Políticas de seguridad de la información en la Universidad Tecnológica Intercontinental

Marandu ñemoañete Universidad Tecnológica Intercontinental-pe

Security Policy for Information at the Intercontinental Technological University

Cristian David Macen Rojas

Universidad Tecnológica Intercontinental
Facultad de Tecnología Informática
davidmacenrojas@gmail.com

Resumen

La información institucional es un activo que, como otros activos de la institución, es esencial que sea protegido adecuadamente. Esta investigación nace de la necesidad de elaborar políticas de seguridad de la información para el Departamento de Tecnología Informática de la Universidad Tecnológica Intercontinental (UTIC). Por ello, se propone describir la realidad que ésta presenta para la construcción de una política de seguridad de la información. Se contempló como núcleo investigativo a los funcionarios de la Sedes de la Regional Central, con lo que la población quedó conformada por 84 (ochenta y cuatro) funcionarios que manejan sistemas de informaciones y 10 (diez) funcionarios del Departamento de Tecnología Informática. Esta investigación es de un enfoque cuantitativo, de nivel descriptivo, el diseño es no experimental. El resultado demostró una proporción global con respecto al manejo de la información de manera insegura 55,95 % y una proporción del manejo seguro de 44,05 %. Como recomendación se presenta el manual de políticas de seguridad de la información para su implementación.

Palabras clave: Política, Seguridad, Información, Sistema.

Mombypykyre

Marandu ningo hína mba'erepy, ambue mba'erepýicha avei oikotevêva oñemo'ã hekópe porã. Ko tembikuaareka heñói ojehecha rupi tekotevêha oñembosako'i política ikatu hagüáicha isegúro marandu oguerekóva UTIC Departamento de Tecnología Informática. Upéicha rupi ohesa'ŷjo mba'éichapa oĩhína UTIC oguerojera hagua política marandu isegúrova. Oñemboguata hagua, oñemba'apo mba'apohára Regional Central Sede peguakuéra ndive; oike ipype 84 (poapypa rundy) mba'apohára oguerekóva ipoguýpe marandu rape ko mbo'ehaovusu pegua ha 10 (pa) mba'apohára Departamento de Tecnología Informática pegua. Ko tembiapo jeporekarã hína cualitativo, ijyvatekuépe descriptivo, ha avei no experimental. Oñemohu'ã rire ojejuhu tuichaháicha 55,95 % marandu ndoku'eiha hape tee rupi ha 44,5 % katu osyryryha hekópe. Mba'ejeruréramo oñemoğuahê kuatiápe mba'éichapa oñemboguatava'erã marandu isegúro hagua ha avei ojejerure toñemboguata umi tembiaporã.

Mba'e mba'e rehepa oñe'ẽ: Política, Seguridad, Marandu, Sistema.

Abstract

Information is an asset which, like other assets of the institution, needs to be adequately protected. This research stems from the need to develop policies of information security for the Department of Information Technology UTIC. It is therefore proposed to describe the reality presented by UTIC for building a policy of security for information. It was thought that the investigative officials of the Central Regional Headquarters compose the core, the population of which was composed of 84 (eighty four) officers which manage information systems and ten (10) members of the Department of Information Technology. This research is of a quantitative approach, on a descriptive level, and whose design is not experimental. The result showed an overall ratio with respect of insecure information management of 55.95 % to safe handling of 44.05 %. As a recommendation, the manual of security policies for information security implementation is presented.

Keywords: Policy, Security, Information, System.

Políticas de seguridad de la información en la Universidad Tecnológica Intercontinental

En cuanto a las políticas de seguridad de la información, la ausencia de la misma puede ocasionar daños a las organizaciones, este concepto formulado originalmente por la Academia Latinoamericana de Seguridad Informática (2009) que se presenta a continuación:

> En la actualidad la ausencia de políticas de seguridad en las organizaciones, puede ocasionar efectos catastróficos. Escenarios como el ocurrido a la Empresa eBay, en diciembre del 2002, son un claro ejemplo de situaciones en las que se muestra la enorme necesidad de contar con estas políticas y mantenerlas al día.
>
> La empresa eBay se dio cuenta que intrusos enviaron fraudulentamente correos a sus 55 millones de usuarios para solicitarles que confirmaran sus datos a través de un portal o sitio de eBay, igualmente falso, para una "comprobación técnica" por ese motivo, pocos clientes de eBay sospecharon que se trataba de un fraude (p. 10).

La nota señala textualmente: "Estas solicitudes a menudo contienen enlaces a páginas Web en las que se les pedirá que dé su información personal... los empleados de eBay nunca le pedirán su contraseña" (p. 10).

Ante esa situación, toda organización necesita contar con política de seguridad de la información. Para la creación de la misma se tiene un previo requisito como señala ARETIO:

> Antes de abordar el proceso de desarrollo de una política de seguridad de la información conviene recordar algunas cuestiones claves como el hecho de comprender que la política de seguridad trata las amenazas a la seguridad de la información y especifica los procedimientos a adoptar en una organización en relación para prevenir la ocurrencia de una amenaza y la reacción frente a la amenaza producida. La

política de seguridad también especifica las reglas generales relacionadas con la utilización de medios electrónicos.

Asimismo, se deben conocer los motivos para implantar una política de seguridad de la información, ya que forma la base de todo programa o plan director de seguridad, así como la importancia del desarrollo de una política robusta y efectiva. Además, las TIC (tecnologías de la información y las comunicaciones) están en constante evolución y traen consigo nuevas y cambiantes amenazas que deben tenerse en cuenta.

Para desarrollar una política de seguridad, se deben seguir cinco fases interrelacionadas:

1. Análisis de riesgos
2. Construcción de la política
3. Implantación de política
4. Mantenimiento de la política
5. Implicación de todo el componente humano. (2008, p. 43).

En cuanto a la Universidad Tecnológica Intercontinental, previa entrevista con el Director de Tecnología Informática, se detectó la ausencia de políticas de seguridad de la información en la misma. En efecto, esta urgencia de creación lleva a esta investigación al desarrollo de las dos primeras fases mencionadas por el autor, que consistirá en el objeto de la presente investigación.

Toda construcción de política supone previamente un diagnóstico sobre:

- Análisis de riesgo de la seguridad de la información, que según AREITIO (2008) “constituye una parte clave consistente en identificar los peligros que afectan a la seguridad, determina su magnitud e identifica las aéreas que necesitan salvaguardas” (p. 54).

- Equipo multidisciplinario, que de acuerdo a la Academia Latinoamericana de Seguridad informática “permite que represente gran parte de los aspectos culturales y técnicos de la organización y que se reúnan periódicamente dentro de un cronograma establecido por el Comité de Seguridad” (p. 8).

- Proceso de elaboración de documento de política de seguridad de la información, "siendo que el objetivo las políticas de seguridad de la información según ISO/IEC 17799 es la de proporcionar a la gerencia la dirección y soporte para la seguridad de la información" (p.10).

- **Comparación de manuales de seguridad de la información en sus elementos comunes**, según la Academia Latinoamericana de Seguridad informática "en esta etapa se identifican y analizan los documentos existentes sobre seguridad de la información y los que tienen alguna relación con el proceso de seguridad, en lo referente a la reducción de riesgos, disminución de trabajo repetido y falta de orientación. Entre la documentación existente, se pueden considerar: libros de rutinas, metodologías, políticas de calidad y otras" (p. 10). La misma permitirá la elaboración de un manual de seguridad de la información, para el Departamento de Informática de la Universidad Tecnológica Intercontinental.

En este sentido nace la siguiente interrogante: ¿Qué realidad presenta la UTIC para la construcción de política de seguridad de la información?, que se desglosa en las siguientes preguntas específicas. ¿Cuál es el riesgo de seguridad de la información que presenta la UTIC para la construcción de la política de seguridad de la información? ¿Cuáles son los aspectos culturales en el manejo de la información en la UTIC? ¿Cuáles son los aspectos técnicos en el manejo de la información en la UTIC? ¿Qué buenas prácticas de seguridad de la información de políticas de seguridad de otras universidades pueden ser emuladas en la UTIC? ¿Cuál es el manual de políticas de seguridad de la información para la UTIC, conforme a los datos obtenidos de la realidad de la misma?

Esta investigación presenta un diagnostico técnico completo de la UTIC previa a la elaboración de una **política de seguridad de la información** y permitirá la elaboración de un manual ajustado a la realidad de la UTIC que sirva para la seguridad de las informaciones.

Además del diagnóstico previo en sus diferentes aspectos técnicos de la seguridad de la información, también se compara diferentes modelos de políticas de seguridad de la información de

otras universidades, para su emulación como buenas prácticas en políticas de seguridad de la información.

La **política de seguridad de la información** será la guía a seguir por la UTIC para asegurar su información valiosa. Para la revista digital protege su información “en primer lugar, no podemos perder de vista la actividad de nuestra organización y lo que este nos exige día a día, por lo tanto, conviene establecer una **política de seguridad de la información** concisa y clara, sin rodeos ni "obligaciones" que posteriormente, por las características de nuestra organización, no podamos cumplir” (p. 5).

De acuerdo a Hugo Cerda, citado por Bernal (2006), “es imposible concebir una investigación científica sin la presencia de un marco teórico, porque a este le corresponde la función de orientar y crear las bases teóricas de la investigación” (p. 125).

Análisis de riesgo de la seguridad de la información

Para entender en qué consiste el análisis de riesgo es importante comprender el valor estratégico de la información que según Herrera (2003): “Cualquier actividad diaria requiere de información para su realización. La humanidad no se concibe sin información. Esta produce y maneja para propiciar el desarrollo de la actividad económica, política y social del mundo. Así, la generación y el intercambio de información es una necesidad primordial del quehacer humano (p.17)”.

Gutiérrez (2003) menciona:

> Que es conocido que vivimos en la era de la información, muchas organizaciones gestionan informaciones a gran volumen, para ellas es un activo valioso como tal valor la información debe ser custodiada con el máximo cuidado porque, sin lugar a duda, será buscada por otros. En otras palabras, al ser las diferentes informaciones elementos valiosos que son apetecidos por terceros, decidimos que la información está sometida a amenazas (p. 4).

En base a los conceptos resaltados sobre la importancia de la información cabe destacar el concepto de seguridad de la información que según la ISO/IEC 17799 (2005):

> La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio (p. 8).

Desde el punto de vista de Gutiérrez (2003):

> El objetivo de la seguridad es de proteger los recursos (personal, información, material, instalaciones) y las actividades. Según sea el recurso a proteger, se utilizan los términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones, o seguridad de operaciones, Cuando se trata de proteger el recurso información, hay que tener en cuenta que la información puede existir en la mente humana, en un documento, o en forma electrónica en un sistema de información y comunicaciones, y por tanto, hay que abordad el problema de la seguridad de la información bajo estos tres aspectos (p. 12).

Comité de seguridad de la información: un equipo multidisciplinario

Es importante conformar el comité de seguridad de la información que según la empresa colombiana SISTESEG (2011):

> La creación de un comité de seguridad de la información es primordial en la elaboración de las políticas de seguridad de la

> información que se encarga de tratar los temas concernientes a la seguridad de la información de la organización, donde se deberá de asignar responsables, tareas, actividades y tomar decisiones en cuanto a seguridad se refiera respaldado por la Alta Gerencia (p. 2).

Para el Ministerio de Ciencia e Innovación de España (2010) "este comité se encargará de coordinar y centralizar todos los esfuerzos sobre la gestión tecnológica en materia de seguridad de la información" (p. 5).

De acuerdo a la Academia Latinoamericana de Seguridad informática (2012):

> Para integrar el comité de seguridad de la información es importante formar un equipo multidisciplinario que represente gran parte de los aspectos culturales (la forma singular que tiene la organización para realizar sus actividades) y técnicos (en cuanto a tecnología) de la organización y que se reúnan periódicamente dentro de un cronograma establecido por el Comité de Seguridad. Este comité es formado por un grupo definido de personas responsables por actividades referentes a la creación y aprobación de nuevas normas de seguridad en la organización. En las reuniones se definen los criterios de seguridad adoptados en cada área y el esfuerzo común necesario para que la seguridad alcance un nivel más elevado. Se debe tener en mente que los equipos involucrados necesitan tiempo libre para analizar y escribir todas las normas discutidas durante las reuniones (p. 8).

Políticas de seguridad de la información

Las políticas de seguridad de la información son un conjunto de documentos de alto nivel (nivel estratégico) donde se definen las directrices a seguir por una organización en un aspecto en concreto para garantizar la confidencialidad, integridad y disponibilidad de la información.

> Es decir, estos documentos deben ser elaborados, revisados y mantenidos por el consejo directivo (preferiblemente) o la

> máxima autoridad de la organización, depende de cómo funcione la misma; la cuestión es que las políticas de seguridad de la información son una decisión y gestión estratégica, no táctica y mucho menos operativa. La intención de ellas es generar y/o confirmar el compromiso de la alta gerencia (de allí la importancia de la participación del consejo directivo) en materia de seguridad de la información (Solís, 2014).

Navarro (2003) considera que las políticas son directrices u orientaciones sobre una determinada materia en un entorno concreto. Se trata de fijar objetivos, sin decir cómo conseguirlos y viene a representar el marco o filosofía de actuación de la entidad. No deben ser largas ni farragosas, una o dos páginas por política, a lo sumo. Tienen que ser fáciles de entender por todo el personal de la empresa (p. 57).

Elaboración de la política de seguridad

El artículo publicado por la Academia Latinoamericana de Seguridad Informática (2013) menciona que la política es elaborada considerando el entorno en que se está trabajando como la tecnología de la seguridad de la información, para que los criterios establecidos estén de acuerdo con las prácticas internas más recomendadas de la organización, con las prácticas de seguridad actualmente adoptadas, para buscar una conformidad mayor con criterios actualizados y reconocidos en todo el mundo.

La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación y compromiso. Es importante considerar que para la elaboración de una política de seguridad institucional se debe Integrar el Comité de Seguridad responsable de definir la política, conformado por un equipo multidisciplinario que represente gran parte de los aspectos culturales y técnicos de la organización, y que se reúnan periódicamente dentro de un cronograma establecido por el Comité de Seguridad. Este comité es formado por un grupo definido de personas responsables de las actividades referentes a la creación y aprobación de nuevas normas de seguridad en la organización. En las reuniones se definen los criterios

de seguridad adoptados en cada área y el esfuerzo común necesario para que la seguridad alcance un nivel más elevado.

Se debe tener en mente que los equipos involucrados necesitan tiempo libre para analizar y escribir todas las normas discutidas durante las reuniones. En síntesis el comité:

- Evalúa las normas y pautas de seguridad así como los procedimientos de notificación de incidentes de seguridad.
- Informa sobre los riesgos de seguridad en los activos TICs.
- Vela por que la seguridad de la información sea parte del proceso de planificación de las Tics de la organización.

Documento de la política de seguridad

Al iniciar el proceso de elaboración sobre una política de seguridad, es necesario recopilar cierta información con los usuarios de activos y realizar estudios de los documentos existentes. El objetivo de esa tarea es definir qué tipo de adaptación debe ser hecha en el modelo de estandarización existente para atender las características de la empresa (con relación a trazado, identificación, numeración y lenguaje utilizado). Si ya existen esos estándares definidos, los documentos de la política de seguridad deben adaptarse a ellos para garantizar una proximidad entre la práctica gerencial existente y la política sugerida (Ibíd).

Si existe ya un estándar de estructura de documentos para políticas dentro de la empresa, éste puede ser adoptado. A continuación se observa un modelo de estructura de política que puede ser desarrollado dentro de su organización. En este modelo se, visualiza que una política de seguridad está formada por tres grandes secciones que describen a continuación.

Directrices estratégicas. Conjunto de reglas generales de nivel estratégico donde se expresan los valores de seguridad de la organización. Es endosada por el líder empresarial de la organización y tiene como base su visión y misión para abarcar toda la filosofía de seguridad de la información.

Las directrices corresponden a las preocupaciones de la empresa sobre la seguridad de la información, al establecer sus objetivos, medios y responsabilidades.

Las directrices estratégicas, en el contexto de la seguridad, corresponden a todos los valores que deben ser seguidos para que el principal patrimonio de la empresa, que es la información, tenga el nivel de seguridad exigido.

Como la información no está presente en un único entorno (microinformática, por ejemplo) o medio convencional (fax, papel, comunicación de voz, etc.), debe permitir que se aplique a cualquier ambiente existente y no contener términos técnicos de informática. Se compone de un texto, no técnico, con las reglas generales que guían a la elaboración de las normas de seguridad (Ibíd).

Las normas en un nivel táctico. Conjunto de reglas generales y específicas de la seguridad de la información que deben ser usadas por todos los segmentos involucrados en los procesos de negocio de la institución, y que pueden ser elaboradas por activo, área, tecnología, proceso de negocio, público a que se destina, etc.

Las normas, por estar en un nivel táctico, pueden ser específicas para el público a que se destina, por ejemplo para técnicos y para usuarios.

- **Normas de Seguridad para técnicos:** Reglas generales de seguridad de información dirigidas a quienes cuidan de ambientes informatizados (administradores de red, técnicos etc.), basadas en los aspectos más genéricos como periodicidad para cambio de claves, copias de seguridad, acceso físico y otros. Pueden ser ampliamente utilizadas para la configuración y administración de ambientes diversos como Windows, Netware, Unix etc. (Ibíd.).
- **Normas de Seguridad para Usuarios:** Reglas generales de seguridad de las informaciones dirigidas para hacer uso en ambientes informatizados, basadas en aspectos más genéricos como cuidados con claves, cuidados con equipos, inclusión o exclusión de usuarios, y otros. Pueden ser

ampliamente utilizadas para todos los usuarios en ambientes diversos, como Windows, Netware, Unix, etc. (Ibíd.).

Procedimientos e instrucciones de trabajo en un nivel operacional

Los procedimientos e instrucciones de trabajo en un nivel operacional, pueden dividirse en las siguientes:

- **Procedimiento:** Conjunto de orientaciones para realizar las actividades operativas de seguridad, que representa las relaciones interpersonales e ínter departamentales y sus respectivas etapas de trabajo para la implantación o manutención de la seguridad de la información. (Ibíd.).
- **Instrucción de trabajo:** Conjunto de comandos operativos a ser ejecutados en el momento de la realización de un procedimiento de seguridad establecido por una norma, establecido en modelo de paso a paso para los usuarios del activo en cuestión. (Ibíd.).

Método

La investigación es de corte positivista, cuantitativa, descriptiva y no experimental.

La población se compuso de los funcionarios del Departamento de Tecnología Informática de la Universidad Tecnológica Intercontinental: 1 Director de Tecnología Informática, 2 Analistas de Sistemas, 2 Programadores, 2 Administradores de Base de Datos y 3 Encargados de Telecomunicaciones.

También se aplicó un cuestionario a los funcionarios de la UTIC que manejan sistemas de informaciones, de las siguientes Sedes: Informática (4 funcionarios), Postgrado y Empresariales (8 funcionarios), Derecho (8 funcionarios), Luque (5 funcionarios), San Lorenzo (10 funcionarios), Ñemby (6 funcionarios), Capiatá (7 funcionarios), Fernando de la Mora (32 funcionarios) y Loma Pyta (4 funcionarios); un total de 84 funcionarios.

A los funcionarios de las Sedes de la UTIC se les entregó un cuestionario, cuyo contenido fue expresado con preguntas que se extrajeron de las dimensiones. Es decir de sus indicadores. Para probar

la validez del cuestionario se aplicó a 9 funcionarios de la UTIC. Se validó la confiabilidad del cuestionario con la técnica Kuder Richardson, que arrojó 0,84 en el rango de 0 a 1.

Para el análisis de riesgo de la seguridad de la información en la UTIC, se aplicó el método de análisis de riesgo propuesto por Markus Erb (2009), que se basa en la siguiente fórmula matemática:

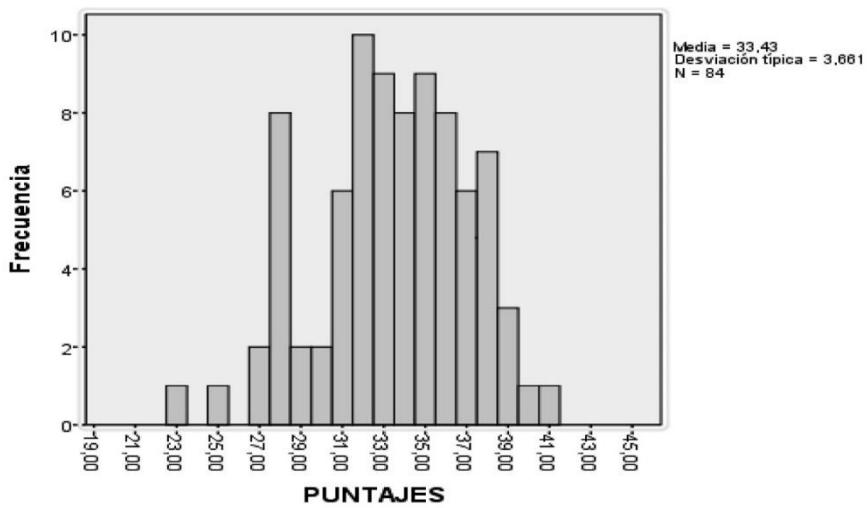
Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4).

Para el análisis e interpretación de los datos recogidos de la entrevista realizada con un cuestionario con preguntas dicotómicas a la Dirección de Tecnología Informática de la UTIC, se utilizó como punto de referencia principal la ISO/IEC 17799.

Resultados

Figura 1. *Resumen estadístico global de las Sedes*



Analizando las puntuaciones de los 84 funcionarios de las nueve sedes examinadas, en función a los estadísticos descriptivos de la distribución de las puntuaciones, arrojan una media de 32,4286 puntos que está relacionado a la desviación típica que deja ver la tendencia de las puntuaciones hacia el manejo inseguro de la información ya que la desviación es de 3,66121 puntos que mide el grado de separación en torno a la media obteniendo un intervalo de (28,76739 ; 36,08981) con mayor recorrido hacia las puntuaciones de manera insegura del manejo de la información. La mediana observada es de 34 puntos, que es mayor a la mediana esperada y reivindica lo demostrado con la desviación típica, que la tendencia va hacia los puntajes más altos. La tabla de frecuencia muestra que las puntuaciones son casi compactas en todo su recorrido, con una puntuación mínima de 23 puntos y una máxima de 41 puntos, donde sobresale la frecuencia modal de diez funcionarios para la puntuación de 32 (seguro) y además expone que el 61,9 % de las puntuaciones se acumula hacia puntajes mayores a los esperados induciendo hacia al manejo inseguro de la información de todos los funcionarios analizados, Los percentiles indican que el 75 % de las puntuaciones está por encima de 31 puntos y que la acumulación de los puntajes va hacia el manejo inseguro de las informaciones.

Teniendo en cuenta la cantidad aproximada de funcionarios por sede, en función a las puntuaciones mayores al valor esperado de 33 puntos, se tiene una proporción global con respecto al manejo de la información de manera insegura con $p = \frac{47}{84} = 55{,}95\ \%$ y una proporción de manera segura con $p = \frac{37}{84} = 44{,}05\ \%$.

Tabla 1. *Detalles de las respuestas negativas por Sedes*

PREGUNTAS	FERNANDO DE LA MORA	SAN LORENZO	EMPRESARIALES Y POSTGRADOS	CAPIATA	ÑEMBY	DERECHO	LUQUE	LOMA PYTA	INFORMATICA
1- Las informaciones transmitidas por medios electrónicos y papel ¿consideras como un activo esencial que está sujeto a amenazas y vulnerabilidades?	28,1%	20,0%	12,5%	28,6%	33,3%	25,0%	100,0%	0,0%	25,0%
2- En la cláusula de su contrato ¿existe un compromiso por parte de la Institución de proteger sus datos y la privacidad de sus informaciones personales?	75,0%	60,0%	87,5%	42,9%	83,3%	75,0%	100,0%	75,0%	75,0%
3- ¿Has firmado un acuerdo de confidencialidad o no-divulgación de las informaciones de la Institución?	59,4%	30,0%	75,0%	42,9%	100,0%	37,5%	80,0%	50,0%	75,0%
4- ¿Existe un listado de las autoridades (bomberos, médicos, policiales etc.) que se puede contactar en caso de incidentes de seguridad de la información (incendios, robo etc.)?	65,6%	30,0%	50,0%	42,9%	16,7%	0,0%	20,0%	100,0%	25,0%
5- ¿Existen reglas o lineamientos para el uso de medios y recursos del procesamiento de la información de la institución. Por ejemplo correo electrónico e Internet, dispositivos móviles etc.?	40,6%	30,0%	75,0%	42,9%	33,3%	37,5%	20,0%	75,0%	25,0%
6- ¿Existen medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil?	65,6%	60,0%	75,0%	57,1%	83,3%	75,0%	60,0%	100,0%	50,0%
7- Los medios de procesamiento de informaciones (computadoras) ¿están en áreas seguras que no permitan el acceso de terceros?	34,4%	60,0%	50,0%	28,6%	16,7%	62,5%	0,0%	100,0%	50,0%
8- ¿Existe un mecanismo que tú conoces sobre los accesos de los visitantes a la institución registrando la fecha y la hora de entrada y salida de los mismos?	46,9%	90,0%	75,0%	42,9%	66,7%	87,5%	80,0%	100,0%	25,0%
9- En caso de corte de energía ¿posee un dispositivo de suministro de energía ininterrumpido (UPS o generador de emergencia)?	59,4%	90,0%	75,0%	42,9%	50,0%	87,5%	40,0%	50,0%	50,0%
10- ¿Se realiza mantenimiento constante a tu computadora?	75,0%	70,0%	75,0%	57,1%	16,7%	62,5%	20,0%	75,0%	50,0%
11- ¿Tienes conocimiento de la instalación de antivirus en tu maquina?	34,4%	10,0%	62,5%	42,9%	50,0%	12,5%	60,0%	25,0%	50,0%
12- ¿Realizas copia de seguridad de las informaciones que manejas?	71,9%	50,0%	62,5%	71,4%	50,0%	62,5%	60,0%	75,0%	25,0%
13- El intercambio electrónico de informaciones con las Sedes ¿realizas con el correo institucional?	31,3%	40,0%	62,5%	71,4%	50,0%	62,5%	40,0%	50,0%	25,0%
14- ¿Utilizas el fax para enviar informaciones de la institución?	6,3%	10,0%	0,0%	14,3%	0,0%	0,0%	0,0%	25,0%	0,0%
15- Los transportes utilizados para la transferencia de documentos de una Sede a otra ¿son confiables?	43,8%	30,0%	50,0%	28,6%	33,3%	50,0%	40,0%	50,0%	75,0%
16- ¿Has firmado un documento para mantener confidenciales las claves secretas de los sistemas de informaciones que maneja?	71,9%	90,0%	100,0%	71,4%	83,3%	50,0%	80,0%	75,0%	75,0%
17- ¿Existe un método de almacenaje seguro para las claves de los sistemas de información?	68,8%	80,0%	87,5%	71,4%	66,7%	75,0%	60,0%	100,0%	50,0%
18- ¿Cierras la sesión de tu computadora, cuando no está trabajando en la misma?	25,0%	40,0%	87,5%	42,9%	16,7%	37,5%	40,0%	50,0%	25,0%
19- Los papeles o medios de almacenamiento electrónicos de la institución ¿Son guardados bajo llaves?	53,1%	90,0%	87,5%	71,4%	83,3%	87,5%	60,0%	75,0%	50,0%
20- ¿Solo los técnicos de la institución pueden instalar programas en tu computadora?	15,6%	10,0%	37,5%	14,3%	33,3%	0,0%	0,0%	75,0%	0,0%
21- ¿Se cierra automáticamente la sesión de su computadora, cuando no está trabajando en la misma?	28,1%	70,0%	62,5%	71,4%	100,0%	37,5%	40,0%	50,0%	75,0%
22- ¿Has recibido capacitación en seguridad de la información en la institución?	75,0%	90,0%	100,0%	71,4%	100,0%	75,0%	80,0%	100,0%	75,0%

Se observa el porcentaje de las preguntas respondidas de manera negativa (NO) por los funcionarios de cada Sede de la UTIC. Teniendo en cuenta un punto de corte del 50 % que es el porcentaje esperado, se indica en la tabla en color amarillo aquellas preguntas que superaron el porcentaje esperado por Sede, considerándose como los puntos más inseguros. En el cuadro también se observan, en color amarillo, los puntos de concordancia entre las Sedes que evidencian el manejo inseguro de las informaciones.

Tabla 2. *Informe global de las respuestas negativas de las nuevas Sedes*

PREGUNTAS		Porcentaje de casos
1-	Las informaciones transmitidas por medios electrónicos y papel ¿consideras como un activo esencial que está sujeto a amenazas y vulnerabilidades?	28,6 %
2-	En la cláusula de su contrato ¿existe un compromiso por parte de la Institución de proteger sus datos y la privacidad de sus informaciones personales?	73,8 %
3-	¿Has firmado un acuerdo de confidencialidad o no-divulgación de las informaciones de la Institución?	58,3 %
4-	¿Existe un listado de las autoridades (bomberos, médicos, policiales etc.) que se puede contactar en caso de incidentes de seguridad de la información (incendios, robo etc.)?	45,2 %
5-	¿Existen reglas o lineamientos para el uso de medios y recursos del procesamiento de la información de la institución. Por ejemplo correo electrónico e Internet, dispositivos móviles etc.?	41,6 %
6-	¿Existen medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil?	67,9 %
7-	Los medios de procesamiento de informaciones (computadoras) ¿están en áreas seguras que no permitan el acceso de terceros?	41,7 %
8-	¿Existe un mecanismo que tú conoces sobre los accesos de los visitantes a la institución registrando la fecha y la hora de entrada y salida de los mismos?	63,1 %
9-	En caso de corte de energía ¿posee un dispositivo de suministro de energía ininterrumpido (UPS o generador de emergencia)?	63,1 %
10-	¿Se realiza mantenimiento constante a tu computadora?	63,1 %
11-	¿Tienes conocimiento de la instalación de antivirus en tu maquina?	35,7 %

12- ¿Realizas copia de seguridad de las informaciones que manejas?	63,1 %
13- El intercambio electrónico de informaciones con las Sedes ¿realizas con el correo institucional?	44,0 %
14- ¿Utilizas el fax para enviar informaciones de la institución?	6,0 %
15- Los transportes utilizados para la transferencia de documentos de una Sede a otra ¿son confiables?	42,9 %
16- ¿Has firmado un documento para mantener confidenciales las claves secretas de los sistemas de informaciones que maneja?	76,2 %
17- ¿Existe un método de almacenaje seguro para las claves de los sistemas de información?	72,6 %
18- ¿Cierras la sesión de tu computadora, cuando no está trabajando en la misma?	36,9 %
19- Los papeles o medios de almacenamiento electrónicos de la institución ¿Son guardados bajo llaves?	69,0 %
20- ¿Solo los técnicos de la institución pueden instalar programas en tu computadora?	17,9%
21- ¿Se cierra automáticamente la sesión de su computadora, cuando no está trabajando en la misma?	50,0 %
22- ¿Has recibido capacitación en seguridad de la información en la institución?	82,1 %

Se observa el porcentaje de las preguntas respondidas de manera negativa (NO) por los 84 funcionarios de la UTIC. Teniendo en cuenta un punto de corte del 50 % que es el porcentaje esperado, se indicaron en la tabla, en color amarillo, aquellas preguntas que superaron el porcentaje esperado considerándose como los puntos más inseguros.

De las 22 preguntas respondidas por los funcionarios, en función a las respuestas negativas (no), se indica en la tabla en color amarillo aquellas respuestas que sobrepasaron la proporción esperada "p" de 50 %, teniendo en cuenta el porcentaje de manera decreciente, predomina la pregunta N° 22 con 82,1 % de respuestas negativas, seguidas por la N° 16 con 76,2 %, la N° 2 con 73,8 %, N° 17 con 72,6 % y la N° 19 con 69 % que son las preguntas con los porcentajes más significativos de la tabla.

Tabla 3. *Análisis del manejo de información con respecto a los aspectos técnicos*

<table>
<tr><th>SI</th><th>Puntos seguros en el manejo de la información</th><th>NO</th><th>Puntos inseguros en el manejo de la información</th></tr>
<tr><td colspan="2">1. La ubicación de los medios de procesamientos de informaciones de la institución ¿está aislada de personas no autorizadas?
“los medios de procesamiento de información se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo” (p. 56).</td><td colspan="2" rowspan="2">3. ¿Existen controles para minimizar el riesgo de amenazas potenciales de los medios de procesamiento de la información? En los siguientes casos: robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones y vandalismo.
“se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo” (p. 56).</td></tr>
<tr><td colspan="2">2. El ángulo de visión de los medios de procesamiento de información ¿es restringida de personas no autorizadas?
“los medios de procesamiento de la información que manejan data confidencia debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y se debieran asegurar los medios de almacenaje para evitar el acceso no autorizado” (p. 57).</td></tr>
<tr><td colspan="2" rowspan="2">4. ¿Se monitorea las condiciones ambientales para los medios de procesamiento de la información, tales como temperatura y ~~H~~ humedad?
“se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información” (p. 56).</td><td colspan="2">5. ¿Existen filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones?
“se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones” (p. 56).</td></tr>
<tr><td colspan="2"></td></tr>
</table>

6. Los medios de procesamientos de informaciones ¿cuentan con dispositivo de suministro de energía ininterrumpido (UPS)? ***"se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas" (p. 57).***	7. Las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información ¿son subterráneas? ***"las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información debieran ser subterráneas" (p. 59).***
8. Los cables de energía ¿están separados de los cables de comunicaciones? ***"los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia" (p. 59).***	9. Los empalmes de las líneas de comunicaciones ¿están documentados? ***"se debiera utilizar una lista de empalmes documentados para reducir la posibilidad de error" (p. 59).***
10. ¿Se realiza el mantenimiento de los equipos de acuerdo a las especificaciones de servicio recomendados por el proveedor? ***"el equipo se debiera mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor" (p. 59).***	11. Los mantenimientos y servicios de los medios de los equipos ¿son solamente llevados a cabo por el personal técnico de la Institución? ***"sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo" (p. 59).***
12. El uso de los equipos de procesamiento de la información fuera de la institución ¿posee una previa autorización? ***"sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera del local de la organización debiera ser autorizado por la gerencia" (p. 60).***	13. Los equipos que se darán de baja ¿son físicamente destruidos? ***"los equipos que contienen información confidencial debieran ser físicamente destruidos o se debieran destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear" (p. 61).***

<table>
<tr><td rowspan="2">14.¿Existen procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación?
“se debieran preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad”
(p. 62).</td><td>15. Los cambios en los medios y sistemas de procesamiento de la información ¿están sujetos a un estricto control gerencial del cambio?
“se debieran controlar por la gerencia los cambios en los medios y sistemas de procesamiento de la información” (p. 63).</td></tr>
<tr><td>16. Los medios de desarrollo, prueba y operación ¿están separados?
“los medios de desarrollo, prueba y operación debieran estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional” (p. 65).</td></tr>
<tr><td>17. ¿Se realiza las proyecciones de recursos necesarios para asegurar el desempeño del sistema?
“se debieran realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema” (p. 69).</td><td rowspan="2">18. ¿Existen criterios de aceptación de los usuarios de los sistemas de información nuevos?
“se debiera establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas y se debieran realizar pruebas adecuadas del sistema(s) durante el desarrollo y antes de su aceptación” (p. 70).</td></tr>
<tr><td>19. ¿Existen controles para evitar, detectar y eliminar los códigos maliciosos?
“la protección contra códigos maliciosos se debiera basar en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio”
(p. 70).</td></tr>
<tr><td></td><td>20. ¿Existen medios de respaldos adecuados que permitan recuperar las informaciones después de un desastre o falla de medios?
“se debiera proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios” (p. 73).</td></tr>
</table>

21. Las copias de respaldos ¿están almacenados en diferentes lugares? ***"las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal"*** ***(p. 73).***	22. ¿Se realiza pruebas periódicas de las copias de respaldo? ***"los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia" (p. 74).***
23. Las copias de seguridad ¿son protegidas por medios de una codificación? ***"en situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación" (p. 73).***	24. ¿Existe un período de retención de las copias de respaldo? ***"se debiera determinar el período de retención para la información comercial esencial, y también cualquier requerimiento para que las copias de archivo se mantengan permanentemente" (p. 73).***
25. ¿Existen los registros de ingreso y monitoreo de la red? ***"se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes" (p. 75).***	26. ¿Utiliza tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red? ***"se debiera de utilizar tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red" (p. 77).***
27. La documentación del sistema ¿se almacena en gavetas de seguridad? ***"la documentación del sistema se debiera almacenar de una manera segura, en gavetas de seguridad" (p. 79)***	28. ¿Se monitorea los sistemas reportando los eventos de seguridad de la información? ***"se debieran monitorear los sistemas y se debieran reportar los eventos de seguridad de la información. Se debieran utilizar bitácoras de operador y se debieran registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información" (p. 89).***
29. ¿Se registran los intentos de acceso fallidos y rechazados al sistema? ***"se debieran producir y mantener registros de auditoría de las actividades, como los registros de intentos de acceso fallidos y rechazados al sistema" (p. 89).***	

30. ¿Se registran las actividades del operador del sistema de informaciones? ***"se debieran registrar las actividades del operador del sistema, la información sobre el evento (por ejemplo, archivos manejados) o falla (por ejemplo, el error ocurrido y la acción correctiva)" (p. 92).***	31. ¿Se registran las fallas del sistema? ***"se debieran registrar y analizar las fallas del sistema, y se debieran tomar las acciones necesarias" (p. 93).***
32. ¿Existe un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información? ***"debiera existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información" (p. 96).***	33. Los sistemas de información ¿permiten el acceso con asignación de privilegios a los usuarios? ***"los privilegios de acceso asociados con cada producto del sistema; por ejemplo, sistema de operación, sistema de gestión de base de datos y cada aplicación, y se debieran identificar los usuarios a quienes se les necesita asignar privilegios" (p. 97).***
34. Los usuarios ¿firman un enunciado para mantener confidenciales las claves secretas que se les asignan para el acceso a los sistemas de información? ***"se debiera requerir que los usuarios firmen un enunciado para mantener confidenciales las claves secretas y mantener las claves secretas grupales sólo dentro de los miembros el grupo; este enunciado firmado se puede incluir en los términos y condiciones de empleo" (p. 98).***	35. ¿Existe una política que mencione que los usuarios sólo deben tener acceso a los servicios para los cuales hayan sido específicamente autorizados? ***"los usuarios sólo debieran tener acceso a los servicios para los cuales hayan sido específicamente autorizados" (p. 103).***
	36. ¿Existen métodos de autenticación para controlar el acceso de usuarios remotos? ***"se debieran utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos, por ejemplo, una técnica basada en criptografía, dispositivos de hardware o un protocolo de desafío/respuesta" (p. 104).***

37. ¿Existe una identificación automática de los equipos en la red? ***"la identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos" (p. 105).***	38. ¿Existe un control al acceso físico y lógico a los puertos de diagnóstico y configuración de la red? ***"se debiera controlar el acceso físico y lógico a los puertos de diagnóstico y configuración" (p. 106).***
39. La red de comunicación de la institución ¿está dividida en dominios? ***"un método para controlar la seguridad de grandes redes es dividirlas en dominios de red lógicos separados; por ejemplo, dominios de red internos y dominios de red externos de una organización; cada uno protegido por un perímetro de seguridad definido" (p. 106).***	40. ¿Utilizan las tecnologías "proxy"? ***"si se emplean tecnologías "proxy" (en inglés, representante o apoderado) y/o de traducción de direcciones de la red, se pueden utilizar los gateways de seguridad para validar las direcciones de la fuente y el destino en los puntos de control de las redes internas y externas" (p. 108).***
41. Los usuarios ¿se autentican para ingresar al sistema operativo? ***"se debieran utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados, por ejemplo autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida" (p. 109).***	42. Las sesiones inactivas ¿se cierran después de un período de inactividad definido? ***"las sesiones inactivas debieran ser cerradas después de un período de inactividad definido" (p. 113).***
43. Los sistemas de información ¿poseen menús para controlar el acceso a las funciones del mismo? ***"se debiera de proporcionar menús para controlar el acceso a las funciones del sistema de aplicación" (p. 115).***	44. Los sistemas confidenciales ¿poseen un ambiente de cómputo dedicado? ***"los sistemas confidenciales debieran tener un ambiente de cómputo dedicado (aislado). Algunos sistemas de aplicación son lo suficientemente sensibles a una pérdida potencial que requieren un manejo especial" (p. 115).***

45. ¿Existen requerimientos de seguridad de la información en los proyectos de sistemas de información? ***"se debieran identificar todos los requerimientos de seguridad en la fase de requerimientos de un proyecto; y debieran ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información" (p. 120).***	46. ¿Se utiliza los controles criptográficos para proteger la información? ***"se debiera desarrollar una política sobre el uso de controles criptográficos. Se debiera establecer una gestión clave para sostener el uso de técnicas criptográficas" (p. 124).***
47. ¿Existen procedimientos para el control de la instalación del software en los sistemas operacionales? ***"se debieran establecer procedimientos para el control de la instalación del software en los sistemas operacionales" (p. 128).***	48. En cuanto a las base de datos ¿existe una base datos dedicada para propósitos de prueba, durante el desarrollo? ***"se debiera evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial para propósitos de pruebas" (p. 130).***
49. ¿Existen políticas de control de acceso al código fuente de los programas y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación)? ***"el acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debieran controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados" (p. 130).***	50. Los cambios propuestos por los usuarios ¿Son revisados por el gerente de TI? ***"los gerentes responsables por los sistemas de aplicación también debieran ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos debieran asegurar que todos los cambios propuestos para el sistema sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación" (p. 132).***

51. ¿Se escanea el flujo de salida de los medios y las comunicaciones en la red? ***"se debiera de escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida" (p. 134).***	52. ¿Se registran las vulnerabilidades técnicas de los sistemas de información? ***"se debiera obtener oportuna-mente la información sobre las vulnerabilidades técnicas de los sistemas de están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados" (p. 136).***

De las 54 preguntas cerradas realizadas a la Dirección de Tecnología Informática de la UTIC, 28 preguntas cumplen con el manejo seguro de la información y 24 de manera insegura, cabe destacar que se realizó una presentación genérica en una tabla de dos columnas de las preguntas que fueron respondidas positiva y negativamente. Como sustentación teórica se tomó la ISO/IEC 17799, cuyos párrafos se colocaron debajo de cada pregunta entre comilla, negrita y el número página.

Comentarios

La investigación sobre las políticas de seguridad de la información para el Departamento de Tecnología Informática cuyo objetivo general fue la de describir la realidad que presenta la UTIC para la construcción de política de seguridad de la información en la Sedes de la Regional Central, el análisis de riesgo desde la percepción de la Dirección de Tecnología Informática arrojó un promedio que no supera el umbral de medio riesgo que está entre el 7,4 y 7.6 del rango 8-9 y no llega al umbral de alto riesgo que representa el rango de 12-16.

En cuanto a los aspectos culturales en el manejo de la información se pudo evidenciar el manejo de la información en las Sedes de la UTIC, arrojando una proporción global con respecto al manejo de la información de manera insegura con $p = \frac{47}{84} = 55{,}95\ \%$ y una proporción de manera segura con $p = \frac{37}{84} = 44{,}05\ \%$. En los aspectos técnicos en el manejo de la información, se pudo demostrar

que 28 puntos de la seguridad de la información cumplen con el manejo seguro de la información y 24 de manera inseguro, desde un análisis e interpretación teórica en base a la ISO/IEC 17799. Con esta investigación se pudo describir la realidad de la UTIC para la construcción de política de seguridad cuya concentración de los datos recogidos arrojaron un alto nivel de inseguridad de 55,95 %. Por la misma se recomienda la implementación de las políticas de seguridad de la información desarrolladas para la UTIC, debiéndose evaluar el resultado de la implementación en un periodo de un año y con una constante actualización.

Referencias

Academia Latinoamericana de Seguridad informática (2009). *La política de seguridad*. Recuperado de http://www.slideshare.net/galactico_87/politicas-de-seguridad-informatica-normas

Areitio, J. (2006). Seguridad de la información: redes, informática y sistemas de información, Madrid, España: Ediciones Paraninfo.

Bernal Torres, A (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales*. México: Pearson Educación.

Gutiérrez, J (2003). *Protocolos criptográficos y seguridad en redes*. Cantabria, España: Publicaciones Universidad de Cantabria.

Herrera Pérez, E. (2003). *Tecnologías y redes de transmisión de datos*. México. Editorial Limusa.

ISO/IEC 17799:2000. *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información*. 2005.

Mcleod, J (2000). *Sistema de información gerencial*. México: Prentice Hall.

Ministerio de Ciencia e Innovación. Orden de Comité de Seguridad de la información. Recuperado de http://www.mineco.gob.es/stfls/mineco/ministerio/ficheros/Orden_CSI_firmada.pdf

Peso Navarro, E. (2003). *Manual de outsourcing informático: (análisis y contratación)*. Madrid, España: Editorial Díaz de Santos

SISTESEG (2011). *Seguridad de la Información*. Recuperado de http://www.sisteseg.com/informatica.html

Solís Salazar, C. (2014). *¿Qué son las Políticas de Seguridad de la Información?* Recuperado de http://www.solis.com.ve/que-son-las-politicas-de-seguridad-de-la-informacion/