HETS Online Journal
Volume 5, Issue 1: October 2014

Análisis sobre los Riesgos de Seguridad Generados por Usuarios para las Tecnologías de Información y Comunicación (TIC)

Candal-Vicente , Isabel [1] y Osorio-Concepción, Dania I. [2]

[1, 2] Universidad del Este, Sistema Universitario Ana G. Méndez

Introducción

La información es un recurso valioso de las organizaciones, por lo tanto se debe garantizar y proteger la continuidad de los sistemas de información, minimizar los riesgos de daño y contribuir a una mejor gestión. El entorno de riesgo de la seguridad de la información es cambiante, debe ser revisada y evaluada continuamente. Se entiende por seguridad de información todas aquellas medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad (Maiwald & Sieglein, 2002). En el estudio titulado "Amenazas a la seguridad de la información computadorizada en las universidades de Puerto Rico" de Torres-Berrio (2012), indica que la tecnología de la información ha evolucionado mediante el uso de Internet facilitando el acceso ilimitado a la información de todo tipo pudiendo afectar de esta manera los sistemas de información. Este nuevo entorno tecnológico causa preocupaciones acerca de la erosión del acceso a determinada información y conocimiento. Según nos plantea Burgos (2008), las organizaciones deben estar preparadas para daños y posibles fallas a causa de la vulnerabilidad de los sistemas. Por tal razón, deben implementar políticas de seguridad, normas, procedimientos y estándares para mantener un nivel apropiado de seguridad de la información. Los autores

también aseguran que el estar preparados evita o previene las posibles amenazas en los sistemas. Las universidades se han vuelto dependientes de la facilidad de acceso a los datos que proporcionan las tecnologías de la información, simultáneamente también se han vuelto más vulnerables a las violaciones de la seguridad de que los sistemas de información tienen (Torres-Berrios, L., 2012).

El objetivo principal de este estudio de investigación es identificar las áreas de necesidad relacionadas con controles de riesgos de seguridad en las TIC asociadas con los usuarios administrativo y docente en una institución de educación superior. Además se pretende examinar si el personal administrativo y la facultad regular ha recibido adiestramiento de cómo controlar los riesgos de seguridad de la información en el área de trabajo y si están dispuestos a ser capacitados.

Planteamiento del Problema

Constantemente en el área de Informática y Telecomunicaciones se generan servicios de apoyo técnico y de consultas, mediante reclamaciones por parte de los usuarios. Éstos indican que tienen problemas de funcionamiento de sus equipos, tal como: la lentitud del sistema, interrupciones de servicio o posiblemente problemas de virus. A raíz de estos problemas cabe preguntarse ¿Cuáles son las actividades susceptibles relacionadas al personal de la Institución que provocan la entrada de virus y amenazas hacia la seguridad de la información?

Torres-Berrios, 2012, sostiene que a medida que se ha incorporado el uso de las computadoras y las redes en las instituciones, mayor es la facilidad de acceso a los datos a través de la tecnología. La posibilidad de interconectarse a través de las “redes”, ha traído un gran mejoramiento de productividad en las organizaciones, no obstante esto acarrea amenazas y

riesgos que pueden poner en juego la estabilidad y el futuro de organizaciones (Alvarado, 2011). Es fundamental establecer requisitos de seguridad mediante el desarrollo de un conjunto de principios y reglas que compendien cómo gestionar la protección de la información.

Justificación

El control de riesgo en las tecnologías de la información y comunicación es un aspecto que demanda la implantación de políticas de seguridad, procedimientos, estándares y procesos de capacitación, para disminuir el riesgo de ataques y mantener la seguridad de la información (Pérez & Palomo, 2007). Al no contar con controles de seguridad, son múltiples los riesgos y pueden llegar a ocasionar daños irreparables. El análisis de riesgos de sistemas de información es un método que se usa para identificar las vulnerabilidades de dichos sistemas. El análisis de riesgos corresponde a evaluar todos los potenciales riesgos en los cuales se pueda ver envuelta la organización por aspectos emanados en las TIC y que impacten en la seguridad de la información. Por lo tanto, el análisis de control de riesgo de los sistemas de información en las instituciones educativas, es un aspecto necesario para minimizar las fallas en los servicios que ofrecen y que pueden perjudicar procesos administrativos y de enseñanza (Burgos, 2008). La Organización Internacional de Normalización, conocida por sus siglas en inglés como ISO, *International Organization for Standardization*, es una norma estándar para el tratamiento de la seguridad de la información dentro del mundo de la informática. ISO 17799, se refiere exclusivamente a la información, su contenido y su seguridad, dentro del mundo informático. La información tiene que estar disponible, tiene que estar archivada en forma segura, se debe mantener su integridad, y debe ser confiable. Estos riesgos se los llama disponibilidad, integridad y confidencialidad. El

implementar las normas de seguridad recomendadas por ISO 17799 en la organización, requiere inversión en capacitación, manuales, hardware y el software.

Preguntas de investigación

El diseño metodológico de la investigación está encaminado a contestar las siguientes preguntas de investigación:

1. ¿Qué porcentaje del personal administrativo y facultad regular conoce las políticas de uso aceptable de Internet y el uso adecuado de los sistemas de correo electrónico establecidas por la institución educativa para la cual labora?
2. ¿Ha recibido adiestramiento el personal administrativo y la facultad regular de cómo controlar los riesgos de seguridad de la información en el área de trabajo?
3. ¿Está el personal administrativo y la facultad regular dispuestos a ser capacitados en el control de riesgos de seguridad de la información en su lugar de trabajo?

Definición de Términos

Los términos que se mencionan a continuación sirvieron de base para clarificar el uso y análisis de la investigación.

1. Activos. (Sena & Tenzer, 2004), definido como aquellos bienes y derechos relacionados con sistemas de información. Ejemplos típicos: datos, hardware, software, servicios, documentos, edificios y recursos humanos.
2. Clasificación del Riesgo. Según Manual de Implementación (2008), se logra a través de la probabilidad de su ocurrencia y el impacto que pueda causar la materialización

del riesgo. El número de veces que el riesgo se ha presentado en un determinado tiempo y la magnitud de sus efectos.

3. COBIT. (Hardy & Heschl, 2008), guía que brinda las mejores prácticas y herramientas aprobadas internacionalmente para el monitoreo y la gestión de las actividades de Tecnología de Información TI. Permite el desarrollo de políticas y mejores prácticas para la administración de TI.
4. Controles. Según Rodríguez (2008), son acciones y mecanismo definidos para prevenir o reducir el impacto de los eventos no deseados que ponen en riesgo la adecuada ejecución de los procesos, las políticas con el fin de definir las acciones conducentes a reducir los riesgos.
5. Evaluación de Riesgo. Según Archiary (2005), se entiende por evaluación de riesgo a la evaluación de las amenazas y relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
6. ISO 17.799. Según Andrade (2009), protección y control de la información manejada sistemáticamente con el uso de medios informáticos.
7. Riesgo. Según Matalobos (2009), estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
8. ITIL. Según (Burgos & Campos, 1980), es una norma de mejores prácticas para la administración de servicios de (TI).

Revisión de Literatura

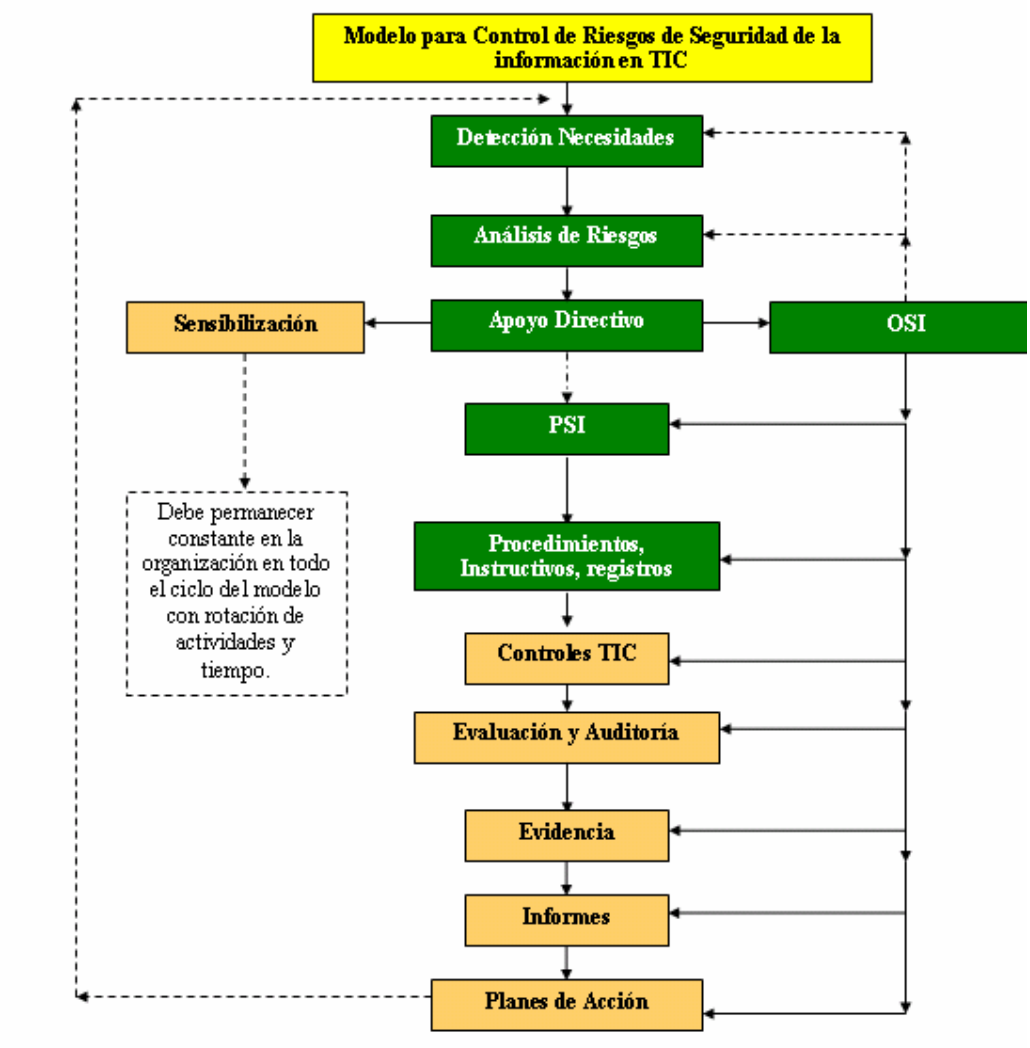
En el estudio realizado por (Computer Security Institute, 2010 citado en Torres, 2012), indica que en la actualidad existen múltiples amenazas a la seguridad de la información, siendo la causa de estas los software maliciosos o *malware*. Las áreas de trabajo de las instituciones educativas en Puerto Rico no son la excepción. Según señala (Granada, 2009), las amenazas y las vulnerabilidades tienen interrelación. Las amenazas a la seguridad de la información y a los sistemas utilizados se incrementan cada día, por lo cual, es necesario ser cautelosos en tomar todas las medidas necesarias para lograr que dichos riesgos sean minimizados en las áreas de trabajo (Calder & Watkins, 2008).

Un estudio realizado por (Pérez & Palomo, 2007) sostienen que la falta de controles de seguridad, y la creación de políticas de seguridad, en las organizaciones pueden verse afectadas por amenazas y ser vulnerables en tener fallas en *hardware*, sistemas operativos, aplicaciones, pérdidas de datos, la infraestructura, lo que pueden repercutir en pérdidas económicas irreparables. Según el estudio realizado "Soluciones administrativas y técnicas para proteger los recursos computacionales de personal interno" (Pérez & Palomo, 2007), reflejó que la mayor causa de amenazas son generadas por personal interno con un 70% y el 30% por el personal externo. La realidad es que existen amenazas tanto dentro como fuera de la organización. La tecnología móvil, computación en nube, las redes sociales y el sabotaje por parte de los empleados son solo algunas de las amenazas internas que enfrentan las empresas.

Al revisar los antecedentes o la literatura, se encontró que el modelo más influyente en investigaciones anteriores sobre factores de éxito de SI es el modelo de Burgos & Campos. Como marco conceptual se utilizó la revisión de literatura y el modelo "Control de riesgo de seguridad

de la información en TIC" (Burgos, 2008) y la revisión de la literatura. Este modelo se fundamenta en los lineamientos entregados por las normas y estándares internacionales del área, de tal manera que sus bases aplican para que cualquier tipo de organización pueda realizar el uso seguro de sus TIC facilitando un nivel adecuado de control de riesgos en las Tecnologías de Información y Comunicación (TIC) con el fin de evitar o disminuir las fallas en los sistemas. Como parte del modelo, se implementa una estructura organizacional basada en estándares, ISO 17.799.

Figura 1. Modelo para Control de Riesgos de Seguridad de la Información en TIC según (Burgos, 2008).



A continuación se describe cada una de las fases del modelo para el mejor entendimiento:

- Detención de Necesidades: Corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con su seguridad de la información (Burgos, 2008).
- Análisis de Riesgo: Corresponde a evaluar todos los potenciales de riesgos en los cuales se pueda ver envuelta la organización por aspectos emanados de las TIC y que impacten en la seguridad de la información (Burgos, 2008).
- Apoyo Directivo: Corresponde a la presentación del resultado de las etapas anteriores con el fin de conseguir el apoyo para concretar la implementación de la seguridad de la información (presupuestos, personal, capacitación) (Burgos, 2008).
- OSI. La organización debe designar a un OSI para que realice, apoye, dirija, pueda llevar el control de implementación y posterior seguimiento a todo el modelo de seguridad de la información. Además el OSI estará presente en todas las actividades haciendo énfasis en la fase de aplicación en la cual participa de forma activa en todas las actividades que se indican de aquí en adelante (Burgos, 2008).
- Confección PSI. Corresponde al diseño de las Políticas de Seguridad de la Información de la organización (Burgos, 2008).
- Confección de procedimientos, instructivos y registros. Corresponde al desarrollo de documentos que formalicen como se deben realizar las actividades y qué información es la que se debe retener como evidencia para dar conformidad a las PSI (Burgos, 2008).

- Controles TIC. Se diseñan y define los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisiones o auditorias del modelo (Burgos, 2008).
- Evaluación y auditoría: Se debe realizar, preparar y desarrollar la revisión que avale todos los procesos de TI que se están cumpliendo y llevando a cabo adecuadamente, lo cual será evaluado por el mismo proceso de auditoría interna o externa (Burgos, 2008).
- Evidencia: Se busca verificar de manera adecuada que todos los registros de TI para todos sus procesos y controles estén disponible para cualquier tipo de revisión, particularmente para los procesos de auditoría (Burgos, 2008).
- Informes: Se contempla la confección de informes del proceso de revisión que derivarán en actividades de mejoras al modelo y con revisiones por parte de la dirección de la organización que permitan confeccionar planes de acción adecuados (Burgos, 2008).
- Planes de Acción: Consiste en la aplicación de los planes de acción conforme a los plazos y actividades que fueron indicados en el proceso de auditoría. Estos planes de acción pueden conformar la revisión y ajustes de todo tipo de actividades, ya sea a nivel de procesos de seguridad, de evidencias, políticas o de cualquier otra actividad que sea identificada (Burgos, 2008).
- Sensibilización: Esta etapa (incluida en ambas fases del modelo) permite entregar constante información (alertas) a la organización sobre la importancia de mantener la seguridad de la información y el resguardo de todas las actividades de TI. Recibe apoyo directivo de la dirección de la organización (Burgos, 2008).

Para garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo a una mejor gestión, es recomendable contar con un plan de continuidad. Un plan de continuidad que identifique las amenazas que puedan ocasionar interrupciones en los procesos, evaluar los riesgos, identificar los controles preventivos, protección de datos y privacidad de la información personal. Periódicamente se deben actualizar las políticas, normas, procedimientos y controles de riesgo de los sistemas de información en TIC con el fin de poder identificar los síntomas del problema, establecer las medidas inmediatas ante la presencia de una anomalía.

Seguridad de la Información

La información tiene que ser protegida según el estándar conceptual de Gestión de Seguridad de la Información internacionalmente reconocida y publicado por la Organización Internacional de Normalización o ISO. El propósito de la confidencialidad es asegurar que la información esté accesible sólo para el personal autorizado. La integridad establece la exactitud de la información y los métodos del procesamiento. La disponibilidad tiene como finalidad que la información pueda ser utilizada cuando sea necesaria (ISO/IEC 17799, 2005). Estos tres conceptos son igualmente aplicables a usuarios de empresas y a usuarios domésticos. Alvarado (2011) señaló que el implementar los procesos, procedimientos, políticas de seguridad y controles ayudarán a estudiar los posibles riesgos y a mejorar los incidentes y amenazas que se detecten en la seguridad de la Información en TIC.

Medidas de Prevención

Dentro de las medidas de prevención recomendadas por los autores (Rodríguez, 2008) y (Ramírez, 2009) está el control de acceso al equipo, utilizar un sistema de protección como lo son los antivirus, tener privacidad de la información, realizar resguardo de información o *backup*, evitar la trasferencia de archivos por dispositivos como los USB (Universal Serial Bus) y en caso de utilizarlo hacerle un análisis con el antivirus. Otras medidas lo son; evitar abrir correo electrónicos de los cuales el remitente sea desconocido y no descargar programas de sitios no oficiales. Lo más importante es capacitar al personal en el uso correcto de los equipos.

Vulnerabilidades

Alvarado (2011) indica que las vulnerabilidades están asociadas a debilidades de los activos de información. La vulnerabilidad en los sistemas de información es considerada como la ausencia o debilidad en los controles que ayudan a disminuir o evitar un riesgo. De acuerdo con (De Freitas, 2009), los activos de información deben ser trazados para identificar su impacto en la organización y realizar un análisis para determinar que activos están bajo riesgo. Las organizaciones se pueden ver afectadas por amenazas y ser vulnerables a tener fallas en los sistemas de las TIC (Pérez & Palomo, 2007).

Implementar y Estructurar controles

Según Yory (2006), a continuación se mencionan algunos controles que se consideran esenciales para una organización, éstos suponen práctica recomendada de uso frecuente en la implementación de la seguridad de la información:

- Protección de datos y confidencialidad de la información personal

- Protección de registros y documentos de la organización
- Documentación de políticas de seguridad de la información
- Asignación de responsabilidades en materia de seguridad de la información

Los autores (Estévez, Fanny & Nuñez, 2012), indican que existen estándares internacionales facilitando y garantizando el cumplimiento de la seguridad de la información. Algunos de los estándares más conocidos son: ISO 17.799, COBIT, ITIL, Ley SOX, ISO 2700; Estos facilitan el análisis y evaluaciones de las vulnerabilidades, identifican las posibles amenazas y ataques en la red.

Provoste (2006) sostiene que existen diversas propuestas de estándares TIC para la formación docente en el mundo. La incorporación de estos estándares son un medio para implementar, mejorar y orientar la evaluación sobre la calidad de lo que hace en la educación, especialmente relacionado en el mejoramiento de sus profesionales.

Metodología

Para la recopilación de los datos se utilizó como instrumento un cuestionario. La validez del cuestionario se midió a través del consenso de expertos constituido por cuatro especialistas de TI, quienes evaluaron el documento de manera independiente. Una vez concluida la revisión del instrumento por el panel de expertos, se añadieron, se eliminaron y se hicieron diversas modificaciones en los ítems. El instrumento de medición constó de 14 preguntas cerradas y 4 preguntas que utilizan escala *Likert* de 5 puntos para medir la posición de los participantes con respecto a las afirmaciones elaboradas en el cuestionario. Se consideraron las alternativas: *muy de acuerdo, de acuerdo, indeciso, en desacuerdo* y *muy en desacuerdo*. La población del estudio

fueron los empleados administrativos y el personal docente de las escuelas de la Institución. La muestra, no probabilística de conveniencia, se obtuvo de los participantes voluntarios que aceptaron completar y entregar el instrumento. La encuesta se administró a un total de 175 personas de una institución de educación superior del área este de Puerto Rico en Puerto Rico. El número total de cuestionarios contestados y recibidos fue 153. La tasa de respuesta global fue de 87%. Los datos fueron ingresados, tabulados y procesados utilizando el programa de computadora "IBM SPSS Statistics".

El diseño de la investigación es cuantitativo no experimental, transeccional descriptivo. La investigación transeccional o transversal recolecta datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado. Es decir, se trata de una investigación donde no se hace variar en forma intencional las variables independientes. La investigación no experimental observa fenómenos tal y como se dan en su contexto natural, para después analizarlos. Hernández Sampieri et al. (2010, 140): "En la investigación no experimental no es posible manipular las variables o asignar aleatoriamente a los participantes" Kerlinger y Lee (2002, 420). Los sujetos se observan en su ambiente natural.

Se recogió evidencia de la confiabilidad de la prueba para la muestra del personal administrativo y docente de la Institución mediante el cálculo del coeficiente alfa de Cronbach ($\propto$).

Tabla 1 Análisis de confiabilidad de la prueba

Muestra	Cronbach's Alpha	N
Personal Administrativo y Docente I parte cuestionario	.726	153
Personal administrativo y Docente II parte del cuestionario	.857	153

Nota: N es el número de cuestionarios para cada una de las muestras

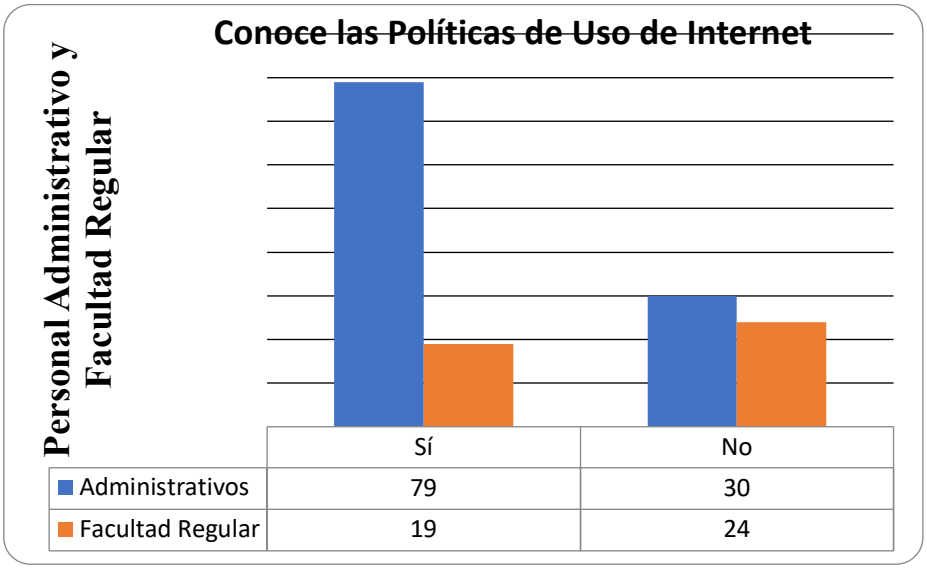
El cálculo del coeficiente alfa para la primera y segunda parte del instrumento fue de .726 y .857 respectivamente. Nunnally (1978), sugiere que los niveles del coeficiente alfa mayores de 0.7 son considerados altos. El resultado abona como evidencia a la confiabilidad del cuestionario.

Esto implica que existe asociación entre los ítems del instrumento con relación a los constructos que lo constituyen (consistencia interna) Crocker y Algina (2006, 135).

Análisis de datos

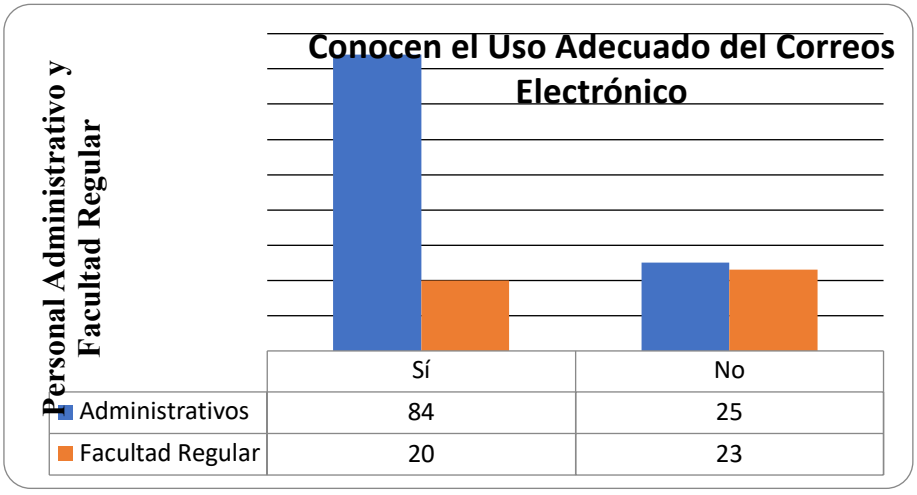
La gráfica 1 presenta que el 64% del personal administrativo y facultad regular conoce las políticas de uso aceptable de Internet. Un total de 98 participantes indicaron conocer las políticas de uso de Internet, 79 personas del personal administrativo y 19 personas de la facultad regular.

Gráfica 1 Conoce las Políticas que Regulan los Servicios de Internet



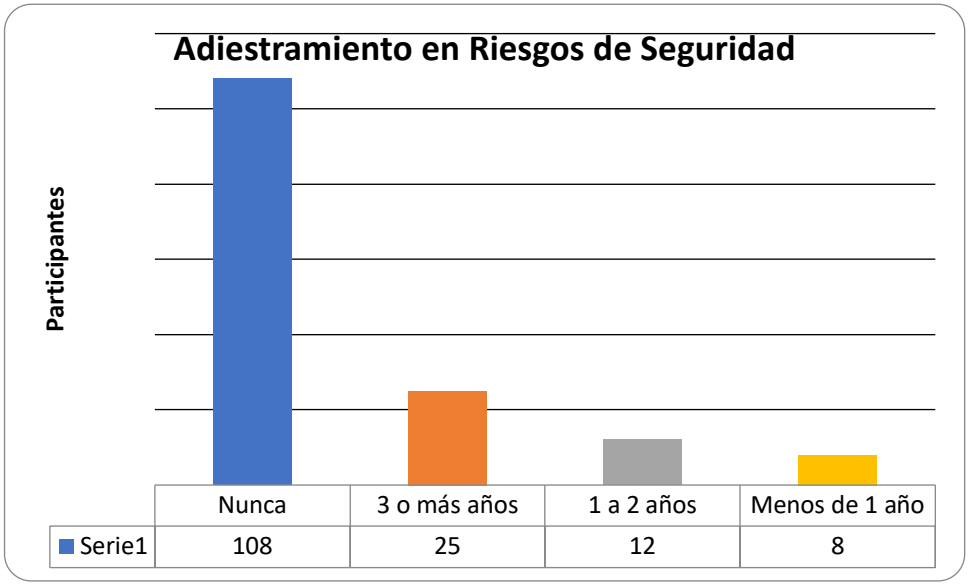
La gráfica 2 demuestra que el 64% de los participantes indicaron tener conocimiento sobre las políticas de uso adecuado de los sistemas de correos electrónicos, el 36% de los participantes dijeron no tener conocimiento. Un total de 98 empleados indicaron conocer las políticas de uso de Internet, 79 personas del personal administrativo y 19 personas de la facultad regular.

Gráfica 2 Conoce el uso Adecuado de los Sistemas de Correo Electrónico



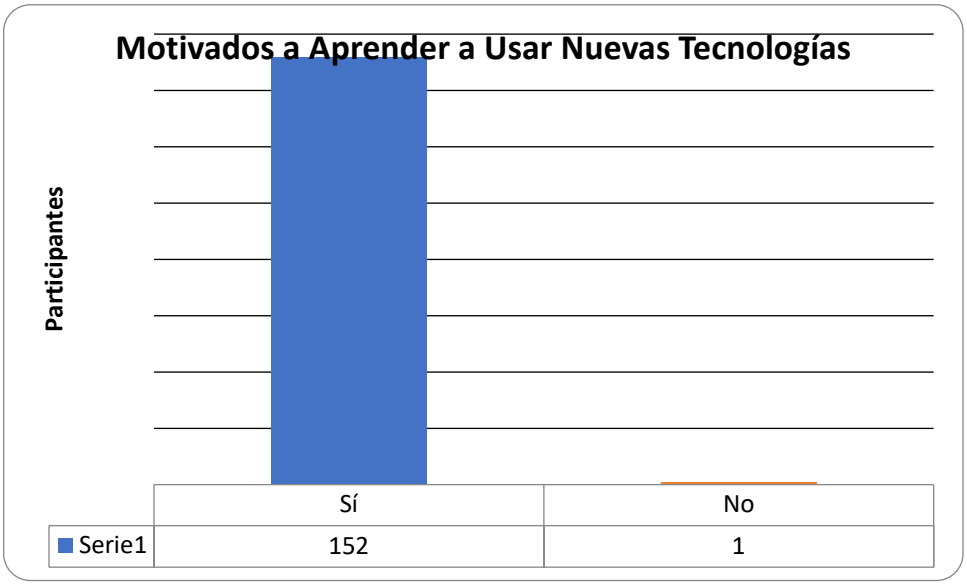
También se les preguntó en el cuestionario si la política que regula los servicios de correo electrónico e Internet por la Institución está accesible a los asociados, 104 de los participantes, o sea, el 68% contestó tener acceso a las políticas de correo electrónico mientras que el 32% de los participantes respondieron no conocer el uso adecuado de los servicios de correo electrónico e Internet.

Gráfica 3 Adiestramiento para controlar los riesgos de seguridad de la información en su área de trabajo



En la gráfica 3 podemos observar que 108 (71 %) de los participantes dijeron nunca haber recibido adiestramiento en riesgos de seguridad versus 45 participantes que revelaron haber recibido adiestramientos en riesgos de seguridad.

Gráfica 4 Motivación para Aprender a Usar de Nuevas Tecnologías



La gráfica 4 muestra que el 99% de los encuestados está motivados

Conclusiones

Es importante notar que a pesar que la Institución tiene políticas establecidas sobre los servicios de Internet y el uso adecuado de los correos electrónicos, un 35% de los encuestados contestó no tener conocimiento de las mismas. Como resultado, el modelo de Control de riesgo de Seguridad de la Información en TIC demostró que existen unas vulnerabilidades internas. Según la revisión de literatura, las vulnerabilidades internas son un factor de riesgo que aumenta el peligro de la propagación de *software* malicioso.

La premisa anterior nos lleva a concluir que la Institución carece de controles eficientes en cuanto a la Seguridad de la Información y manejo de riesgo a lo que está expuesto.

Los encuestados manifestaron estar motivados a aprender sobre el uso de las nuevas tecnologías y desean ser adiestrados para prevenir el impacto de los *malware*.

El estudio demostró que la Institución no tiene un plan de capacitación y publicación de políticas en el uso y manejo adecuado de los sistemas de información.

Recomendaciones

Publicar periódicamente las Políticas del Uso Adecuado del Internet y Correo Electrónico.

Realizar una encuesta sobre el Control de Riesgos Informáticos, para un estudio futuro, donde se incluya la participación de la facultad conferenciante y estudiantes.

Considerar la aplicación de normas, procedimientos y estándares bajo un esquema generalizado y adaptable a la Institución, según el modelo para Seguridad de la Información en TIC (Burgos, 2008).

Limitaciones

La limitación mayor de esta investigación es el periodo de tiempo establecido para hacer el estudio. El tamaño de la muestra fue una por conveniencia y estuvo delimitada al personal administrativo y facultad regular. No se incluyó al estudiantado ni a la facultad conferenciante de una institución educativa, en el área este de Puerto Rico, por lo tanto, sus resultados no pueden ser generalizados.

Referencias

Alvarado, L. (2011). Diseño de un Plan de Gestión de Seguridad de la Información. *Alcaldía del Municipio Jiménez del Estado Lara*, 4-26.

Burgos, J. (2008). “Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC)”, Informe de Proyecto de Título, Ing. (E) Computación e Informática, Universidad del Bío-Bío, Concepción, Chile.

Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002.* Philadelphia: Kogan Page.

Crocker, L & Algina, J. (2006): *Introduction to Classical and Modern Theory*, Thompson/Learning Wadsworth, USA.

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Revista Venezolana de Información, Tegnología y Conocimiento*, 43-55.

Estévez, F., Fanny, P., & Núñez, J. (2012). Diseño de un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A en la cuidad de Quiro, aplicado las normas ISO 27001 e ISO 27002.

Granada, C. (2009). *Gestión de Seguridad de la Información en el sector bancario. Especialización en Gerencia de Sistemas y Tecnología*. Colombia.

Hernández Sampieri, R., Fernández Collado, C. & Baptista Lucio, P. (2010): *Fundamentos de metodología de la investigación*, Mc Graw-Hill/Interamericana de España, S.A.U.

ISO/IEC 17799. (2005). Information technology -- Security techniques -- Code of practice for information security management. Recuperado el 3 de marzo de 2014, http://www.iso.org/iso/catalogue_detail?csnumber=39612

Kerlinger, F.N. y Lee, H.B. (2002), *Investigación sobre el comportamiento: Métodos de investigación en ciencias sociales*, México: McGraw-Hill Interamericana Editores.

Maiwald, E., & Sieglein, W. (2002). *Security Planning and Disaster Recovery.* New York: McGraw-Hill Osborne Media.

Nunnally, J.C. (1987).*Teoría Psicométrica.* MC Graw-Hill, Inc. Mexico.

Pérez, M., & Palomo, A. (2007). Soluciones administrativas y técnicas para proteger los recursos computacionales de personal interno-*insiders*.

Provoste, Y. (2006). Estándares en tecnología de la Información y la Comunicación para la Formación Inicial Docente. *Gobierno de Chile Ministerio de Educación.*

Ramírez, A. (2009). El MALWARE en las organizaciones. *Sistemas Telemáticos y las Organizaciones Inteligentes en la Sociedad del Conocimiento*, 3-100.

Rodríguez, E. (2008). Guía General para el Diseño, Desarrollo e Implementación de cada uno de los Subsistemas, Componentes y Elementos de Modelo Estándar de Control Interno.

Manual de Implementación, 72. Obtenido de http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=579

Torres-Berrios, L. (2012). *Amenazas a la seguridad de la información computadorizada en las universidades en Puerto Rico desde la perspectiva de los profesionales del área de sistemas de información. Universidad del Turabo (Puerto Rico).* Obtenido de ProQuest Dissertations and Theses, 260. espanol: ttp://search.proquest.com/docview/1018558484?accountid=130249.(1018558484).

Yory, J. (2006). Un acercamiento a las mejores prácticas de seguridad de información internacionalmente reconocidas en el estándar ISO 17799:2005. Bogotá, Colombia.