UNIVERSIDAD POLITÉCNICA SALESIANA
Centros de Investigación
Perfil de Proyecto de Investigación Científica

21-feb-2018 4:17 PM

1. DATOS GENERALES DEL PROYECTO

Código:	CIDII-061113
Centro de Investigación:	CENTRO DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN EN INGENIERÍA
Programa:	Telemática aplicada a las redes de información
Título del Proyecto:	Estudio de las Seguridades Informáticas y de las TICs en el Campo de las Seguridades de la Información.
Grupo de Investigación:	Grupo de Investigación en Electrónica y Telemática
Area de Conocimiento:	Ciencia y Tecnología
Línea de Investigación:	Telemática
Tipo de Investigación:	Básica Aplicada
Campo :	Tecnologías
Investigador Principal :	JOSE RENATO CUMBAL SIMBA
Proyectos Vinculados :	
Duración del Proyecto :	12 Meses
Localización del Proyecto :	UPS Sede Quito Campus Sur
Fecha de ingreso :	02/10/2013 11:26

2. ANTECEDENTES

La creciente difusión de los sistemas informáticos y de las TICs en todo ámbito de la sociedad, va teniendo mucha trascendencia y un impacto bien marcado ya que un muchos de los casos ha causado revolución y se ha convertido en un factor relevante en el mundo moderno, hasta el punto que estos sistemas se han convertido en una necesidad importante y hasta obligatoria en toda organización social e individual. Sin embargo los sistemas que procesan la información son vulnerables a diferentes tipos de amenazas que pueden significar grandes pérdidas o perjuicios de distinta naturaleza, por lo tanto las Seguridades de la Información (SI) han crecido y evolucionado de igual manera. La investigación en el campo de las SI es un reto para las organizaciones, en ciertos lugares ha tenido mayor impacto y relevancia como se da en las culturas occidentales, el resto del mundo han pasado por alto y poco se ha hecho para examinar el cumplimiento de las SI, aunque la gente expresa su preocupación por la seguridad de su información, pocos toman acciones para protegerla, que incluso lo hacen a costos muy limitados.

3. JUSTIFICACIÓN

El presente trabajo pretende explicar de forma general la importancia de las Seguridades de la Información (SI) en el campo de las Tecnologías de la Información y Comunicación (TICs), especialmente se hace énfasis en ciertos temas puntuales como es el campo de la investigación, el académico entre otros, que cada vez se vuelven más relevantes el aplicarlos en las organizaciones, tomando en cuenta que las SI tiene un campo muy amplio y diverso, cada uno con su respectiva valoración e importancia. La investigación y la formación en SI juega un papel muy vital en toda organización ya que el preparar, defender y actuar ante los acontecimientos que surgen puede significar el proteger o administrar correctamente los activos en el entorno de la información, de igual forma el aplicar las políticas adecuadas, los roles de cada usuario y analizar los riesgos que llevan en este entorno puede conducir a tener sistemas más seguros. Hay casos de estudio de los cuales se puede rescatar experiencias, sugerencias y consejos que pueden servir en la administración de los sistemas de SI, es más se sugiere que se haga frecuentemente este tipo de práctica para tener mayor experiencia. Con lo dicho anteriormente se pretende entregar un informe de la situación actual de los sistemas con sus respectivas conclusiones y recomendaciones que a futuro servirán para seguir generando nuevos proyectos importantes en este campo.

4. OBJETIVOS

4.1 Objetivo General

Analizar, estudiar y probar las seguridades, técnicas de vulnerabilidades y protección de la información mediante el uso de material relevante y Sistemas Operativos orientado a las Seguridades Informáticas y de las TICs.

4.2 Objetivos Especificos

1. Analizar, estudiar los conceptos fundamentales de las Seguridades de la Información
2. Estudiar los Sistemas en Software y Hardware para Protección de Datos y Seguridades de estos
3. Pruebas y estudio de las Vulnerabilidades de los Sistemas Informáticos y de las TICs desde varios Sistemas Operativos (Windows, Mac y GNU/Linux)
4. Elaboración de un artículo sobre los resultados obtenidos de esta investigación

5. ESTADO DEL ARTE

La investigación y formación en seguridades de la información son amplias, muy diversas y tiene varios campos de acción para cumplir con el objetivo de proteger y mitigar las amenazas de los elementos que conforman el entorno de la información [1], uno de ellos podemos mencionar ya que en ciertos resultados se resaltan que las personas son la parte más débil en la defensa en lo que se refiere a las amenazas internas y externas que sufren las organizaciones, esto indica que las violaciones de seguridad son realizadas más frecuentemente por empleados internos de las organizaciones que por personas fuera de las mismas [1]. Existen varias investigaciones como la Teoría de Prevención General (GDT) que estudian el comportamiento humano y su relación con los delitos informáticos y el abuso intencional en los sistemas, de igual manera la Teoría de Motivación para la Protección (PMT)que trata de entender los comportamientos de los individuos cuando se trata de realizar una serie de medidas de seguridad, como por ejemplo el cumplimiento de políticas de seguridad, copias de seguridad de los datos, uso debido de elementos de seguridades de los sistemas, etc. [1].
En este campo se presentan una serie de oportunidades para explorar temas relacionados con las personas, tecnología y organización, entonces el reto para lograr aportes significativos en la investigación es cada vez más complejo y exige nos mantengamos al tanto con los cambios que se van produciendo y sus relaciones

con otras disciplinas [1]. Los problemas prácticos relacionados con las personas y la tecnología se unen, y es evidente establecer políticas y prácticas para que la tecnología sea accesible, usable y eficaz para la gente pueda hacer su trabajo, mientras es segura y fiable al mismo tiempo [2].

En la Ciberseguridad otro campo de las seguridades de la información existe un déficit de especialistas, contra las constantes amenazas informáticas y la necesidad de tener personas especializadas en esta área se está convirtiendo en una responsabilidad urgente en instituciones académicas con el fin de tener el personal adecuado que permita preservar la información de las organizaciones [3]. En estos tiempo los ataques cibernéticos van en aumento, varios gobiernos del mundo están tomando medidas proactivas y preventivas para reducir los riesgos de ataques exitosos en los sistemas. La seguridad Cibernética no es nueva y ha sido objeta de varias discusiones en el gobierno, la industria y el mundo académico desde casi dos décadas [3], por ejemplo la Organización Internacional de Normalización analiza el ISO/IEC 27032 que son directrices para la Ciberseguridad se define la Ciberseguridad como la conservación de la confidencialidad, integridad y autenticidad de la información en el ciberespacio y el ciberespacio está definido como el entorno complejo que resulta de la interacción de las personas, software y servicios de internet por medio de herramientas tecnológicas [3], dentro de este esquema la Ciberseguridad es un área de debate, interés e intención de la que surge la importancia de tener un plan de formación académica e investigación [3]. Las SI en su definición más básica significa proteger la información y su entorno con sus respectivo acceso, uso, divulgación, alteración, modificación o destrucción, con ello su objetivo es reducir al mínimo los riesgos relacionados con los tres objetivos principales como son la confidencialidad, integridad y autenticidad que se le conoce como (CIA) [4]. Además existen normas para las políticas de y se describen en las normas internacionales ISO/IEC 27002, ISO/TR 13569 e ISO/IEC 15408 [5].

6. METODOLOGÍA

La propuesta metodológica del presente estudio se basa en la elaboración de diversos métodos o estados de investigación de la siguiente manera:
Estado Descriptivo: en el cual se recopila información relevante del proyecto, así como cada una de sus definiciones formales, componentes, campos de acción y recomendaciones. La información será debidamente clasificada con los resultados de la misma y será tomada de fuentes reales y originales. A nivel de software se detallará los Sistemas Operativos a utilizar y sus respectivos componentes adicionales que se usaran para el desarrollo de las prácticas e investigación de la misma manera se realizarán a nivel de hardware.
Estado interactivo: se encontrarán soluciones a los problemas suscitados en el estado descriptivo ya que se espera tener algunas experiencias en el momento de interactuar con estos sistemas.
Por último se encuentra el análisis y la evaluación de los resultados, el mismo que servirá para poder concluir y recomendar este trabajo.

7. BIBLIOGRAFÍA

[1] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, ¿Future directions for behavioral information security research,¿ Computers & Security, vol. 32, no. 0, pp. 90 ¿ 101, 2013.
[2] D. C. Rowe and B. Lunt, ¿Mapping the cyber security terrain in a research context,¿ in Proceedings of the 1st Annual conference on Research in information technology, ser. RIIT ¿12. New York, NY, USA: ACM, 2012.
[3] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, ¿The role of cyber-security in information technology education,¿ in Proceedings of the 2011 conference on Information technology education, ser. SIGITE ¿11. New York, NY, USA: ACM, 2011
[4] L. Fuchs, G. Pernul, and R. Sandhu, ¿Roles in information security a survey and classification of the research area,¿ Computers & Security, vol. 30, no. 8, pp. 748 ¿ 769, 2011.
[5] D. Chernyavskiy and N. Miloslavskaya, ¿A concept of unification of network security policies,¿ in Proceedings of the Fifth International Conference on Security of Information and Networks, ser. SIN ¿12. New York, NY, USA: ACM, 2012.

8. RESULTADOS ESPERADOS

Informes sobre los datos relevantes en este estudio, así como conclusiones y recomendaciones para la implantación de mejores servicios de Seguridad de la Información dentro de la UPS y a futuro se siga con la creación de un Centro de Incidencias Informáticas SCIRT Académico y Certificado en el cual se haga investigación y formación en muchas áreas del campo de las Seguridades de la Información. Además el artículo científico para la publicación en revistas indexadas.

9. TRANSFERENCIA DE TECNOLOGÍA Y/O SOCIALIZACIÓN DE RESULTADOS DE INVESTIGACIÓN

Con la experiencia obtenida del proceso de investigación se va a estructurar cursos de capacitación y seminarios sobre diversos campos de las Seguridades de la Información, para los estudiantes de los niveles

superiores, egresados y graduados de la carrera de Ingeniería Electrónica e Ingeniería de Sistemas de la UPS, así como la representación nacional e internacional de la UPS en varios eventos orientados a esta temática como por ejemplo congresos, conferencias, tutorías y participaciones en General.
El estudio a desarrollar en gran parte surge de la necesidad de crear generar conocimiento mediante la investigación en esta área en la Carrera de Electrónica de la UPS, incluyendo y motivando a docentes y estudiantes en los diversos grados de formación a seguir en este campo del saber.

10. IMPACTOS DEL PROYECTO

-En la academia:
o Situación Actual de la Universidad con respecto a la temática,
o Tesis Generadas,
o Docentes o Estudiantes Vinculados a la Investigación,
o Seminarios, Congresos y Representatividad de la Universidad a nivel externo

11. INFORMACIÓN DE COFINANCIADORES (en caso de que existieran)