Fecha de Realización:	15/01/2019
Programa:	Especialización de Seguridad Informática
Título:	Diseño del sistema de gestión de seguridad de la información para el instituto tolimense de formación técnica profesional- ITFIP para el departamento de sistemas, bajo la norma ISO 27001:2013
Autor(es):	Padilla Ubaque Mario Andrés
Director:	Magíster. Torres Mantilla Eduard Antonio

RESUMEN

El presente proyecto de grado se enfocó en la elaboración del diseño de un sistema de gestión de seguridad de la información (SGSI) en la dependencia de sistemas en la Institución de Educación Superior – ITFIP del Espinal, Tolima. Bajo la norma ISO 27001:2013 utilizando como herramienta metodológica para el análisis y gestión de riesgos MAGERIT V3. Como cualquier entidad pública del estado maneja recursos del tesoro nacional, en diferentes proyectos, llevando un volumen muy alto de información como el de empleados, contratistas y estudiantes, manejando diferentes niveles de seguridad en su información, el departamento de sistemas es uno de los más sensibles en el manejo de esta información, en este departamento se aloja la mayoría de información en sus servidores y aplicaciones.

PALABRAS CLAVE

Seguridad de la Información, Seguridad informática, Vulnerabilidades, Análisis de riesgos, ISO/IEC 27001.

CONTENIDO

El documento presenta tres fases con 25 capítulos en total

Fase 1

- Recolección de información de la institución y estado actual del ITFIP con respecto al Sistema de Información.
- Estado actual del sistema de información con respecto ISO/IEC 270001:2013 en el departamento de sistemas del ITFIP
- Fase 2 Análisis de Riesgos
- Efectuar un análisis de riesgo empleando la metodología MAGERIT
- Inventarios de activos
- Clasificación de los activos
- Valoración de los activos según su importancia
- Análisis de la jerarquía de los activos entre sus grupos internos
- Estimación de los valores de criterio en sus dimensiones de aplicabilidad
- Estimación de las amenazas que pueden afectar los activos.
- Identificación de vulnerabilidades de los activos de información ante las amenazas potenciales
- Inspección visual de los activos de información(informe)

- Estimación de las vulnerabilidades que pueden afectar a cada uno de los activos.
- Estimación del impacto que causaría la PÉRDIDA de cada activo
- Estimación de la probabilidad de que ocurra perdida del activo
- Estimación del riesgo
- Aplicación de las salvaguardas a cada tipo de activo
- Estrategia para el tratamiento de los riesgos de cada uno de los activos de la dependencia
- Técnicas para el tratamiento del riesgo
- Informe y evaluación de los tratamientos de riesgo
- Identificación
- Tratamiento del riesgo
- Técnicas para el tratamiento del riesgo
- Fase 3 Declaración de aplicabilidad

DESCRIPCION DEL PROBLEMA

Con el gran volumen de información que maneja la institución, la universidad no cuenta con un sistema de gestión de seguridad de información formal, por ende el departamento de sistemas tampoco lo tiene, por esta razón resultan dos interrogantes ¿es suficiente la seguridad que se presta actualmente para proteger toda la información? y ¿El sistema de gestión seguridad y sus correspondientes controles en riesgos basados en la ISO27001:2013 puede minimizar las vulnerabilidades, riesgos y amenazas de la información administrada por la dependencia de sistemas de la Institución de Educación Superior - ITFIP?

OBJETIVOS

Objetivo general

Diseñar el sistema de gestión de seguridad de la información para la institución de educación superior – ITFIP, para el departamento de sistemas, bajo la norma ISO/IEC 27001:2013.

Objetivos específicos

Realizar un estudio para describir en qué estado está la dependencia de sistemas en temas de seguridad de la información. Para de identificar procesos o políticas de seguridad de la información.

Efectuar un análisis de riesgo utilizando la metodología MAGERIT. Con el propósito de determinar y valorar los riesgos amenazas y vulnerabilidades.

Construir una declaración de aplicabilidad para mitigar los riesgos basados en la ISO27001:2013, con el fin de minimizar los riesgos que fueron identificados.

Proponer mediante un documento políticas y lineamientos de seguridad de información, de acuerdo con el análisis realizado, basados en la norma ISO 27001:2013.

METODOLOGIA

La Institución de Educación Superior – ITFIP permitió utilizar la norma internacional ISO 27001:2013 en sus 14 dominios para la aplicación en la institución. Como marco referente para el proyecto aplicado, también en su desarrollo se utilizó la metodología MARGERIT para el desarrollo del análisis de riesgos, utilizando metodologías certificadas para un buen desarrollo.

REFERENTES TEÓRICOS Y CONCEPTUALES

Para este proyecto se utilizó varios conceptos que aplicaran bajo la normatividad legal del estado colombiana, como referentes directos para este proyecto están los estándares ISO son un marco legal y permitido para aplicarlo en Colombia, que fue aplicado en su totalidad como ISO27001:2013, también la metodología de análisis de riesgos de información sistemas de información mencionada en el ítem 12, junto a otras ciencias como metodologías de investigación a nivel tic, dieron como resultado un detallado enfoque para la detección y mitigación de riegos, amenazas y vulnerabilidades, para minimizar el máximo el impacto que produciría estas situaciones.

RESULTADOS

ESTADO ACTUAL DE LA SI CON RESPECTO ISO/IEC 270001:2013 EN EL DEPARTAMENTO DE SISTEMAS DEL ITFIP, con este objetivo se dio como resultado que aunque la INSTITUCION DE EDUCACIÓN SUPERIOR ITIFIP, en su DEPARTAMENTO DE SISTEMAS, aunque tiene dificultades o problemas con respecto en la seguridad de información, no está del todo mal, ya que me forma mediana la tienen en cuenta más sin embargo entre una escala de, Rojo, Naranja y Amarillo, donde Rojo es CRITICO, Naranja es MODERADO y Amarillo es TENÚE, el DEPARTAMENTO DE SISTEMAS, se encuentra en estado Naranja.

EFECTUAR UN ANÁLISIS DE RIESGO EMPLEANDO LA METODOLOGÍA MAGERIT, como resultados de este objetivo, en el documento se puede apreciar, la clasificación de todos los activos que el DEPARTAMENTO DE SISTEMAS, tiene en su disposición, también la representación de que tan importantes son estos activos, el ¿Qué pasaría si alguno desapareciera?, ¿Qué tan probable es que esto ocurra? O ¿Qué tan vulnerables son estos activos a ciertas amenazas?

DECLARACIÓN DE APLICABILIDAD, BAJO LA NORMATIVA ISO/IEC 27001, aquí encontramos como o que se debe realizar en el DEPARTAMENTO DE SISTEMAS, para que las amenazas encontradas anteriormente sean minimizadas o si se llegan a presentar saber qué hacer, para que no pasen a mayores.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE SISTEMAS, las políticas y pasos que debe tener en cuenta el encargado del área de sistemas, para que primero personas sin autorización no ingresen a documentos o información importante del área, como también los planes de contingencia para cuando alguna amenaza ocurra los funcionarios sepan que pasos deben seguir para que estas no pasen a mayores.

CONCLUCIONES
El área de sistemas tiene un estado Moderado en su seguridad de información, lo cual nos permite entender que el área tiene ciertos inconvenientes en algunos puntos o apartados que la ISO/IEC 27001 evalúa. La importancia que tienen algunos activos o información en el área de sistemas y el saber que puede ocurrir si alguno de estos falla o no se encuentran,
FUENTE BIBLIOGRAFICA
Dirección general de modernización administrativa, P.e (2012). MAGERIT versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información Madrid. ISO27001 – Sistema de Gestión de la Seguridad de la información. http://www.iso27000.es/download/doc_sgsi_all.pdf ITFIP, Institución de Educación Superior. Manual de Procesos y Procedimientos. “ITFIP” Versión N.º 5.0. Lugar de Publicación: Espinal-Tolima, diciembre de 2016. MAGERIT V3, Libro 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Administraciones Públicas de España. MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones públicas, 2012. RAE.REAL ACADEMIA ESPAÑOLA. Definición de Investigación, Análisis, Gestionar, Recolectar, Hardware, Disponible t: http://dle.rae.es