Metodología para seleccionar políticas de seguridad informática en un establecimiento de educación superior

***Juan Diego Muñoz*[1], *Diego Ponce Vásquez*[2]**

[1] Maestría en Gestión Estratégica de Tecnologías de la Información y Comunicación, Universidad de Cuenca, Av. 12 de Abril y Av. Loja, Cuenca, Ecuador, 01.01.168.

[2] Facultad de Ingeniería, Universidad de Cuenca, Av. 12 de Abril y Av. Loja, Cuenca, Ecuador, 01.01.168.

Autores para correspondencia: juan.munoz@ucuenca.edu.ec, diego.ponce@ucuenca.edu.ec

Fecha de recepción: 30 de julio de 2017 - Fecha de aceptación: 15 de agosto de 2017

RESUMEN

La selección e implementación de políticas de seguridad informática a momentos resulta dificultoso cuando no se emplea un procedimiento adecuado. A esto se suma un problema más, que en varias ocasiones no se tiene datos históricos como por ejemplo auditorías informáticas para determinar la situación actual y el grado de madurez de la seguridad informática en los establecimientos de educación superior. El presente trabajo busca desarrollar una metodología para obtener datos que nos permitan determinar la situación actual de la seguridad informática en la Dirección de Tecnologías de Información y Comunicación (DTIC) de la Universidad de Cuenca. En este estudio se aplica el método Delphi para hacer consulta a expertos en dónde se utilizaron todos los controles de la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 para elaborar los cuestionarios que nos permitan, en primer lugar, identificar las vulnerabilidades y, en segundo lugar, priorizar los controles de seguridad para seleccionar las políticas de seguridad informáticas específicas que se necesitan implementar en la DTIC. Los resultados obtenidos demuestran que existen pocas políticas de seguridad informática, las cuales están definidas en términos muy generales dentro de la institución. Adicionalmente, se determinó que no se realiza una adecuada revisión y verificación del cumplimiento.

Palabras clave: Políticas de seguridad, NTE INEN-ISO/IEC 27002:2009, método Delphi, CC.

ABSTRACT

The selection and implementation of computer security policies is sometimes difficult when an adequate procedure is not in place nor used. An additional problem to this situation is that rarely we possess historical data, such as computer audits, as to determine the current situation and the maturity degree of computer security at higher education institutions. The present study attempted to develop a methodology to collect data that permit the determination of the current situation of computer security in the Department of Information and Communication Technologies (DTIC) of the University of Cuenca. The Delphi method was applied to consult experts if all the controls of the NTE INEN-ISO/IEC 27002:2009 Ecuadorian Technical Standard were used as basis for the elaboration of questionnaires. The questionnaires allowed to identify the vulnerabilities and prioritize security controls and permitted to select the specific IT security policies needed to be implemented in the DTIC. The obtained results demonstrate that there are few computer security policies in place, and in addition they are defined in very general terms within the institution. Further, the study revealed that an adequate review and verification of compliance is not performed.

Keywords: IT security policies, NTE INEN-ISO/IEC 27002:2009, Delphi Method, CC.

1. INTRODUCCIÓN

En la última década la penetración de las Tecnologías de Información y Comunicación (TIC) en la vida de las personas ha generado un cambio radical, la gran mayoría de la humanidad utiliza las TIC para sus propósitos personales. Así también los sectores industriales, empresariales y educativos no son ajenos a los cambios que trajo consigo la inclusión de las TIC en la vida diaria. Sin embargo, existen retos también asociados a su adopción, como por ejemplo garantizar la confidencialidad, disponibilidad e integridad de los datos cuando exista un ataque informático como lo indica Chavez (2009). Muchas entidades públicas y privadas, así como las educativas, utilizan el internet para sus transacciones diarias, por ejemplo: muchos establecimientos educativos utilizan sistemas web para uso tanto de docentes como de estudiantes, los mismos que pueden ser blanco de innumerables ataques informáticos.

Según Dussan (2006) "Las vulnerabilidades en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crackers que penetran los sistemas de seguridad". Solórzano, Triviño, & Alfonso (2013) señalan que un estudio realizado en el año 2013 a empresas corporativas ecuatorianas revela que un 24% de empresas realiza outsourcing de seguridad informática, otro 50% dispone de un área de seguridad informática dentro de cada organización y un 80% tiene establecido políticas de seguridad informática de manera general y están conscientes de que existe la probabilidad de sufrir pérdidas de información. Los establecimientos de educación superior no están exentos de sufrir ataques informáticos y pérdidas de información. Baldeón & Coronel (2012) indican que desde el año 2002 se han efectuado 308 ataques informáticos exitosos a las páginas web de las instituciones educativas de Ecuador.

Por un lado, las instituciones educativas hacen grandes esfuerzos para implementar mecanismos de control, pero se ha dejado a un lado aspectos muy importantes como por ejemplo la implementación de políticas de seguridad informática específicas, aquí surgen las siguientes interrogantes: ¿Son suficientes los mecanismos de seguridad implementados en la actualidad? ¿El personal técnico tiene el conocimiento de los reglamentos para garantizar la seguridad informática? ¿Conocen los usuarios finales las consecuencias de violentar un mecanismo de seguridad informática?

Uno de los grandes inconvenientes que se tiene al momento de implementar políticas de seguridad informática es el desconocimiento del punto de partida, debido entre otras causas a la ausencia de datos históricos, como, por ejemplo, acceso a la información de auditorías informáticas que puedan ayudar a determinar la situación actual y el grado de madurez de la seguridad informática en cualquier establecimiento.

Existen algunos procedimientos para contrarrestar este inconveniente. Algunos investigadores utilizan una metodología en la cual clasifican las áreas primordiales para la seguridad, siendo las áreas Gerenciales, TIC y Administrativas las más críticas, usan matrices de cobertura para aplicar las políticas de seguridad. Romo & Valarezo (2012) emplean otra metodología en la cual utilizan una matriz causa-efecto, para clasificar los problemas de seguridad e implementar las políticas de seguridad. Estos procedimientos se basan en implementar medidas correctivas, como, por ejemplo, controles y políticas de seguridad informática. Sin embargo, no realizan un levantamiento de información previo para identificar las vulnerabilidades actuales de los establecimientos.

En el presente trabajo se utilizó el método Delphi, como lo utilizaron Cabero & Infante (2014), cuando no se tienen datos históricos. El método nos permitió obtener información por medio de consultas a los expertos informáticos que laboran en la DTIC. Aquí se utilizaron todos los controles de la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 para elaborar los cuestionarios que nos permitieron determinar la situación actual e identificar las vulnerabilidades informáticas. Posteriormente se realizó una selección de políticas de seguridad informáticas específicas como medidas correctivas para mejorar los niveles de seguridad informática en la DTIC.

El documento tiene la siguiente estructura: en la sección método se presenta el procedimiento empleado para realizar un levantamiento de datos que nos permitió identificar la situación actual y el grado de madurez de la seguridad informática, también se detalla quiénes son los expertos que proporcionaron la información, así como los materiales utilizados. En la sección de resultados se detallan tanto los porcentajes de cumplimiento obtenidos por medio de los cuestionarios, como

también la importancia que tienen los dominios de la norma, para luego seleccionar y listar las políticas de seguridad que se necesitan implementar en la DTIC. En la sección discusión se realiza un breve análisis de los resultados obtenidos y se finaliza con algunas conclusiones.

2. MÉTODO

1.1. Expertos

Los participantes fueron 10 funcionarios que laboran en la DTIC (4 mujeres, 6 hombres), comprendidos entre las edades de 25 a 40 años, todos son ingenieros de sistemas. Son considerados expertos informáticos porque son quienes desarrollan y administran los sistemas informáticos, administran los equipos de redes y comunicación. También está incluido el personal que brinda soporte a los usuarios finales.

1.2. Materiales

Norma NTE INEN-ISO/IEC 27002:2009

Se utilizó esta norma ya que es una adopción idéntica de la Norma Internacional ISO/IEC 27002:2005 traducida al español y adaptada a nuestra región, esta norma recopila un gran número de controles informáticos para garantizar la seguridad informática en cualquier establecimiento, la norma es de fácil interpretación y es muy utilizada como herramienta de apoyo para aplicar medidas correctivas de seguridad informática, cada organización puede hacer uso de esta herramienta según sus intereses y objetivos (LEXIS S.A., 2004).

Políticas de seguridad informática - Mejores prácticas internacionales

Se utilizó este manual para seleccionar las políticas de seguridad a implementar en la DTIC, ya que recopila un sinnúmero de políticas de seguridad informática de todo ámbito con una estructura estándar, lo que facilita su modificación y adaptación para implementar en cualquier tipo de empresa y establecimientos educativos (Wood, 2002, pág. 44).

1.3. Procedimiento

Para una mejor comprensión, el proceso se dividió en dos fases, las mismas que se detallan a continuación:

Fase 1: Levantamiento de información y determinación de la situación actual en la DTIC

Aquí se elaboró los cuestionarios en base a todos los controles de la norma NTE INEN-ISO/IEC 27002:2009. La norma está conformada por 11 *dominios* principales, 39 objetivos de control y 133 *controles*, estructurada de la siguiente forma: un *dominio* puede tener uno o varios *objetivos de control*, y un objetivo de control tiene varios *controles*. Los cuestionarios fueron ponderados con un rango que va desde el 10 al 100% de cumplimiento, para lo cual se utilizó indicadores similares a los que se usan en la medición de la gestión, como lo utilizó Lanche (2015).

Se clasificó las preguntas de acuerdo con las actividades que realizan cada uno de los expertos informáticos que laboran en la DTIC. Por medio de las visitas de campo se empleó los cuestionarios para que los expertos establezcan los porcentajes de cumplimiento de acuerdo con su criterio con una debida justificación. El resultado del porcentaje de cumplimiento total para cada pregunta fue obtenido mediante el promedio de todas las respuestas.

Una vez obtenido los porcentajes de cumplimiento en los cuestionarios, el siguiente paso fue realizar una cuantificación de estos datos en porcentajes de cumplimiento basados en *objetivos de control*. Posteriormente se cuantificó estos nuevos datos en porcentajes de cumplimiento basados en los *dominios de la norma*, para lo cual se utilizó la siguiente expresión matemática que puede ser utilizada para hacer cuantificaciones en análisis de decisiones multicriterio, como le utilizaron Ishizaka & Nemery (2013):

$$D = \sum_{i=1}^{N} POC_i \sum_{j=1}^{M} ((PC_j * k)/100)$$

Siendo D = dominio, N = cantidad de objetivos de control, i = objetivo de control, POC = porcentaje objetivo de control, M = cantidad de controles, j = controles, PC = porcentaje control, k = (100/N)/M. Este cálculo matemático se utilizó para cuantificar en porcentajes de cumplimiento total para cada uno de los 11 dominios de la norma.

Fase 2: Priorización de los Dominios de la norma y selección de las políticas de seguridad informática

Para priorizar que *dominios* de la norma son los más necesarios de implementar en la DTIC, se identificó en primer lugar la importancia de estos *dominios* mediante juicio de expertos, para lo cual se elaboró otro cuestionario donde se estableció una ponderación de *baja, media, alta*. Por medio de otra visita de campo se empleó los cuestionarios para que los expertos establezcan la importancia que ellos consideran necesaria con su respectiva justificación. La importancia final para cada uno de los 11 *dominios* se obtuvo mediante la contabilización de la mayor cantidad de respuestas iguales. El siguiente paso fue categorizar los *dominios* de acuerdo con los porcentajes de cumplimiento, aquí se utilizó la siguiente escala de categorización: bajo = ≤35% de cumplimiento; medio = ≥36 y ≤70% de cumplimiento; y alto ≥71%. La misma que es usada en las matrices de toma de decisiones, como la utilizaron Medina, Ortiz, Franco, & Aranzazú (2010).

El último paso fue realizar una priorización de los 11 *dominios* de la norma de acuerdo con la importancia y porcentajes de cumplimiento. Para los cual se utilizó la siguiente tabla de criterios (ver Tabla 1) de valoración establecida por juicio de expertos, como lo utilizaron Mosquera, Andrade, & Sierra (2013). Las priorizaciones a los Dominios de la norma permitieron la selección de las políticas que se necesitan implementar en la DTIC para mejorar la seguridad informática.

Tabla 1. Criterios de valoración para *dominios*

Cumplimiento / Importancia	Alta	Media	Baja
Bajo	Alta	Alta	Media
Medio	Alta	Media	Baja
Alto	Media	Baja	Baja

3. RESULTADOS

Los resultados se presentan de acuerdo con cada una de las dos fases del punto anterior.

Fase 1: Levantamiento de información y determinación de la situación actual en la DTIC

En la Tabla 2 se puede apreciar los porcentajes de cumplimiento que tiene la DTIC con respecto a los 11 dominios de la norma.

De manera general se puede observar que los dominios de alto cumplimiento son los relacionados con “Gestión de activos”, “Gestión de comunicaciones y operaciones”, “Controles de acceso”, “Gestión de la continuidad del negocio”; debido a la implementación de algunos controles, pero falta definir nuevos mecanismos se seguridad específicos. Los dominios de cumplimiento bajo son los relacionados con: “Políticas de seguridad”, “Cumplimiento”; debido posiblemente al desconocimiento de la importancia de establecer políticas de seguridad específicas y realizar verificaciones del correcto cumplimiento. Con la obtención de los porcentajes de cumplimento de los 11 *dominios* se realizó un cálculo del promedio para determinar el porcentaje de cumplimiento total que fue del 52%.

Tabla 2. *Dominios* y porcentaje de cumplimiento.

	Dominios	% Cumplimiento
1	Política de seguridad	30
2	Aspectos organizativos de seguridad de la información	46
3	Gestión de activos	60
4	Seguridad ligada a los recursos humanos	55
5	Seguridad física y del entorno	61
6	Gestión de comunicaciones y operaciones	60
7	Control de acceso	67
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	56
9	Gestión de incidentes de seguridad de la información	55
10	Gestión de la continuidad del negocio	54
11	Cumplimiento	30

Fase 2: Priorización de los Dominios de la norma y selección de las políticas de seguridad informática

En la Tabla 3 se puede apreciar la importancia que establecieron los expertos a los 11 dominios.

Tabla 3. *Dominio*s y su importancia.

	Dominios	Importancia
1	Política de seguridad	Alta
2	Aspectos organizativos de seguridad de la información	Media
3	Gestión de activos	Media
4	Seguridad ligada a los recursos humanos	Baja
5	Seguridad física y del entorno	Alta
6	Gestión de comunicaciones y operaciones	Media
7	Control de acceso	Media
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	Baja
9	Gestión de incidentes de seguridad de la información	Media
10	Gestión de la continuidad del negocio	Media
11	Cumplimiento	Alta

Los dominios considerados de alta importancia son: “Políticas de Seguridad”, “Seguridad física y del entorno” y “Cumplimiento”, los dominios considerados de baja importancia son: “Seguridad ligada a los recursos humanos” y “Adquisición, desarrollo y mantenimiento de los sistemas de información”. La priorización de los Dominios de la norma se puede apreciar en la Tabla 4.

Tabla 4. Priorización de los *dominios*.

Dominios	Cumplimiento	Importancia	Prioridad
Política de seguridad	Bajo	Alta	Alta
Aspectos organizativos de seguridad de la información	Medio	Media	Media
Gestión de activos	Medio	Media	Media
Seguridad ligada a los recursos humanos	Medio	Baja	Baja
Seguridad física y del entorno	Medio	Alta	Alta
Gestión de comunicaciones y operaciones	Medio	Media	Media
Control de acceso	Medio	Media	Media
Adquisición, desarrollo y mantenimiento de los sistemas	Medio	Baja	Baja
Gestión de incidentes de seguridad de la información	Medio	Media	Media
Gestión de la continuidad del negocio	Medio	Media	Media
Cumplimiento	Bajo	Alta	Alta

Como resultado del análisis, las políticas de seguridad informática específicas que se consideran necesarias de implementar en la DTIC fueron seleccionadas de acuerdo con las prioridades (alta y media) de los *dominios*, las políticas son las siguientes: 1) Acceso a la información de las aplicaciones de producción; 2) Registros en sistemas y aplicaciones sensibles; 3) Registros de auditoría en los

sistemas; 4) Prueba e información del software; 5) Controles de datos de salida; 6) Funcionalidad de los sistemas; 7) Documentación de cambios en sistemas de producción; 8) Documentación de adiestramiento y operaciones; 9) Intentos de introducir contraseña; 10) Registro de intentos de acceso; 11) Protección de la información; 12) Manejo, acceso y uso de la información; 13) Revocación de privilegios de acceso; 14) Computadores portátiles con información sensible; 15) Propiedad de la información; 16) Acceso de lectura a información sensible; 17) Comité de gestión de seguridad informática; 18) Acuerdos de confidencialidad; 19) Preparación y mantenimiento de planes de contingencia; 20) Accesibilidad del plan de contingencia; 21) Prueba del plan de contingencia; 22) Pruebas de honestidad y estabilidad emocional; 23) Revisión de antecedentes; 24) Destrucción de información; 25) Conciencia del usuario sobre registros de violaciones de seguridad; 26) Estructura de las contraseñas; 27) Informes de incidentes; 28) Acceso físico para terceros.

El tiempo, estrategia, procedimiento que se utilice para implementar, revisar y verificar el correcto cumplimiento de las políticas de seguridad antes descritas va a ser responsabilidad del director de la DTIC y de las autoridades universitarias.

4. DISCUSIÓN

Como indican Tirado, Ramos, Álvarez, & Carreño (2017), el término de seguridad informática ha sido objeto de estudio por varios expertos informáticos y algunos autores de artículos, quienes llegan a la conclusión que "la seguridad informática está conformada por un conjunto de medidas y procedimientos para garantizar que la información siempre esté disponible, manteniendo la integridad y confidencialidad de los datos". Para esto se deben de cumplir con estándares de seguridad y que sólo el personal autorizado pueda acceder a la información.

Los resultados del presente trabajo revelan que, en primer lugar, no se da la debida atención a la selección e implementación de políticas de seguridad informática específicas, porque se encontró que existen políticas definidas de manera general, una posible explicación puede ser el desconocimiento de la importancia que tienen las políticas en la seguridad informática. Por citar un ejemplo, se evidenció que no existe una política específica para definir las claves de acceso, tiempo de vigencia, complejidad; lo que puede generar una vulnerabilidad ya que los hackers pueden utilizar ataques de fuerza bruta implementando técnicas de ataques de diccionario para adivinar las contraseñas de los usuarios como lo indica Gómez (2011).

En segundo lugar, al no tener definidas políticas de seguridad específicas según las necesidades de la DTIC, no se realiza un adecuado control y verificación de cumplimiento. De nada sirve disponer de políticas específicas y dejarlas en el olvido, muchas de las amenazas de seguridad tienen que ver con el factor humano, por ejemplo, el desconocimiento, negligencia, ingeniería social; un usuario que haga caso omiso de las políticas de seguridad pone en riesgo a la universidad. Una posible explicación también puede ser el desconocimiento de la importancia que tiene la verificación del cumplimiento, ya que las políticas no son eternas y necesitan ser revisadas, evaluadas y modificadas. Solarte, Enríquez, & Benavides (2015) dicen que otra vulnerabilidad a considerar es la desorganización del área informática, ausencia de responsabilidades, falencias en los manejos de los activos informáticos que pueden experimentar algunas organizaciones.

En tercer lugar, se pudo evidenciar que la DTIC tiene inconvenientes para garantizar la continuidad del negocio en el momento que exista interrupciones del servicio, uno de los motivos puede ser la falta controles adecuados para disponer en lugares seguros los manuales de usuario, manuales técnicos, planes de contingencia; estos documentos deben estar actualizados, revisados y disponibles en todo momento. Avalos & Gómez (2015) indican que la amenaza de negación de servicios, conocida como Denial of Services (DoS), se ha vuelto muy utilizada en la actualidad, la cual tiene como principal objetivo atacar una red de computadoras causando que los servicios sean inaccesibles para los usuarios, dicho ataque genera pérdida total de conectividad a la red por el aumento excesivo del consumo de ancho de banda.

En cuarto lugar, cuando se habla de la seguridad informática en una organización se la ha relacionado exclusivamente con la implementación de mecanismos de control sean físicos y lógicos, en la DTIC no es la excepción ya que se han dejado a un lado aspectos muy importantes como es el factor humano, que puede ser la parte más vulnerable si no se le da la debida atención y pueden ser víctimas, por ejemplo, de las amenazas intencionales (robo de información, propagación de código malicioso, ingeniería social), y las amenazas no intencionales (negligencia, desastres naturales) (Universidad Luján, 2015).

5. CONCLUSIONES

Como ya se mencionó en el punto anterior unos de los principales problemas que tiene la DTIC es disponer de pocas políticas de seguridad informática, la mayoría de las políticas son desconocidas por el personal técnico y por los usuarios finales; las autoridades universitarias deben establecer, aprobar, difundir y verificar el correcto cumplimiento de cada una de las políticas establecidas tanto para el personal técnico como para los usuarios finales. La metodología aplicada en el presente trabajo nos da una visión general y detallada de las vulnerabilidades que tiene actualmente la DTIC, en base a los porcentajes de cumplimiento de cada uno de los 133 controles de la norma, identificando los porcentajes de cumplimiento bajo y facilitando el diseño de las políticas de seguridad informática indispensables que ayudarán a tomar correctivos en aquellos puntos débiles que tiene el establecimiento. El uso de los controles de la norma NTE INEN-ISO/IEC 27002:2009 facilita realizar un levantamiento de información y seleccionar las medidas correctivas, como, por ejemplo, políticas de seguridad informática. La implementación de la norma no requiere muchos conocimientos avanzados en seguridad informática, ya que, al ser un estándar, con una lista completa de controles de seguridad, esaplicable a cualquier tipo de establecimiento, sea público o privado. Como ya se mencionó anteriormente, la selección de los controles necesarios que ayudarán a mejorar la seguridad informática dependerá directamente de los objetivos que se proponga alcanzar cada institución.

AGRADECIMIENTOS

Un agradecimiento a todo el personal que labora en la DTIC de la Universidad de Cuenca por la apertura para realizar el trabajo de investigación.

REFERENCIAS

Avalos, H., Gómez, E. (2015). Seguridad de la información, generación y mitigación de un ataque de denegación de servicios. *Revista Tecnológica ESPOL*, *28*(5), 54-72. Disponible en http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/425

Baldeón, M., Coronel, C. (2012). *Plan maestro de seguridad informatica para la UTIC de la ESPE con lineamientos de la Norma SO/IEC 27002*. Maestría Gerencia de Sistemás. ESPE. http://repositorio.espe.edu.ec/handle/21000/6025

Cabero, J., Infante, A. (2014). Empleo del método Delphi y su empleo en la investigación en Comunicación y Educación. *EDUTEC*, *48*, 1-16. Disponible en https://idus.us.es/xmlui/bitstream/handle/11441/32234/edutec-e_n48_cabero-infante.pdf?sequence=1&isAllowed=y

Chavez, A. (2009). *Seguridad informática*. Informe, CLACSO, Universidad de Buenos Aires.

Dussan, C. (2006). Políticas de seguridad informática. *Entramado*, *2*(1), 86-92. Disponible en http://www.redalyc.org/pdf/2654/265420388008.pdf

Gómez, A. (2011). *Gestión de incidentes de seguridad informática* (1ª ed.). 128 p. Madrid, España: Starbook Editorial.

Ishizaka, A., Nemery, P. (2013). *Multi-criteria decision analysis: Methods and software*. 310 p. Wiley.

Lanche, D. S. (2015). *Diseño de un sistema de seguridad de la información para la Compañía Acotecnic Cía. Ltda. basado en la norma NTE INEN ISO/IEC 27002*. Tesis de Maestría en Telematica, Universidad de Cuenca, Cuenca, Ecuador, 181 p.

LEXIS S.A. (2004). *Ley orgánica de transparencia y acceso a la información publica.* Ley 24, Registro Oficial Suplemento 337 de 18-may.-2004. 13 pp. Disponible en https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Medina, J., Ortiz, F., Franco, C., Aranzazú, C. (2010). *Matriz de priorización para toma de decisiones*. Facultad de Ciencias de la Administración, Universidad de Valle, Cali, Colombia. 23 p. Disponible en http://sigp.sena.edu.co/soporte/Plan/03_Matriz%20de%20priorizacion

Mosquera, L., Andrade, D., Sierra, L. (2013). Guía para apoyar la priorización de riesgos en la gestión de proyectos de tecnologías de la información. *Revista Gerencia Tecnológica Informáti*ca, *12*(33), 15-32. Disponible en http://revistas.uis.edu.co/index.php/revistagti/article/view/3550/3650

Romo, D., Valarezo, J. (2012). *Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil*. Tesis pregrado, Facultad de Ingeniería, Universidad Politécnica Salesiana, Guayaquil, Ecuador, 183 p. Disponible en https://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

Solarte, F., Enriquez, E., Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*, *28*(5), 492-507.

Solórzano, L. S., Rezabala, J. (2013). *Estudio sobre el estado del arte de la seguridad informática en el Ecuador*. Artículos de Tesis de grado, Facultad de Ingeniería en Electricidad y Computación, ESPOL, 8 pp. Disponible en https://www.dspace.espol.edu.ec/handle/123456789/24298

Tirado, N. R., Ramos, D., Alvarez, E., Carreño, S. (2017). Seguridad informática, un mecanismo para salvaguardar la información de las empresas. *Revista Publicando, 4*(10), 462-473. Disponible en https://www.rmlconsultores.com/revista/index.php/crv/article/viewFile/367/pdf_332

Universidad Luján. (2015). *Amenazas a la seguridad de la información*. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Wood, C. C. (2002). *Políticas de seguridad informática - Mejores prácticas internacionales* (Versión 9). Houston, TX, USA: NetIQ, Inc.