

Fecha de Realización: 12/12/2019
Título: SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA SGSI EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO – COLOMBIA
Autor: BUITRAGO GIRALDO, Ruby Esperanza
Palabras Claves: Seguridad informática, sistema de gestión, universidad pública, Eje Cafetero, SGSI.
Descripción: Trabajo de grado, monografía para optar al título de Especialista en Seguridad Informática de la UNAD.
Fuentes: 78 fuentes bibliográficas
<p>Contenido del documento: La ecorregión Eje Cafetero, en Colombia, se caracteriza geográfica, social e históricamente por estar ubicada en el corazón de su zona andina y porque ha generado una cultura propia y una forma de vida alrededor del cultivo y comercialización del café, como uno de los tradicionales y trascendentes contribuidores al desarrollo del país por la vía de su exportación y del reconocimiento mundial de su calidad. En ella, se tienen cinco universidades públicas: Universidad Nacional de Colombia sede Manizales, Universidad de Caldas, Universidad Tecnológica de Pereira, Universidad del Quindío y Universidad Nacional Abierta y a Distancia UNAD sede Dosquebradas. Se quiso, entonces, con esta monografía, indagar sobre el estado de cosas de los sistemas de gestión de la información que se lleva en ellas.</p> <p>El documento que sustenta la monografía incluye primero una introducción donde se expresa que el panorama de la implementación de sistemas de gestión de seguridad informática en infinidad de organizaciones en Colombia no aparece muy claro y que, dentro de estas organizaciones, lamentablemente se encuentran también universidades públicas y privadas del país, y en ellas aparecen las universidades públicas del Eje Cafetero colombiano. Seguidamente, se plantea el problema, es decir, la necesidad que tiene toda organización y entre ellas las universidades de manejar las TIC's, los SGSI y las BDs, así como las redes de Internet e Intranet, pero, a su vez, de garantizar al máximo la seguridad de la información que posee, por lo que se vuelven organismos en donde no es fácil garantizar la total seguridad de sus sistemas y herramientas de la información. Por ello, ameritaba desarrollarse con criterio académico una monografía que diera claridades sobre ello y que sirviera a las autoridades académicas de esas universidades para la toma de decisiones al respecto en la mejor dirección posible. Lo anterior dio pie para que, a continuación, se formularan los objetivos, general y específicos, los alcances y los resultados esperados con este estudio. Lo que continuaba de la investigación, definida como de tipo documental, exigió la inclusión de un marco teórico conceptual, desarrollando brevemente los temas de la sociedad de la información, algunas definiciones de seguridad informática, la importancia de tener claros los conceptos de amenaza, vulnerabilidad y riesgos informáticos, así como todo lo relacionado con los distintos tipos de ataques</p>

informáticos, la trascendencia que adquieren cada vez más el que se tracen políticas de seguridad informática en las organizaciones, la existencia y la aplicación de normas internacionales y leyes de seguridad informática, la relación entre la seguridad de la información y los sistemas de gestión de esta, es decir, los denominados SGSI. Sobre estos, se incluye la definición del Ciclo de Mejora Continua PDCA en el establecimiento de un SGSI y las etapas de implementación de este.

Seguidamente, se discuten las metodologías y herramientas existentes para el análisis y gestión de riesgos potenciales y las dificultades para la implementación de un SGSI en las universidades públicas en Colombia y en el Eje Cafetero. Con fines de ilustración y comparación, se analizan varios referentes para este estudio en otros países y en Colombia, y se plantea por qué se justifica implementar un SGSI en las universidades en estudio, lo que obliga a analizar en detalle la ley colombiana 1273 de 2009 y su aplicación en las universidades públicas del eje cafetero.

Luego, en procura de conocer el estado del arte de la seguridad informática en las cinco universidades escogidas, se presenta una información general sobre ellas y su contexto histórico y geográfico, acompañada de información estadística de las mismas.

Avanzando en el documento, se encuentra una disertación sobre la selección de una herramienta adecuada para la recopilación de información sobre seguridad informática y la posibilidad de que se tuviera un SGSI en las universidades del estudio, se selecciona entre esas herramientas un cuestionario para ser enviado por correo electrónico a los funcionarios encargados del asunto en cada una, se justifica el porqué de esa herramienta y no otra, se diseña el cuestionario, se hace la pesquisa sobre a quiénes se les debe dirigir y se les envía, sin descartar la posibilidad de tener entrevistas personales con tales funcionarios cuando fuera del caso.

Recogida la información, se pasó a la fase de análisis de las respuestas al cuestionario, las cuales se plasmaron en un cuadro que las recoge todas y que sirve incluso con fines comparativos, y sobre él se hizo dicho análisis, que alimentaron las conclusiones del estudio.

Dada la importancia que en el desarrollo de las etapas de un SGSI tienen las políticas de seguridad informática en cualquier entidad (y en este caso particular, en una universidad pública), se investigó exhaustivamente la existencia y las características de estas políticas en cada una de las cinco universidades y se incluyeron en el documento las de todas, pues todas tienen.

El siguiente paso fue el de hacer un análisis de las políticas de seguridad informática de las universidades públicas del Eje cafetero, resaltando virtudes y

debilidades y, seguidamente, una propuesta con mecanismos para reforzar la importancia de un SGSI en esas universidades. Así, se tuvo todo listo para extraer las conclusiones que se tuvieron del trabajo, las cuales se complementaron con unas recomendaciones para las universidades y sus funcionarios del área, algunas de las cuales se incluyen enseguida:

Si alguna universidad de las estudiadas aquí no posee aún un SGSI, convendría trazarse como una meta de su desarrollo institucional el contar con este sistema en un plazo no mayor a dos (2) años.

Para poder garantizar lo anterior, se haría necesario reforzar las OTIC de esas universidades tanto en su estructura orgánica como en la vinculación de personal especializado en el tema de la seguridad informática y de los SGSI.

En alguno casos concretos conocidos por la autora de la monografía, se deja entrever cierta laxitud y hasta bajas de guardia en el seguimiento y evaluación de los procesos que llevan, así como en la aplicación de las políticas de seguridad informática que tienen, lo que justifica el recomendar acciones de auditoria periódicas de dichos procesos (por ejemplo, cada año).

Metodología: Por su carácter de monografía, se define como una investigación documental.

Conclusiones: Se consideran logrados los objetivos de la monografía en cuanto a que se tiene con ella un panorama bastante claro del estado de cosas de los sistemas de gestión de la información que se lleva en las cinco universidades públicas del Eje Cafetero: Universidad Nacional de Colombia sede Manizales, Universidad de Caldas, Universidad Tecnológica de Pereira, Universidad del Quindío y Universidad Nacional Abierta y a Distancia UNAD sede Dosquebradas, en las cuales se pudo indagar el conocimiento y uso que en ellas se tiene de normas -especialmente la 27001- y metodologías para la definición de sus políticas de seguridad informática y otras acciones en dirección a poner en marcha -y lograrlo en algunos casos- un SGSI.

El uso de una herramienta como un cuestionario para indagar tales cosas, con la cual se ganó la confianza de los funcionarios que lo contestaron -a pesar de que pudieron mostrarse algo más recelosos y reservados, pero no lo fueron a nuestro parecer- contribuyó sustancialmente al logro de los resultados destacados arriba. Esto pudiera interpretarse como una forma de manifestar gran interés en el tema, de demostrar que se estaba efectivamente trabajando de manera ardua en él y que su importancia y trascendencia se encontraba al orden del día en cada una de sus universidades. Se considera que, al calor de charlas y de cuestionarios y de enterarlos de la ejecución de esta monografía se hizo por parte de la autora un

reforzamiento en ellos de la importancia del asunto ante las vulnerabilidades y riesgos que enfrentan por ataques informáticos, cada vez mayores.

Como asunto particular, pero de mucha importancia, sorprende que el 40% de las universidades que aquí se están estudiando no cuenten con funcionarios que sean expertos en el tema de la seguridad informática, porque esta es una de las manifestaciones más contundentes de la vulnerabilidad de la entidad frente a ataques informáticos, a pesar de la disposición de ánimo y el conocimiento que al respecto pudiera tener el funcionario actualmente encargado.

Del análisis discriminado por universidad en el capítulo 11, el autor encuentra de manera satisfactoria que los adelantos en la implementación de un SGSI logrados por las Universidades UNAD y UTP se muestran hasta ahora mayores que los alcanzados por las otras tres universidades, pero mantiene la esperanza de que ellas estén en el proceso para igualar y hasta superar los de las mencionadas, para lo cual mantendrá sus ojos puestos en ello, en su condición de especialista en el área que está cercana -geográfica y profesionalmente- a dos de ellas, la UNAL y la UDECALDAS.

La autora considera que hubiera sido posible conseguir información más particularizada en cada universidad sobre detalles de los estándares y metodologías usados, pero también concluye que esto tal vez no se tuvo por razones obvias, como los criterios de confidencialidad con que deben manejar hacia afuera de la entidad dicha información.

Finalmente, se tiene un documento monográfico bien concebido y suficientemente detallado, que establece diagnósticos y análisis de la situación de los SGSI en cinco universidades públicas del eje cafetero colombiano, da claridades sobre la aplicación de normas internacionales y nacionales al respecto, y que aspira a llevar a las directivas que menos han avanzado en el asunto a ampliar sus niveles de conciencia sobre la inmensa importancia que tiene hoy en día la implementación de un SGSI en su universidad, so pena de incurrir en pérdidas graves de la información o en daños a la misma por ataques informáticos, causados por inescrupulosos o por hackers que tienen un interés particular en alterar y dañar el bien preciado de la información institucional.

AUTOR: RUBY ESPERANZA BUITRAGO GIRALDO