Informática. Lo consideramos el más importante para la realización del proyecto lo cual cuenta con el siguiente problema:

La seguridad de la información porque el Instituto Nacional de Estadista e Informática no cuentan con prevención para poder mitigar los riesgos o amenazas que pueden presentar a las diferentes informaciones obtenidas estadísticamente por la organización ya que las informaciones tiene que ser confiable y no revelarse hasta que llegue a su destino tampoco debe ser manipulados por personas no autorizadas para el manejo. Para el siguiente trabajo de investigación formulamos el siguiente problema

¿De qué manera evaluaremos la seguridad de la información al instituto nacional de estadística e informática?

El trabajo de investigación se considero la siguiente definición operacional teóricos.

COBIT (ISACA, 1996)

Las mejores prácticas descritas en ITIL son tan relevantes que se han convertido en un estándar de facto en el mercado de TI. Sus conceptos se aplican en los niveles operacional y táctico y permiten que la estructura departamento de TI el ciclo de vida de sus servicios en su conjunto, con el fin de alcanzar la excelencia operativa.

Sin embargo, la Metodología COBIT se centra en el nivel estratégico, y es un marco de control, permite Tiene su rendimiento medido y sus riesgos debidamente designados y tratados.
Al estudiar el marco de COBIT con mayor profundidad es posible para identificar que especifica los objetivos de control, pero no detalla cómo se pueden definir los procesos.

COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir administradores IT, usuarios y por supuesto los auditores involucrados en el proceso.

Las siglas de COBIT significan objetivos de control para tecnología de información y tecnologías relacionadas El modelo es el resultado de una investigación con expertos de varios países, desarrollado por **ISACA (**Information Systems Audit and Control Association ISACA 1996).

ISO 27001 (Alberto G, 2007)

El nuevo estándar internacional, el ISO 27001:2005, esta orientado a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externa o interna.

Maigti: Metodología para la auditoria integral de la gestión de la tecnología de la información (Antonio, 2011)

MAIGTI lanza los diversos conceptos de COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), Y PMBOK, sobre la base de una simplificación del proceso

general de auditoría descrito en la norma ISO 19011:2002, y sobre la base de una adaptación del esquema de proceso de la ISO 9001:2000 (ISO 2000). MAIGTI comprende los siguientes elementos: Objetivo (la finalidad de la auditoría), Alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría), Entradas (requerimientos de información), Proceso de MAIGTI (evaluaciones a realizar), Salidas (papeles de trabajo e informe de auditoría).

Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los subprocesos de MAIGTI, comprende la siguiente estructura: Objetivo (la finalidad del procedimiento de auditoría), Alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría a realizarse a través del procedimiento), Entradas (requerimientos de información para ejecutar el procedimiento de auditoría), Proceso (detalle de los pasos a seguir en el procedimiento de auditoría), Salidas (hallazgos evidenciados como resultado de la ejecución del proceso). (Antonio, 2011)

Evaluación (Cappilletti, 2004)

La evaluación pone al descubierto información referidos a la forma de operar el sistema para desarrollar estrategias y tomar decisiones destinadas a lograr un grado de perfección mayor de dicho sistema. Los datos recogidos pueden reunirse en cuatro grandes grupos: los que se valoran positivamente, fortalezas, los que se consideran deficientes, debilidades y los referidos al entorno, es decir, aquellos que influyen sobre el sistema y este no puede cambiar a prioridad. De ellos, a su vez, los que favorecen el funcionamiento del sistema, oportunidades y los que no, amenazas.

Un proceso evaluativo debe contar con un programa de ejecución que organice adecuadamente las diferentes tareas relacionadas con las etapas principales: la descripción del estado actual, con el fin de buscar y compilar los datos aplicando los métodos y las técnicas adecuadas, el análisis crítico de ese estado, de forma tal, que se emita un diagnóstico de las condiciones en que se encuentra lo que se pretende evaluar con el fin de determinar si ha ocurrido algún cambio de acuerdo con lo que estaba establecido y en que dirección y finalmente la etapa de proposiciones en la

cual se recomiendan los cambios según las estrategias que se trazan sobre la base de las decisiones que se toman en la etapa anterior.

Es importante definir el alcance que ha de tener la evaluación a realizar en un sistema de información y esto se refiere si solamente va a atender aspectos técnicos (eficacia) o si se ocupará también de los económicos (eficiencia). Aquí entran a jugar los costos que vienen dados por los gastos al adquirir determinados recursos necesarios y que hay que pagar. También están los aspectos referidos a los beneficios obtenidos por los usuarios del sistema con el uso de dicha información y finalmente el impacto, que viene dado por los resultados que se obtienen en la práctica y las transformaciones que puedan producirse como efecto de ese uso. Esto constituye los niveles de la evaluación: Eficacia, Costo eficacia, Costo-beneficio, Impacto.

Define evaluación Como el –"Cálculo para calificar y medir el logro y la forma de satisfacer los objetivos propuestos de un determinado sistema o unidad." La autora considera que un requerimiento de cualquier actividad es la comprobación de sus resultados y el impacto de estos, lo cual no es posible con éxito si no se evalúan misión, objetivos, estrategias y la implantación de las mismas, teniendo siempre en cuenta las condiciones del entorno. (Cappilletti, 2004)

Teoría de la Información (Shannon, 1948)

La investigación sobre el concepto de información se remite a la Edad Media, donde se decía que la información y, más específicamente la palabra, daba forma e impregnaba de carácter a la materia y a la mente. De alguna manera, se manejó siempre, la idea de que la información es un "agente activo", un principio universal.
Que específica el significado de las cosas e indica, mediante códigos, los modelos del pensamiento humano. Este hecho condujo a pensar que la información estaba relacionada únicamente con los seres humanos. Aunque es así en cierta forma, algunos especialistas consideran que todos los seres vivos emplean información del medio para su supervivencia. La superioridad de los seres humanos radica, sin embargo, en su capacidad de generar y perfeccionar, tanto códigos como símbolos con significados que conformaron lenguajes comunes útiles para la convivencia en

sociedad, a partir del establecimiento de sistemas de señales y lenguajes para la comunicación. (Claude E. Shanon 1948).

Este trabajo de Investigación por ser una investigación descriptiva la hipótesis está implícito.

Se plante como objetivo general: Elaborar la evaluación de la seguridad de información al Instituto Nacional de Estadística e Informática. Se tomaron como objetivo específicos:

Determinar los procesos relativos de la seguridad de información.

Aplicar la metodología MAIGTI para la seguridad de información.

Establecer los lineamientos de cambio para la mitigación de las amenazas de la seguridad de información.

METODOLOGIA

El Informe de investigación fue de tipo APLICADA; Se caracteriza porque busca la aplicación o utilización de los conocimientos que se adquieren.

El siguiente proyecto de investigación fue de carácter DESCRIPTIVO; porque la recopilación de datos obtenidos por instrumentos de investigación nos permitió observar, conocer y describir la situación en la que se encuentra el Instituto Nacional de Estadística e Informática.

El diseño de la investigación fue no experimental de corte transversal por que los datos serán tomados en una sola vez utilizando los instrumentos de recolección de datos. La población que se involucra para esta investigación son los miembros del Instituto Nacional de Estadística e Informática que fueron el personal principal para el estudio de nivel de cumplimientos de los lineamientos y estándares internacionales de la seguridad informática. P=30.

Por ser una población pequeña se tomará la cantidad del personal que trabaja en la Instituto Nacional de Estadística e Informática M=10

Las técnicas e instrumentos de validación empleados para el informe de investigación son:

Tabla 01
Técnicas de instrumentos

Técnicas	**Instrumentos**
Análisis Documental	Texto, tesis, revistas y estudios previos
Encuesta	Cuestionarios de preguntas

Se estructuraron preguntas abiertas y cerradas que brindaron información muy certera, para obtener mayor información y reforzar el tema de la documentación, se utilizó el internet para obtener los instrumentos.

El siguiente trabajo de investigación su procesamiento y análisis de la información su técnica de análisis de los datos se realizara a través del procedimiento de estadísticas descriptivas , para realizar el procesamiento de la recolección de datos se procederá a

tabular en una matriz datos, de ser necesario codificando MS Excel, encontrando promedios, Varianza, correlación y pruebas de hipótesis.

Para la investigación utilizamos La metodología MAIGTI y con sus respectivos elementos:

- Objetivo (la finalidad de la auditoría).
- Alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría).
- Entradas (requerimientos de información).
- Proceso de MAIGTI (evaluaciones a realizar).
- Salidas (papeles de trabajo e informe de auditoría).

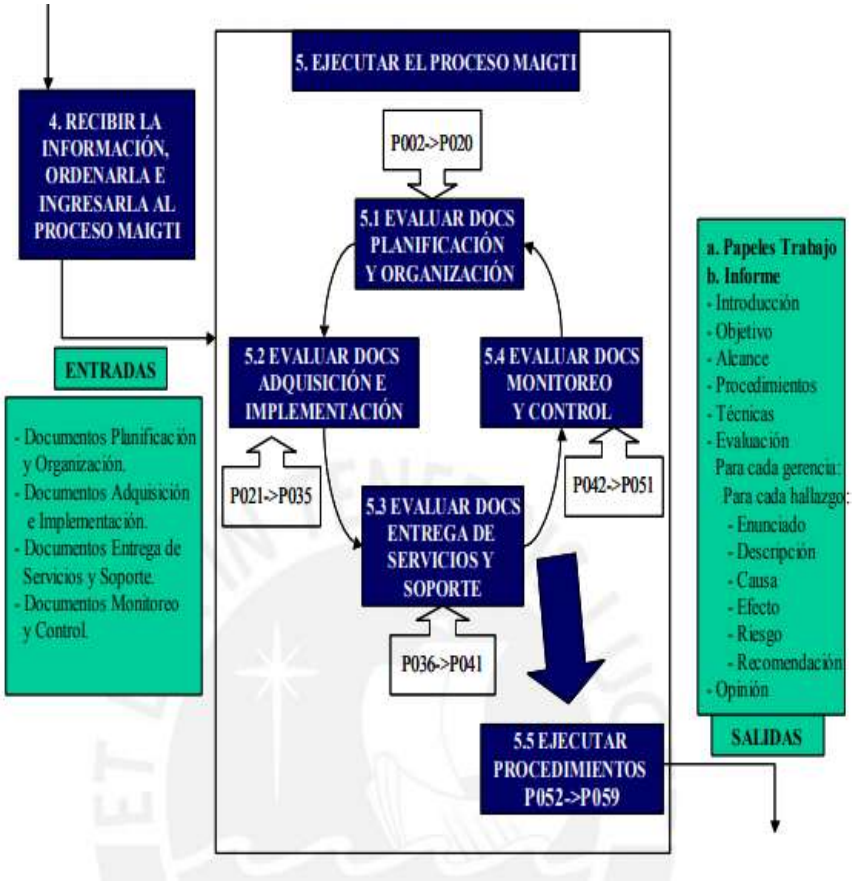


Figura 1 El proceso de MAIGI
Fuente: Antonio, 2011

Así mismo utilizamos los siguientes procedimientos para nuestra investigación:

P004 Procedimiento para la auditoria de la evaluación de riesgo**.**

P008 Procedimiento para la auditoría del plan de contingencias de informática.

P010 Procedimiento para la auditoría del plan de seguridad de la información.

P**011** Procedimiento para la auditoria del plan de licenciamiento de software.

P012 Procedimiento para la auditoria del plan de capacitación

P013 procedimiento para la auditoria del plan de mantenimiento preventivos de hardware de computadoras, redes y equipos relacionados.

P014 Procedimiento para la auditoria del plan de mantenimiento correctivo de Hardware de computadoras, Redes y equipos relacionados.

P016 Procedimiento para la auditoría del plan de calidad.

P020 Procedimiento para la evaluación del Currículum Vitae del personal de tecnología de Información.

P037 Procedimiento para la auditoría de la seguridad de acceso a los sistemas de Información.

P038 Procedimiento para la auditoria de la seguridad de acceso a las carpetas en los servidores.

P054 Procedimiento para la auditoría de la seguridad de acceso al centro de cómputo principal.

RESULTADOS

Según el primer objetivo especifico es la determinación de los procesos relativo de la seguridad de la información en el Instituto Nacional de Estadística e Informática.

Instalación y configuración de software

Solamente se podrá utilizar software aprobado por el departamento de informática
El personal de informática es el único autorizado para instalar, modificar o eliminar aplicaciones o software en general por ellos las personas deben de estar previamente capacitados.

Instalación y configuración del hardware

Las estaciones de trabajo solamente podrán utilizar hardware aprobado por el departamento de sistema, según lo amerite el perfil del usuario.

El personal de sistemas es el único autorizado para instalar, modificar o eliminar componentes de hardware según sea el requerimiento. Por ellos los equipos informáticos deberán pasar por mantenimiento mensualmente

Mantenimiento preventivo a los equipos Informáticos del área de informática

Los personales de área de informática realizan los mantenimientos preventivos a los equipos informáticos para la detección de los puntos débiles del sistema dicho mantenimiento lo hacen anualmente.

El personal encargado ingresa al sistema con sus respectivos usuarios y contraseñas

Es el personal encargado de crear cuenta de usuario aprobado en la sede de lima del Instituto Nacional de Estadística e Informática es el que puede eliminar bloquear el usuario y la contraseña para mayor seguridad.

El uso de la cuenta de usuario es responsabilidad exclusiva de la persona asignada.

La cuenta de usuario será protegida mediante una contraseña, la contraseña e personal e intransferible, no debe compartir la cuenta de usuario con otra persona.

Ingreso autorizados a personal que laboran en área de informática

Las personas que solo laboran en la organización podrán pasar a las instalaciones del Instituto Nacional de Estadística e Informática.

Capacitación al personal que laboran en el Instituto Nacional de Estadística e Informática

El Instituto Nacional de Estadística e Informática realizan capacitaciones para su personal que laboran en la organización.

Evaluación de los expediente de los personal que laboran en el Instituto Nacional de Estadística e Informática

El personal encargado de recibir los currículum vitae de los personal es el área de recursos humanos ellos evalúan los expediente y envían al área de informática los personales que ganaron el puesto.

Actualización de antivirus

El Instituto Nacional de Estadística e Informática cuentan con antivirus lo cual los encargados de instalar y actualizar antivirus son los personales del área de informática.

Según el segundo objetivo específico1; es Aplicar la metodología MAIGTI a la seguridad de la información y por ellos solo utilizamos algunos procedimientos ya mencionados.

P004 Procedimiento para la auditoria de la evaluación de riesgo.

Objetivo

Evaluar y analizar el proceso de evaluación de amenazas que pueden presentar el Instituto Nacional de Estadística e Informática

Alcance

- Verificación al desarrollo de conformación de los equipos para la evaluación de amenazas o riesgos.
- Verificación de los resultados de la evaluación de riesgo.
- Verificación de los contratos de los antivirus que tiene las computadoras del INEI.
- Verificación de los antivirus que contiene las equipos informáticos

Entradas

- Plan estratégico del Instituto Nacional de Estadística e Informática
- El plan estratégico de cada una de las áreas del Instituto Nacional de Estadística e informática.
- Respuesta de gerencia antes la evaluación de riesgo.

Proceso

- Los equipos Informáticos del Instituto Nacional de estadística e informática cuentan con antivirus pero no se actualizan automáticamente los personal encargado de los equipos lo actualizan cuando crean conveniente.

Salidas

- Al desarrollar la evaluación encontramos que el Instituto Nacional no cuentan con Antivirus que no se actualizan automáticamente.

- El Instituto Nacional de Estadística e Informática los personales no realiza evaluación de riesgo.

P008 Procedimiento para la auditoría del plan de contingencias de informática

Objetivo

Analizar el proceso de elaboración y ejecución del plan de contingencia de la información, con el fin de identificar las pérdidas debido a los errores de diversos procesos.

Alcance

- Revisión el plan de contingencia si esta elaborado.
- Revisión del presupuesto asignado para la ejecución del plan de contingencia.
- Revisión del proceso de conformación del equipo de elaboración del plan de contingencia.

Entradas

- Para realizar la evaluación se requiere consultar por medio de una encuesta al personal si cuentan con un plan de contingencia el Instituto Nacional de Estadística e Informática.

Proceso

- Por medio de una pregunta de la encuesta dirigida al personal de la Institución deducimos que el Instituto Nacional de Estadística e Informática no cuenta con un plan de contingencia.

Salida

- Al desarrollar la evaluación del instituto Nacional de Estadística e Informática no cuenta con un plan de contingencia lo cual sugerimos a la Institución que cuente con dicho plan por el bien de su rentabilidad de la Institución ya que hoy en día hay muchos ataque de amenazas para la seguridad de la información

P010 Procedimiento para la auditoría del plan de seguridad de la información.

Objetivo

Analizar y evaluar el proceso elaboración y ejecución del plan de seguridad de la información del Instituto Nacional de Estadística e Informático, con el fin de identificar pérdida de información o fallas de diversos procesos que involucra.

Alcance

- Revisión del documento del plan de seguridad de la información.
- Revisión de la implementación de las acciones indicadas sobre el ingreso de la información al sistema.
- Evaluación de los ataques de intrusos y diversos problemas de seguridad de la información que hubiera sucedido durante el periodo en evaluación.

Entradas

- Realizamos una encuesta para determinar si existe un plan de seguridad en el Instituto Nacional de Estadística e Informática

Proceso

- Verificar si la seguridad de la información por la Institución sea su prioridad para todos los personales que laboran, para evitar que la información sufra perdidas ya que hoy en día hay demasiado riesgo para la seguridad de la información porque si no cuidamos la seguridad en el Instituto Nacional de Estadística e Informática pueda perder su prestigio como organismo que da información veraz al Gobierno

Salida

Según la documentación presentada por el responsable del área, se indica:

- El Instituto Nacional de Estadística e Informática cuenta con un plan de seguridad de la información del año 1997 lo cual no esta actualizada con los riesgos que pueden presentarse.
- El personal cuentan con sus respectivos usuarios y contraseñas lo cual las contraseñas no son de alta seguridad porque no esta en nivel de confiabilidad es decir ni es secreta porque lo saben otros personales que laboran en dicha Institución.

P011 Procedimiento para la auditoria del plan de licenciamiento de software

Objetivo

Analizar y evaluar el proceso de elaboración y ejecución de licenciamiento de software de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

Alcance

- Revisión del plan de licenciamiento del software.
- Verificación de la asignación de presupuesto cronograma y responsabilidad para la ejecución del plan de licenciamiento de software.

Entrada

- Realizamos una encuesta a las personas que elaboran en el Instituto Nacional de Estadística e Informática para obtener respuesta si existen un plan de licenciamiento de software.

Proceso

- Verificamos por medio de la encuestas realizamos la muestra donde nos indican que el personal de la Institución no saben el correcto manejo del software ya que no se cuentan con el manejo del manual del software.

Salida

- El Instituto Nacional de Estadística e Informático los personales no están capacitados para el uso del software por lo tanto recomendamos capacitación sobre el software.

P012 Procedimiento para la auditoria del plan de capacitación

Objetivo

Analizar y evaluar el proceso de elaboración y ejecución del plan de capacitación para el área informática de la organización con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

Alcance

- Supervisar los procesos de elaboración del Plan de capacitación del área de informática.
- Revisión del currículum vitae del personal del área de informática actualizado.
- Verificación del plan de capacitación al plan estratégico de la información.
- Verificación del análisis de generación de valor del plan de capacitación del área de la informática.

Entradas

- Realizamos la evaluación y los personales de Instituto Nacional de Estadística e Informático si están actualizados como manejar el software y sobre los riesgos que pueden encontrar en el momento de ingresar la información, realice una encuesta sobre las personas y la muestra nos dio como resultado el que es más porcentaje que no sabe manejar el software. Por lo cual sugerimos al Instituto Nacional de Estadística e Informática que los personales realicen capacitaciones sobre el funcionamiento de sus labores que ocupan en la organización.

Procesos

- Preguntamos a los trabajadores por medio de una encuesta si realizaron capacitación de los cuales la organización realizan capacitación anualmente lo cual no es necesario para un personal que laboran en la Institución porque ellos están más propenso a recibir amenazas de la seguridad de información.

Salida

Al desarrollar la evaluación es común encontrar la siguiente observación.

- El Instituto Nacional de Estadística e Informática no cuentan con un plan de capacitación la organización solo realizan capacitación anual por sugerencia de la sede de Lima pero la ODEI de Huacho no cuentan con un plan de capacitación; lo cual sugerimos que la ODEI de Huacho cuente con un plan de capacitación para que los personales puedan mitigar las amenazas que se presenta.

P013 Procedimiento para la auditoria del plan de mantenimiento preventivos de hardware de computadoras, redes y equipos relacionados

Objetivo

Evaluar el proceso de elaboración del plan de mantenimiento preventivos de Hardware de computadoras, redes y equipos relacionados en el Instituto Nacional de Estadístico con el fin de poder identificar las fallas que puedan ocasionadas la Perdida de información.

Alcance

- Verificación de los procesos de elaboración del plan de mantenimiento. preventivo del Hardware de computadoras, redes y equipos relacionados.
- Verificar el funcionamiento de los equipos informáticos.

Entradas

- Los inventarios de los equipos que son utilizados para el área de informática.
- Listas de los equipos que requieren mantenimiento preventivos ordenado y clasificado por quien debe realizar dicho mantenimiento.
- Informes y las fechas de los últimos mantenimiento que se realizo los equipos informáticos.

Proceso

- Revisar si hay un plan de mantenimiento donde esta la programación de los equipos que van a realizar un mantenimiento preventivo lo cual no encontramos, por medio de una encuesta a los personales obtuvimos una muestra que los personales realizan mantenimiento a sus equipos a cargos cuando sean necesario es decir cuando vean que esta fallando los siguientes equipos: monitores, teclado, mouse, impresora, scanner, cámaras de computadora, computadoras portátiles, etc. Equipos de red, router, firewalls,

switches, hubs, cableado, etc. Equipos eléctricos: caja de control de suministro de la energía.

Salida

Al desarrollar la evaluación encontramos las siguientes observaciones:

- EL Instituto Nacional de Estadística e Informática no cuenta con un plan de mantenimiento solo cuenta con una lista que le dan los trabajadores cuando encuentran fallas en la computadora.
- El Instituto Nacional de Estadística e Informática no solicita informes del mantenimiento que realizan los trabajadores.
- El Instituto Nacional de Estadística e Informática no realizan mantenimientos a todos los equipos solo de algunos que están fallando.

P014 Procedimiento para la auditoria del plan de mantenimiento correctivo de hardware de computadoras, redes y equipos relacionados

Objetivo

Analizar y evaluar el proceso de elaboración y ejecución del plan de mantenimiento correctivo de hardware de computadoras, redes y equipos relacionados en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

Alcance

- Revisión de los equipos informáticos del Instituto Nacional de estadística e Informática.
- Verificación del cronograma de mantenimiento de los equipos informáticos del Instituto Nacional de Estadística e Informática.

Entrada

- Los inventarios de los equipos que son utilizados para el área de informática.
- Listas de los equipos que requieren mantenimiento correctivo ordenado y clasificado por quien debe realizar dicho mantenimiento.
- Informes y las fechas de los últimos mantenimiento que se realizo los equipos informáticos.

Proceso

- Revisar si hay un plan de mantenimiento donde esta la programación de los equipos que van a realizar un mantenimiento preventivo lo cual no encontramos, por medio de una encuesta a los personales obtuvimos una muestra que los personales realizan mantenimiento a sus equipos a cargos cuando sean necesario es decir cuando vean que esta fallando los siguientes equipos: monitores, teclado, mouse, impresora, scanner, cámaras de computadora, computadoras portátiles, etc. Equipos de red, router, firewalls, switches, hubs, cableado, etc. Equipos eléctricos: caja de control de suministro de la energía.

Salida

Al desarrollar la evaluación encontramos las siguientes observaciones:

- El Instituto Nacional de Estadística e Informática no cuenta con un plan de mantenimiento solo cuenta con una lista que le dan los trabajadores cuando encuentran fallas en la computadora.
- El Instituto Nacional de Estadística e Informática no solicita informes del mantenimiento correctivo que realizan los trabajadores.
- El Instituto Nacional de Estadística e Informática no realizan mantenimientos a todos los equipos solo de algunos que están fallando.

P016 Procedimiento para la auditoría del plan de calidad.

Objetivo

Analizar el proceso de elaboración el plan de calidad con el fin de identificar las pérdidas debido a las fallas en los diversos procesos.

Alcance

- Verificar el proceso del plan de calidad
- Verificar los currículum vitae del personal del área informática
- Revisión el plan de calidad del área informática

Entrada

- La relación del personal contratado directamente de la organización
- Realizamos una encuesta a los personales para poder saber si los personales se capacitan o actualizan sobre su perfil

Proceso

- Realizar capacitaciones a los personales para que puedan estar capacitados y poder tomar las medias drástica sobre la prevención de las amenazas y así puedan mitigarlos a tiempos antes que ellos no haga daño a la información ya que si eso sucediera la Institución perdería su rentabilidad.
- Revisión de su currículum vitae actualizado a los personales para poder saber si ellos se capacitan y actualizan sobre su perfil.

Salida

- El Instituto Nacional de Estadística e informático no cuentan con un plan de calidad de la información.
- La organización no cuenta con el currículum actualizado del personal que laboran en dicha organización.

P020 Procedimiento para la evaluación del Currículum Vitae del personal de tecnología de la Información

Objetivo

Analizar y evaluar el currículum vitae del personal del área de tecnología de la información de la organización con el fin de identificar la probable pérdida de valor debido a fallas en los procesos de selección de personal.

Alcance

- Revisión de los Currículum Vitae del personal del área de la Información.

Entrada

- El Instituto Nacional de Estadístico e Informático no evalúa los currículum vitae a los personales que ya están laborando es decir solo revisa cuando el personal ingresa a trabajar pero no esta atento sobre sus actualizaciones, un profesional debe de estar en constante actualización para que puedan saber como mitigar a las amenazas que puedan surgir a la seguridad de la información.

Proceso

- Revisión constante a los currículum de los personales para saber quiénes de los personales están capacitados y quienes no para que la Institución pueda optar en realizar un plan de capacitaciones.

Salida

- La Institución no cuentan con la alternativa de revisión de currículum después de que el personal sea contratado, lo cual recomendamos que revisen los currículum vitae de los personales para que puedan saber que personal esta acorde con su puesto.

P037 Procedimiento para la auditoría de la seguridad de acceso a los sistemas de información

Objetivo

Analizar y evaluar la seguridad de acceso al sistema del Instituto Nacional de Estadística e informático con el fin de identificar las posibles amenazas.

Alcance

- Revisión que cada personal autorizado cuente con su usuario y contraseña.
- Revisión del procedimiento para otorgar accesos al personal.
- Análisis de pérdida de valor que se podría originar en caso se violase la seguridad de acceso o se otorgara un acceso indebido.

Entradas

- Relación de todas las personas que tienen acceso al sistema.
- Procedimiento para otorgar accesos a los usuarios.

Proceso

- Revisar detalladamente los accesos del personal sobre las opciones de los diversos sistemas de información.
- Revisar el procedimiento para otorgar accesos al personal. Verificar que por lo menos la autorización de la gerencia.
- Verificar que la contraseña que manejan cada personal sea confidencialidad y que la contraseña del un personal sepa otros.

Salida

- Diversas personas del área manipulan directamente la base de datos, por que los personales no fueron discretas con sus contraseñas por ellos recomendaría cambiar de contraseñas y sean más responsable discretos con sus contraseñas.

P038 Procedimiento para la auditoria de la seguridad de acceso a las carpetas en los servidores

Objetivo

Analizar y evaluar la seguridad de acceso a las carpetas en los servidores de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

Alcance

- Revisión de los accesos del personal sobre las carpetas en los servidores.
- Verificación los pasos para otorgar acceso al personal.
- Analizar si hubiera pérdida de valor si en caso se violase la seguridad de acceso o se otorga un acceso indebido.

Entrada

- Las contraseñas que manejan los personal del Instituto Nacional de Estadística no son secretas no están tomando con responsabilidad las contraseñas que fueron obtenías para la seguridad de la información.

Proceso

- Verificar que las carpetas del servidor tenga contraseña y que solo un personal responsable maneje la contraseña y ser bloqueadas cuando ya no utilicen el acceso al servidor automáticamente para que así se mas segura la contraseña.

Salida

- En el Instituto Nacional de Estadística e Informática algunos personales que no están autorizados tienen acceso a las carpetas de los servidores.

P054 Procedimiento para la auditoría de la seguridad de acceso al centro de cómputo principal

Objetivo

Analizar el acceso del área informática del Instituto Nacional de Estadística e Informática, con el fin de identificar las amenazas y fallas de los diversos procesos involucrados.

Alcance

- Revisión del acceso donde se encuentra la puerta donde esta ubicado el área informático del Instituto Nacional de Estadística e Informático.
- Revisión donde se recepcionan las personas visitantes al Instituto Nacional de Estadística e Informática.
- Análisis que puede suceder si violase el acceso de seguridad de la información que obtiene el Instituto Nacional de Estadística e Informática.

Entrada

- Relación de personal que ingrese a las instalaciones del área de informática.
- Capacitación al personal de seguridad de la puerta donde se encuentra ubicado dicha área para que tenga criterio para decir si tiene permiso en entrar o no a la instalación.
- Informes sobre lo sucedido a la seguridad de acceso.

Proceso

- Revisar la puerta de acceso al área de informática.
- Revisar maletas u otros que puedan transportar cosas peligrosas que puedan perjudicar.
- Detección de objetos que puedan ocasionar daños o puedan servir para perjudicar la seguridad de la información.
- Verificar el acceso si es el personal autorizado para ingresar a dicha área.

- Revisar si quien esta entrando sea la persona autorizada a la instalación.

Salida

- El Instituto Nacional de Estadista e Informática permite el ingreso a persona que no laboran en el área de informática.
- Permiten el ingreso a personas no autorizadas que no laboran, personas que solo vienen hacer gestiones de otras organizaciones.
- El personal de seguridad de recepción permite el ingreso de personas ajenas sin preguntar a quien va a visitar.
- La puerta de acceso al área se encuentra abierta durante las horas laboral
- No se lleva un registro de las personas que entra o sale del Instituto Nacional de Estadística e Informática.
- En el modulo de asignación de accesos se puede ver la clave de las personas además al tener acceso a la base de datos, también pueden hacer lo mismo.
- La contraseña de un usuario no esta en confidencialidad.

El tercer objetivo especifico establecer los lineamientos para mitigar las amenazas de la seguridad de información

- El Instituto Nacional de Estadística e Informática se recomienda realizar su plan de contingencia ya que no cuenta con un plan de contingencia ya que en fundamental que toda organización cuenten con su plan de contingencia ya que se utilizara cuando existan señales de advertencia que indiquen el riesgo que puede ocurrir.
- Solicitar un plan de capacitación para que los personales que laboran en el Instituto Nacional de Estadística e Informática para que puedan tener conocimientos de cómo contrarrestar las amenazas a la seguridad de la información.
- Los equipos informáticos cuenten con un plan de mantenimientos mensual para verificar que los equipos se encuentren un buen estado y no esperar que se malogren para recién realizar sus respectivos mantenimientos.

- Los antivirus de los equipos informáticos deben actualizarse automáticamente cuando el equipo esta prendido.
- Las contraseñas deben ser cambiadas al año dos veces y que se bloque si un usuario olvida cerrarlo se cierre automáticamente si no estamos registrando información.

ANALISIS Y DISCUSION

Así mismo, la investigación Hans Ryan Espinoza Aguinaga contribuye a esta investigación de tesis porque se tomo como referencia analizar y diseñar un sistema de gestión de seguridad de información, basado en la norma ISO /IEC 27001:2015.

La investigación de , Jorge Luis Valdiviezo Troya y Roberto Josué Rodríguez Poveda (2015) contribuye a esta investigación de tesis porque se tomo como referencia la norma ISO 27001 para la evaluación de la seguridad de la información, para identificar los activos, amenazas, vulnerabilidades, y a través de niveles de valoración para cada elementos.

Esta investigación contribuye a esta investigación de tesis porque se utilizo la metodología MAIGTI. Elaborando el plan de mejora basándose en la NTP ISO/IEC 27001 y las buenas prácticas de COBIT.

En Piura Carmen Cynthia Elizabeth Ramos Arca (2015), esta investigación de tesis nos contribuye a la tesis porque nos habla sobre "Propuesta de auditoría Informática, la Norma Técnica Peruana ISO 27001 y lo cual en nuestra investigación nos vamos aplicar sobre seguridad de la información lo que se refiere el ISO 27001.

Sangolqui, Sofía Montserrat Viteri Diaz, (2013), se considero utilizar esta tesis de investigación porque utilizamos la recomendaciones basadas en el estándar ISO 27001 porque se encuentre en capacidad de aplicar medidas de seguridad para mantener la información disponible, confiable y oportuna.

CONCLUSION Y RECOMENDACIÓN

CONCLUSION

- La evaluación de la seguridad de la información nos permitirá prevenir las amenazas que puedan enfrentar la información día a día ya que la inseguridad es un proceso continuo que exige aprender sobre las propias experiencias debido a la constante amenazas en que se encuentran en los diferentes procesos de seguridad en necesario que los usuarios enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con la que cuentan para hacerle frente posible ataques informáticos que luego se pueden traducir en grandes pérdidas, lo cuales los personales del Instituto Nacional de Estadística e Informática no están haciendo resonancia en la seguridad de la información, El Instituto Nacional de Estadística e Informática no llevan un buen control para el ingreso de las instalaciones del área de informática.
- Los personales del Instituto Nacional de Estadística e Informática no cuentan con una capacitación de seguridad de información y eso hace que los personales que laboran sean vulnerables en prevenir los riesgo de pérdidas de información, se identifico las presuntas amenazas que pueden poner en riesgo a la información al no realizar un mantenimiento preventivo a los equipos Informáticos del Instituto Nacional de Estadística Informática, A través de la metodológico de MAIGTI permitió dirigir de mejor manera las actividades de cada una de las fases de la evaluación para poder saber los riesgos que pueden presentar la información.
- Establecer los lineamientos para mitigar las amenazas atreves de los procedimientos de MAIGTI obtuvimos la información adecuada para prevenir las amenazas que pueden presentar la información ya que los usuarios cuentan con contraseña para ingresar al sistema, lo cual su contraseña no lo manejan en modo secreto lo divulgan para todos los personales que laboran.

RECOMENDACIÓN

- La recomendación seria que los personales sean capacitados sobre la seguridad de la información para que ellos puedan saber como contrarrestar una amenaza a la información y que tengan un ontrol en la entrada a las Instalaciones del Instituto Nacional de Estadística e Informática recomendamos que las personas que ingresen sea monitoreada a donde se dirigen.

- Emplear mantenimientos preventivo y correctivo a todos los equipos informáticos cada dos meses para prevenir su mal funcionamiento y elaborara plan de contingencia ya que es una herramienta muy valiosa que basada por lo general en un análisis de riesgo, nos permitirá ejecutar un conjunto de normas, procedimientos y acciones básicas de respuesta que se debería tomar para afrontar de manera oportuna, adecuada y efectiva , la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir en las instalaciones y equipos informáticos.

- En cuanto los acceso a las instalaciones del Instituto Nacional de Estadística e Informática deben ser más controlada y no dejar ingresar a personas que no están autorizadas al ingreso de dicha organización

AGRADECIMIENTO

Quisiera expresar mi más sincera gratitud a mis queridos padres Modesto Laurente castillejo y a mi madre Clara Carreño Rodriguez que son la luz mi guía quienes supieron brindarme su amor y aprecio para concluir con mis sueños y ser una persona de bien, y a todas aquellas personas e Instituciones que han mostrado interés y apoyo en la elaboración y conclusión de mi presente tesis.

Gracias a toda la plana de docente de la universidad, por los conocimientos que allí se imparten.

Tania Estela Laurente Carreño

REFERENCIA BIBLIOGRAFÍCAS

Alberto G, A. G. (2007). *Implantacion del ISO 27001:2005 Sistema de Gestion de seguridad de informacion.* LIMA: CENTRUM.

Antonio, A. P. (2011, noviembre 29). *Metodologia MAIGTI.*

Bravo, M. V. (2015). *"Auditoria al control y mantenimiento de la infraestructura tecnologica del departamento tecnologico de la ESPAM MFL"* Escuela Superior Politecnica Agropecuario de Manuel Felix Lopez. Retrieved from http://repositorio.espam.edu.ec/bitstream/42000/64/1/Mar%C3%ADa%20V%C3%ADctoria%20Rivera%20Ch%C3%A1vez%20-%20Mar%C3%ADa%20Fernanda%20Zambrano%20Bravo.pdf

Cappilletti, I. (Julio). *Evaluacion Educativa Fundamentos y practicas* (Reimpresa ed.). Brasil: ERNEST ABADAL.

Diaz, S. M. *"Evaluacion Tecnica de la seguridad informatica del data center de la brigada de fuerza especiales NO.9 Patria".* Escuela Politecnica del ejercito, Sangolqui.

Espinoza Aguinaga, H. R. (25 de Octubre de 2013). *Analisis de diseño de un sistema degestionde seguridad de informacion basada en la norma ISO/IEC27001:2005* Universidad Catolica del Peru. Recuperado el 2013, de google: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4957/espinoza_hans_analisis_sistema_gestion_seguridad_informacion_iso_iec%2027001_2005_comercializacion_productos_consumo_masivo.pdf?sequence=1

ISACA. (1996). *COBIT.* Boston: Comite Directivo de COBIT.

Poveda, J. L. (2015, Marzo). *Informe de evaluación de seguridad en la información Basada en la norma ISO 27001 en el departamento de TI de una Empresa de Lácteos",* Universidad Politécnica Salesiana de Ecuador . Retrieved 2015, from https://dspace.ups.edu.ec/bitstream/123456789/10307/1/UPS-GT001204.pdf

Ramos Arca, C. C. (2015). *" Propuesta de auditoria informatica para el sistema de informaxion en salud y el aplicativo para los sistemas mas importantes de cada establecimiento de salud de la unidad ejecutora 400 en la region Piura " Universidad Nacional de Peru.* Retrieved from

http://repositorio.unp.edu.pe/bitstream/handle/UNP/683/IND-RAM-ARC-15.pdf?sequence=1&isAllowed=y

Shannon, C. (1948). *Informacion informatica e internet del ordenador personal a la empresa 2.0.* España: vision libros.

Yan Carranza, F., & Zavala Vasquez, C. L. (2013). *"Plan de mejora de la seguridad de Informacion y continuidad del centro de datos de la Gerencia Regional de Educacion La Libertad aplicando lineamientos ISO 27001 y buenas practicas COBIT"* Universidad Privada Antenor Orrego Trujillo. Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/10307/1/UPS-GT001204.pdf

ANEXOS

ANEXO – 01

MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	VARIABLES
Problema General ¿De qué manera Evaluaremos la seguridad de la información al instituto nacional de estadística e inf ormática?	**Objetivo General** • . Realizar la evaluación de la seguridad de información al Instituto Nacional de Estadística e Informática **Objetivo Especifico** • Determinar los procesos relativos de la seguridad de información. • Aplicar la metodología MAIGTI para la seguridad de información. • Establecer los lineamientos de cambio para la mitigación de las amenazas de la seguridad de información.	**Variable de Estudios** Evaluación de la Seguridad. **Indicadores** ✓ Analizar los procesos relativos de la seguridad de información ✓ Emplear la metodología MAIGTI para la seguridad de información. ✓ Establecer los lineamientos de cambio para la mitigación de las amenazas de la seguridad de información.

ENCUESTA DE LzA SEGURIDAD DE LA INFORMACION AL INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

1¿EL PERSONAL QUE INGRESAN EN LAS INSTALACIONES SE IDENTIFICAN ?

- SI
- NO

2¿TIENES SOFTWARE ANTIVIRUS INSTALANDO EN TU COMPUTADORA?

- SI
- NO
- NO SE

3¿CON QUE FRECUENCIA ACTUALIZAN UN SOFTWARE ANTIVIRUS?

- SE HACE AUTOMATICAMENTE
- AL MENOS DOS VECES POR SEMANAS
- AL MENOS UNA VEZ POR SEMANA
- AL MENOS UNA VEZ AL MES
- DE VES EN CUANDO , CUANDO RECUERDO
- NUNCA
- ESPECIFIQUE……

4¿UTILIZAS UN SOFTWARE DE FIREWALL EN TU ORDENADOR?

- SI
- NO
- NO SE

5¿LA ADMINISTRADORA ESTA MONITOREANDO TU COMPUTADOR?

- SI
- NO
- NO SE

6¿CUENTAN CON UN PLAN DE CONTINGENCIA ?

- SI
- NO
- NO SE

7¿CUENTAN CON UN PLAN DE CAPACITACION?

- SI
- NO
- NOSE

8¿CON QUE FRECUENCIA REALIZAN UN PLAN DE MANTENIMIENTO PREVENTIVO A LOS EQUIPOS INFORMATICO ?

- AL MENOS DOS VECES POR SEMANAS
- AL MENOS UNA VEZ POR SEMANA
- AL MENOS UNAVEZ AL MES
- DE VES EN CUANDO , CUANDO RECUERDO
- NUNCA
- ESPECIFIQUE……..

9¿ CON QUE FRECUENCIA REALIZAN UN PLAN DE MANTENIMIENTO CORRECTIVO A LOS EQUIPOS INFORMATICO.

- AL MENOS DOS VECES POR SEMANAS
- AL MENOS UNA VEZ POR SEMANA
- AL MENOS UNAVEZ AL MES
- DE VES EN CUANDO , CUANDO RECUERDO
- NUNCA
- ESPECIFIQUE……..

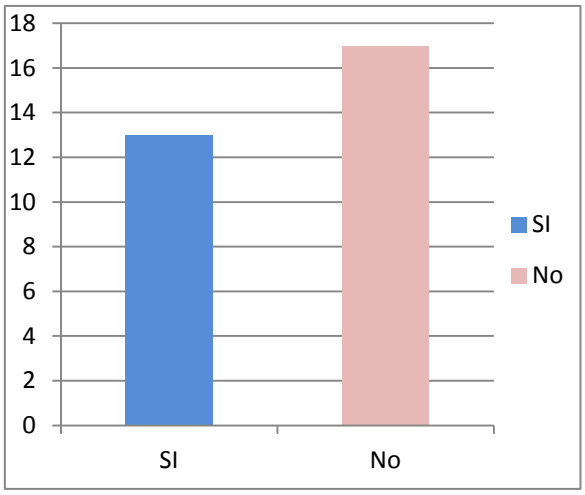
10¿CON QUE FRECUENCIA REALIZAN CAPACITACIONES?

- AL MENOS UNA VEZ POR SEMANA
- AL MENOS UNAVEZ AL MES
- DE VES EN CUANDO , CUANDO RECUERDO
- NUNCA
- ESPECIFIQUE……....

Aplicación de la Encuesta

1¿El personal que ingresan en las instalaciones del INEI se identifican?

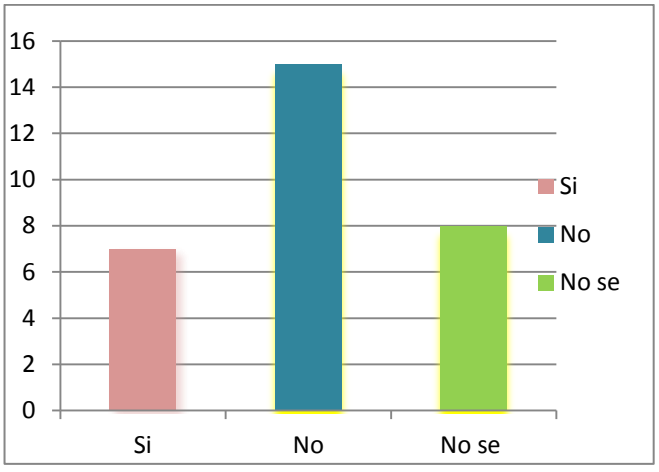
1. SI
2. NO



Interpretación:
SI = 13 Personas
NO = 17 Personas

2¿Tienes software antivirus instalando en tu computadora?

- SI
- NO
- NO SE

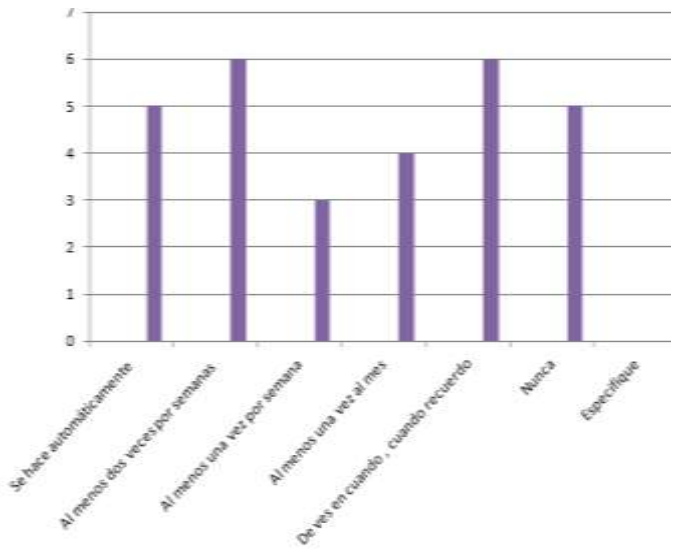


Interpretación:
SI = 7 Personas
NO = 15 Personas
NO SE = 8 Personas

3¿Con que frecuencia actualizan un software antivirus?

- Se hace automáticamente
- Al menos dos veces por semanas

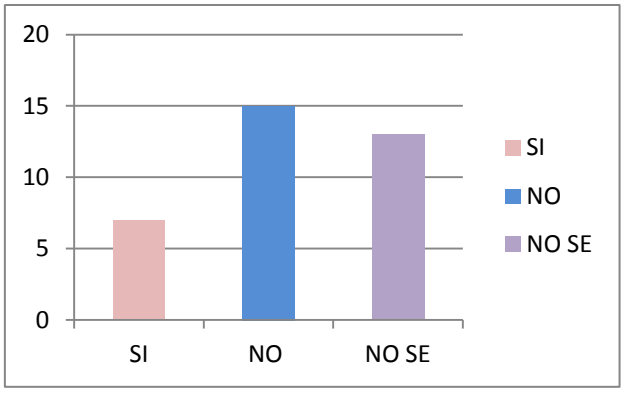
- Al menos una vez por semana
- Al menos una vez al mes
- De vez en cuando , cuando recuerdo
- Nunca
- Especifique……



Interpretación:
Se hace automáticamente = 5
Al menos dos veces por semanas = 6
Al menos una vez por semana = 3
Al menos una vez al mes = 4
De vez en cuando , cuando recuerdo = 6
Nunca = 5
Especifique = 0

4¿Utilizas un software de firewall en tu ordenador?

- SI
- NO
- NO SE

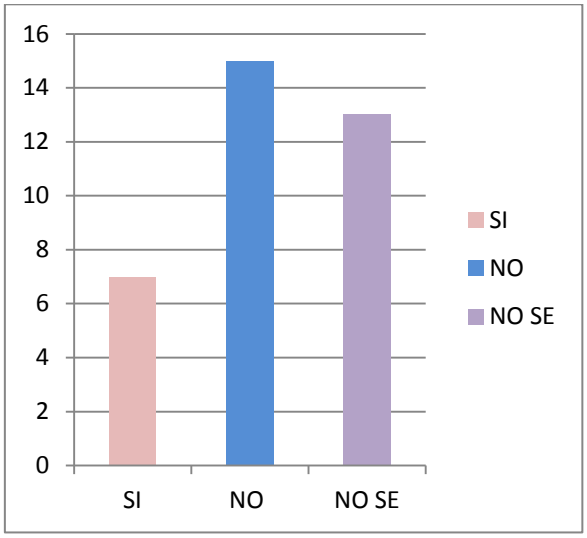


Interpretación:
SI = 8
NO = 15
NO SE = 17

¿La administradora esta monitoreando tu computador?

- SI

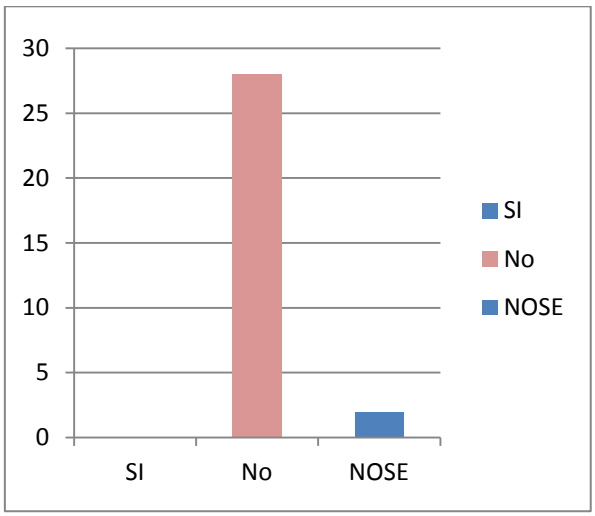
- NO
- NO SE



Interpretación:
SI = 20 Personas
NO = 5 Personas
NO SE = 5 Personas

6¿Cuentan con un plan de contingencia?

- SI
- NO
- NO SE

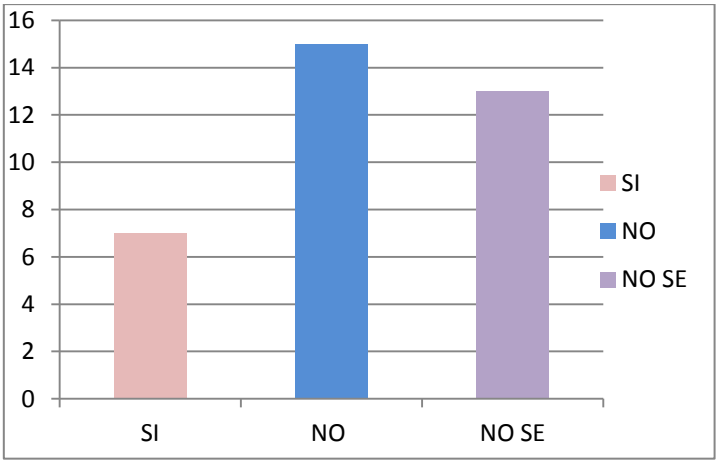


Interpretación:
SI = 0 Personas
NO = 28 Personas
NO SE = 2 Personas

7¿Cuentan con un plan de capacitación?

- SI

- NO
- NO SE

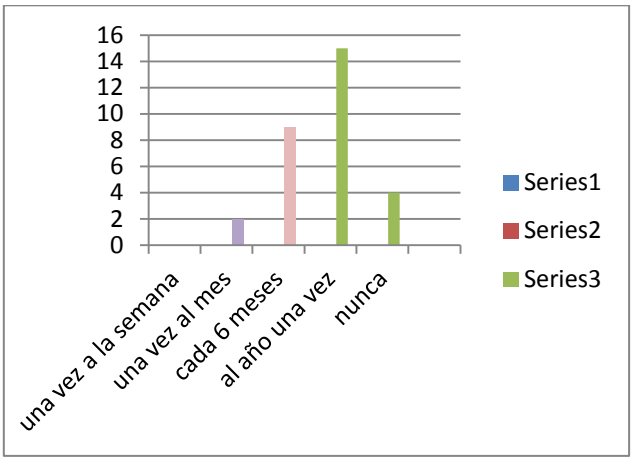


Interpretación:
SI = 0 Personas
NO = 28 Personas
NO SE = 2 Personas

8¿Con que frecuencia realizan un plan de mantenimiento preventivo a los equipos informático ?

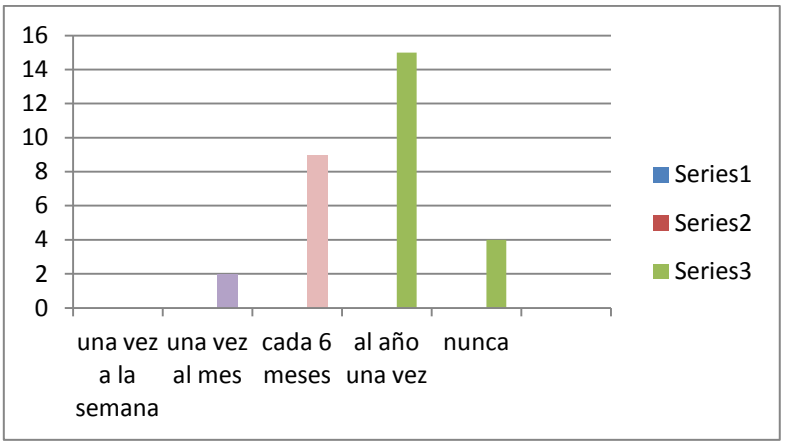
- al menos dos veces por semanas
- al menos una vez por semana
- al menos unavez al mes
- de ves en cuando , cuando recuerdo
- nunca
- especifique……

Interpretación:
Al menos dos por semana = 0 persona
Al menos una vez por semana = 6 personas
Al menos una vez al mes = 15 personas
De ve en cuando, cuando recuerdo =9 personas
Nunca = 0 personas
Especifique = 0 personas



9¿ Con que frecuencia realizan un plan de mantenimiento correctivo a los equipos informático?

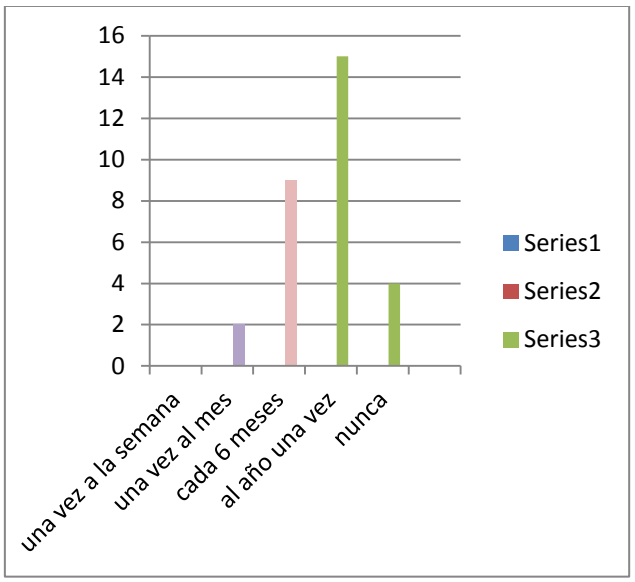
- Al menos una vez por semana
- Al menos una vez al mes
- Una vez al año
- Nunca



Interpretación:
Al menos una vez por semana = 0 persona
Al menos una vez al mes = 0 personas
Una vez al año = 30 personas
Nunca = 0 personas

10¿Con que frecuencia realizan capacitaciones?

- al menos una vez por semana
- al menos una vez al mes
- Cada 6 meses
- Una vez al año
- Nunca



Interpretación:
Una vez a la semana = 0 personas
Una vez al mes = 2 personas
Cada 6 meses = 9 personas
Al año una vez = 15 personas
Nunca = 4 personas