Fecha de Realización:	19/05/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Proyecto Aplicado
Título:	Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del Sena Regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT.
Autor(es):	Palacios Palacios, Jeysser Aurelio
Palabras Claves:	Análisis, Riesgo, Seguridad, Controles, Integridad.
Descripción:	Con el desarrollo del presente proyecto aplicado se busca a través de la aplicación de una metodología de gestión de Riesgo como es MAGERIT. Se realice un inventario de los activos de información con los que cuenta la dependencia de Formación Profesional Integral del SENA Regional Guainía. Para posteriormente identificar los riesgos, vulnerabilidades y amenazas asociados a dichos activos de información. Y a partir de este se puedan definir los controles y salvaguardas necesarias enfocadas a proteger los activos de información y la infraestructura tecnológica de la dependencia.

Fuentes bibliográficas destacadas:

ALVAREZ SOSA, Yenny Maribel. Diseño De Una Metodología Para El Análisis De Riesgo En Los Sistemas De Gestión De Seguridad De Información (Marisgsi) En Las Universidades De Barquisimeto Estado Lara. Trabajo De Grado Magister Scientiarum En Ciencias De La Computación. Barquisimeto: Universidad Centroccidental “Lisandro Alvarado”. 2013. 2-34p

LOPEZ, Jhon Alexander y ZULUAGA TAMAYO, Andrés Fabián. Desarrollo De Una Metodología Para El Control De Riesgos Para Auditoria De Base De Datos. Tesis De Grado Ingeniería De Sistemas Y Computación. Pereira: Universidad Tecnológica De Pereira. 2013. 5-51p.

MATALOBOS VEIGA, Juan Manuel. Análisis de Riesgo de Seguridad Informática. Trabajo de Grado analista de sistemas de información. Madrid. Universidad Politécnica de Madrid. 2009. 46-55p.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 (23, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

<table>
<tr><td colspan="2">Bogotá D.C. El Ministerio, 2013. 11 p.

VÁSQUEZ GAONA, karina del Rocio. APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANALISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A EN LA CIUDAD DE MACHALA. Tesis de grado para la obtención del título Ingeniera de sistemas. Cuenca: Universidad Politécnica Salesina. Sede cuenca. Facultad de Ingeniería. 2013. 53-79p.

DUARTE MARTINEZ, Maria Carolina. DISEÑO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA. Trabajo de grado presentado como requisito para optar al título de: Especialista en Seguridad Informática. Cúcuta: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2019. 29-56p.</td></tr>
<tr><td>Contenido del documento:</td><td>Introducción
Título Del Proyecto
1. Formulación Del Problema
1.1 Presentación
1.2 Planteamiento Del Problema
2. Justificación
3. Objetivos
3.1 Objetivo General
3.2 Objetivos Específicos
4. Alcance Y Delimitación
4.1 Alcance
4.2 Delimitación
5. Marco Referencial
5.1 Antecedentes
5.2 Marco Teórico
5.2.1 Seguridad Informática.
5.2.2 Seguridad De La Información.
5.2.3 Sistema De Gestión De Seguridad De La Información (SGSI).
5.2.4 Metodología De Gestión De Riesgo.
5.2.5 Análisis De Activo.
5.3 Marco Conceptual
5.3.1 Seguridad.
5.3.2 Amenazas.
5.3.3 Vulnerabilidades.
5.3.4 Ataques.
5.3.5 Confidencialidad.
5.3.6 Autenticación.
5.3.7 Integridad.
5.3.8 Control De Acceso.
5.3.9 Base De Datos.
5.3.10 Activo De Información.
5.3.11 Disponibilidad.
5.4 Marco Legal
5.4.1 ISO 27000.</td></tr>
</table>

	5.4.2 ISO/IEC 27001 5.4.3 ISO/IEC 27005 5.4.4 ISO/IEC 27002 5.4.5 Ley 1273 Del 2009 5.4.6 Ley 1581 Del 2012 5.4.7 Decreto 1377 Del 2013 5.5 Marco Contextual 6. Diseño Metodológico 6.1 Metodología De Aplicación 6.2 Población Y Muestra 6.3 Técnicas De Recolección De Información 6.4 Metodología De Desarrollo 7. Aplicación De La Metodología 7.1 Metodología De Gestión De Riesgo 7.2 Alcance Del Análisis 7.3 Fase 1 7.3.1 Identificación Y Clasificación De Activos. 7.3.2 Descripción De Los Activos. 7.3.3 Dependencia De Activos. 7.3.4 Valoración De Activos. 7.4 Fase 2. 7.4.1 Clasificación De Amenaza A Los Activos. 7.4.2 Identificación De Las Amenaza De Los Activos. 7.4.3 Matriz De Riesgos. 7.4.4 Evaluación Del Riesgo. 7.4.5 Análisis De Resultados De La Matriz De Riesgos. 7.5 Fase 3 7.5.1 Plan Tratamiento De Riesgo. 7.5.2 Declaración De Aplicabilidad. 8. Conclusión 9. Recomendaciones 10. Bibliografía Anexos
Marco Metodológico:	Para poder solución a cada una de las actividades inmersas dentro de los objetivo definidos y en función al problema planteado. Se trabajó aplicando la secuencia de actividades que contempla la metodología MAGERIT. Proporcionado los insumos que permitieron a partir del hacer, hallar los resultados esperados para el aseguramiento de los activos de información asociados a la dependencia de Formación Profesional Integral del SENA Regional Guainía.
Conceptos adquiridos :	Con el desarrollo de este proyecto aplicado se abordaron procedimientos que permitieron clarificar conocimientos con relación a los controles de la norma ISO 27002:2013 para la protección de los activos de información, la gestión de riesgo para la identificación de amenazas. Igualmente se trabajaron conceptos relacionados con la integridad, la confidencialidad y disponibilidad de los datos, ataques y salvaguardas que los

	afectan.
Conclusiones:	Una vez desarrollado el proyecto aplicado. “Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del Sena regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología MAGERIT”. Se puede concluir la necesidad de establecer las condiciones de seguridad necesarias para proteger los activos de información con los que la dependencia de Formación Profesional Integral del SENA Regional Guainía. Utiliza diariamente para el cumplimiento de la meta institucional asignada por Dirección General. Lo anterior identificando las vulnerabilidades, amenazas y riesgos asociados a cada activo y de allí definir las salvaguardas y controles pertinentes que permitan realizar un tratamiento adecuado a dicha riesgo. Las medidas de seguridad adoptadas se recomiendan en el entendido de garantizar la continuidad del negocio, a partir de velar porque no sé afecte la integridad, confidencialidad y disponibilidad de los activos de información asociados a la dependencia de formación. Una apropiada y eficiente aplicación de la gestión del riesgo provee los insumos necesarios para minimizar o en su defecto eliminar los peligros que rodean no solo la información, sino también demás activos hardware y software con los que cuenta la dependencia de formación. Definir un plan de auditoria que basada en el modelo PHVA permita evaluar la eficiencia de los controles y salvaguardas adoptados, para mitigar el riesgo sobre cada activo de información. Determinar si el control adoptado fue o no el apropiada permitirá de manera temprana realizar las acciones de mejora a que haya lugar. Establecer un plan de capacitación a los funcionarios de la dependencia de formación sobre los protocolos de seguridad de la información y su importancia. Los cuales fueron definidos en las políticas de seguridad de la información, con el ánimo que estos sean aplicados contribuyendo al tratamiento adecuado de los datos personales de los aprendices, instructores y funcionarios, basados en la normatividad legal vigente. Siendo la información un activo valioso para la dependencia de formación. Debe en la medida de lo posible adoptar todos y cada una de las recomendaciones planteadas con el desarrollo de este proyecto. Ya que van orientadas a garantizar la confiabilidad e integridad de la información producida allí bajo estándares de seguridad internacional a través de los controles definidos en la ISO 27001:2013.