ROCA
revista científico - educacional de la provincia Granma.

RPNS: 2090 | **ISSN**: 2074-0735

Volumen 16 (2020)

ORIGINAL

El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador).

Janeth Mora Secaira. [jmora@uteq.edu.ec]
Universidad Técnica Estatal de Quevedo. Ecuador.

Raúl Díaz Ocampo. [rdiaz@uteq.edu.ec]
Universidad Técnica Estatal de Quevedo. Ecuador.

Emilio Zhuma Mera. [ezhuma@uteq.edu.ec]
Universidad Técnica Estatal de Quevedo. Ecuador.

Igor Ernesto Díaz Kovalenko. [ie.diazk@uea.edu.ec]
Universidad Estatal Amazónica. Ecuador.

Resumen

Con el objetivo de describir una metodología para un Sistema de Gestión de Seguridad de la Información (SGSI) para instituciones de educación superior del Ecuador, bajo la norma NTE INEN-ISO/IEC 27001, la cual será de utilidad en el momento de su aplicación y facilitará el desarrollo de las fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar) a nivel institucional. Se tomó como referente a la Universidad Técnica Estatal de Quevedo (UTEQ), se identificaron los procesos claves de la universidad estudio de caso, se identificaron y clasificaron los activos de información y controles que permitieron contextualizar los alcances del SGSI según la norma ISO 27001 y que permitirán a la UTEQ organizar, diseñar y gestionar de manera sistemática su SGSI, plantear estrategias de cambio y mejora, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades. Finalmente, la aportación de este estudio es una propuesta para la puesta en práctica del Sistema de Gestión de Seguridad de la Información (SGSI) en la UTEQ, que contempla una serie de políticas y procedimientos teniendo en cuenta los hallazgos identificados, tales como el procedimiento de la organización de la estructura, un plan de concienciación y capacitación, políticas específicas de seguridad de la información y un plan de continuidad del negocio; los cuales deben ser implementados a fin de que contribuyan al mejoramiento de los niveles de confidencialidad, integridad y disponibilidad de la información de la UTEQ.

Palabras claves: estructura; procedimientos; sistemas de información; vulnerabilidades.

Recibido: 12/11/2019 | **Aceptado**: 25/01/2020

The information security management system under the NTE ISO / IEC 27001 standard in Institutions of Higher Education (Ecuador).

Abstract

With the objective of describing a methodology for an Information Security Management System (ISMS) for higher education institutions in Ecuador, under the NTE INEN-ISO / IEC 27001 standard, which will be useful at the time of its application and will facilitate the development of the phases of the PHVA cycle (to Plan, to Do, to Verify and to Act) at the institutional level. It was taken as a reference to the State Technical University of Quevedo (STUQ), the key processes of the case study university were identified, the information assets and controls that allowed contextualizing the scope of the ISMS according to ISO 27001 and that will allow STUQ to organize, to design and to manage systematically its ISMS, propose strategies for change and improvement, value and insure its assets from possible risks and vulnerabilities. Finally, the contribution of this study is a proposal for the implementation of the Information Security Management System in the STUQ, which includes a series of policies and procedures taking into account the identified findings, such as the procedures for the organization of the structure, an awareness and training plan, specific policies of information of the security and a business continuity plan; which must be implemented in order to contribute to the improvement of the levels of confidentiality, integrity and availability of the STUQ information.

Keyword: structure; procedures; information systems; vulnerabilities.

Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) han dotado al mundo actual de un sinnúmero de posibilidades que le permiten al ser humano gozar de comodidad y rapidez en sus procesos cotidianos, sin embargo, a raíz de estos adelantes tecnológicos también surge la necesidad de proteger y salvaguardar los sistemas informáticos a nivel de software, hardware y datos, de amenazas y vulnerabilidades que impidan su correcto funcionamiento y puedan afectar la integridad, disponibilidad y confidencialidad de la información.

La información es uno de los activos más importantes para las universidades y por lo tanto debe ser protegido de forma adecuada. La seguridad de la información gira en torno a los conceptos de confidencialidad, integridad y disponibilidad de información (Whitson, 2003) y en los últimos años se ha incrementado su importancia en las organizaciones modernas, entre ellas en las instituciones de educación superior (Marks, 2007; Okibo y Ochiche, 2014, Bongiovanni, 2019).

Los estudiantes, profesores, personal administrativo y visitantes acceden regularmente a las infraestructuras de TI de las universidades para consumir y producir datos, de manera

multimodal: desde teléfonos móviles personales, a través de computadoras portátiles corporativas y tabletas, sensores de laboratorio y sistemas de tarjetas de acceso deslizante, el intercambio de datos entre universidades como organizaciones y sus diferentes categorías de usuarios finales es continuo (Bongiovanni, 2019).

La implementación de un SGSI se encuentra determinada por la estructura organizacional de las instituciones, lo cual abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001.

Se requiere el diseño de una metodología que les permita a las universidades identificar su estado actual en cuanto a seguridad informática y realizar los procesos para implementar su propio SGSI y a suvez complementar sus procesos de certificación de calidad ISO91001. De ahí que el objetivo fue describir una metodología para un Sistema de Gestión de Seguridad de la Información (SGSI) para instituciones de educación superior del Ecuador, bajo la norma NTE INEN-ISO/IEC 27001.

Población y muestra

El presente estudio se llevó a cabo empleando diferentes aproximaciones metodológicas, en primer lugar, se realizó una revisión de literatura existente en el campo de estudio elegido. Una vez recopilada toda la información relacionada con el estado del arte del tema se aplicaron métodos de investigación para el logro de los objetivos de investigación planteados, tales como encuestas y entrevistas a informantes de calidad, un estudio de caso que investiga fenómenos en el contexto real cotidiano conforme se desarrollan. La combinación de los diferentes métodos de investigación citados de manera sistémica, permite obtener conclusiones más robustas.

Partiendo de lo planteado, se presenta en este trabajo el desarrollo de una metodología basada en la Norma NTE INEN ISO IEC 27001 para la implementación de un Sistema de Gestión de Seguridad de la Información, se exploraron los problemas de seguridad de la información en la IES seleccionada, utilizando un enfoque estructurado al abordar la organización a través de un análisis cualitativo de los contenidos provenientes de los documentos seleccionados y a partir de las entrevistas a informantes de calidad,en primer término se analizó la estructura organizacional de la UTEQ.

La implementación de un SGSI deberá ser asumida con una visión sistémica, donde existan roles y responsabilidades bien definidos con miras al éxito del proceso. En la presente metodología se propone la selección de los siguientes roles: comité de seguridad de la

información, equipo de proyecto y director de proyecto.

Análisis de los Resultados

Fases y actividades de la metodología para la implementación la implementación del sistema de gestión de la seguridad de la información

La metodología que se propone para la implementación del SGSI en la UTEQ se basa en el ciclo de mejora continua PHVA de la norma NTE ISO/IEC 27001. Las fases y sus actividades para la aplicación de la metodología propuesta:

Tabla 1. Fases y Actividades ciclo PHVA - SGSI

FASES CICLO PHVA	ACTIVIDADES
Planear	• Determinación del alcance del SGSI • Definición de la política de seguridad de la información • Diseño del método de evaluación de riesgos. • Inventario de Activos. • Valoración de los activos. • Identificar amenazas y vulnerabilidades. • Identificar el impacto. • Análisis y evaluación de riesgos. • Selección de los controles. • Estado de aplicabilidad, definición de controles y excepciones
Hacer Verificar	• Plan de acción para el tratamiento de los riesgos. • Implementar el plan de tratamiento de riesgos • Implementar los controles • Formar y concienciar. Plan de Concienciación (capacitación y formación del personal). • Aplicar el SGSI • Revisar el SGSI • Medir la eficacia de los controles. Seguimiento de objetivos marcados. • Revisar los riesgos residuales • Realizar auditorías internas del SGSI. Programas de auditorías. • Registrar eventos y acciones
Actuar	• Implementar mejoras al SGSI. Mejoramiento y actualización SGSI. • Aplicar acciones correctivas • Aplicar acciones preventivas • Comprobar la eficacia de las acciones • Plan de continuidad.

Fuente: Norma ISO 27001.

Planear

Alcance del SGSI

La UTEQ tendrá que definir el alcance del SGSI en función de sus características como IES, localización, activos y tecnología utilizada en el desarrollo de sus funciones sustantivas: docencia, investigación y vinculación con la sociedad.

En el SGSI se identificarán las necesidades y expectativas de las partes interesadas que pueden ser internas o externas. Entre las partes interesadas internas se incluye a los estudiantes, profesores, administrativos, funcionarios de la universidad, personal de apoyo y terceros no vinculados directamente a la institución, que presten sus servicios y utilicen las TIC. Algunas partes interesadas externas pueden ser: proveedores, acreedores, gobiernos, sociedad u otros. Por otra parte en el SGSI también se incluyenlos activos informáticos, incluidos los equipos propios de la universidad o arrendados y a los equipos de personas externas que sean conectados a la red de la UTEQ.

Políticas del SGSI

Las políticas deben estar alineadas con los objetivos, características, ubicación, activos y tecnología de la UTEQ. Las políticas de seguridad son documentos que contienen reglas y principios para el logro de los objetivos de seguridad aplicados a los sistemas informáticos, su organización y buen uso.

El nivel de criticidad de los activos para la clasificación y valoración de los activos relacionados con el sistema de información, se lo hace en relación con los parámetros económicos, legal y prestigio.

Tabla 1. Valoración de activos

Orden	Identificación del activo	Confidencialidad			Integridad			Disponibilidad		
#	Activo	Económico	Legal	Prestigio	Económico	Legal	Prestigio	Económico	Legal	Prestigio
1	Servidores	4	2	4	4	2	3	4	2	3
2	Backbone LAN	4	3	3	4	2	2	4	2	3
3	LAN y Firewall	4	3	3	4	2	2	4	2	3
4	Telefonía IP	3	2	2	3	2	2	3	2	2
5	Equipos respaldos eléctrico	2	2	2	2	2	2	2	2	2
6	Sistema operativos servidores	4	2	3	4	2	3	4	2	3

7	Sistema operativos personal	3	2	2	3	2	2	3	2	2
8	Software institucional	3	2	3	3	2	3	3	2	3
9	Software académico (SGA)	4	2	4	4	2	4	4	2	4
10	Información carreras de grado	3	2	4	3	2	4	2	2	3
11	Información de investigación	3	2	4	3	2	4	3	2	4
12	Información de vinculación	3	2	4	3	2	4	3	2	4
13	Información carreras de posgrado	3	2	4	3	2	4	3	2	4
14	Información financiera	4	4	4	4	4	4	4	2	4
15	Información personal	4	4	4	4	4	4	3	2	3
16	Información institucional	4	3	4	4	3	4	3	2	3
17	World wide web	3	2	3	3	2	3	3	2	3
18	Correo electrónico	2	2	3	2	2	3	2	2	3
19	Página web	2	2	3	2	2	3	2	2	3
20	Proxy	4	4	4	4	4	4	4	2	4
21	Almacenamiento de ficheros	1	2	2	1	2	2	1	2	1
22	Unidad de TIC	4	2	3	4	2	3	4	2	3
23	Área de desarrollo de sistemas de información y administración de redes	3	3	3	3	2	3	3	2	3
24	Seguridad privada	4	3	3	4	3	3	4	2	3
25	Campus Central	4	4	4	4	4	4	4	4	4
26	Campus la María	4	3	4	4	4	4	4	3	4

La crediticidad se valora de la siguiente forma:

Muy Bajo = MB; Bajo = B; Medio = M; y Alto =A

Tabla 2. Consolidados de la valoración de activos

Identificación del activo	Confidencialidad			Integridad			Disponibilidad			Promedio			Crediticidad		
	Económico	Legal	Prestigio	Económico	Legal	Prestigio	Económico	Legal	Prestigio	Económico	Legal	Prestigio	Económico	Legal	Prestigio
Servidores	4	2	4	4	2	3	4	2	3	4	2	3	A	B	M
Backbone LAN	4	3	3	4	2	2	4	2	3	4	2	3	A	B	M
LAN y Firewall	4	3	3	4	2	2	4	2	3	4	2	3	A	B	M
Telefonía IP	3	2	2	3	2	2	4	2	2	3	2	2	M	B	M
Equipos respaldos eléctrico	2	2	2	2	2	2	2	2	2	2	2	2	B	B	B
Sistema operativos servidores	4	2	3	4	2	3	4	2	3	4	2	3	A	B	M
Sistema operativos personal	3	2	2	3	2	2	3	2	2	3	2	2	M	B	M
Software institucional	3	2	3	3	2	3	3	2	3	3	2	3	M	B	M
Software académico (SGA)	4	2	4	4	2	4	4	2	4	4	2	4	A	B	A
Información carreras de grado	3	2	4	3	2	4	2	2	3	3	2	4	M	B	A
Información de investigación	3	2	4	3	2	4	3	2	4	3	2	4	M	B	A
Información de vinculación	3	4	4	3	2	4	3	2	4	3	3	4	M	M	A
Información carreras de posgrado	3	2	4	3	2	4	3	2	4	3	2	4	M	B	A
Información financiera	4	4	4	4	4	4	4	2	4	4	3	4	A	M	A
Información personal	4	4	4	4	4	4	3	2	3	4	3	4	A	M	A
Información institucional	4	3	4	4	3	4	3	2	3	4	3	4	A	M	A
World wide web	3	2	3	3	2	3	3	2	3	3	2	3	M	B	M
Correo electrónico	2	2	3	2	2	3	2	2	3	2	2	3	B	B	M
Página web	2	2	3	2	2	3	2	2	3	2	2	3	B	B	M
Proxy	4	4	4	4	4	4	4	2	4	4	3	4	A	M	A
Almacenamiento de ficheros	1	2	2	1	2	2	1	2	2	1	2	2	MB	B	B
Unidad de TIC	4	2	3	4	2	3	4	2	3	4	2	3	A	B	M
Área de desarrollo de sistemas de información y administración de redes	3	3	3	3	2	3	3	2	3	3	2	3	M	B	M

Seguridad privada	4	3	3	4	3	3	4	2	3	4	3	3	A	M	M
Campus Central	4	4	4	4	4	4	4	4	4	4	4	4	A	A	A
Campus la María	4	3	4	4	4	4	4	3	4	4	3	4	A	M	A

Análisis de Riesgos

En esta etapa se deben identificar las amenazas asociadas a cada uno de los procesos de negocio, activos de información, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas.

A continuación, se identifican las amenazas a las que están expuestos los activos seleccionados de la UTEQ.

Tabla 3. Clasificación de amenazas

N°	Amenazas
Físicas	
1	Incendio
2	Inundaciones
3	Sismo
4	Polvo
5	Falta de ventilación
6	Sobrecarga eléctrica
7	Falla de corriente
8	Falla de sistema / daño disco duro
Usuario	
1	Falta de inducción, capacitación y sensibilización sobre riesgos
2	Mal manejo de softwares y herramientas
3	Pérdida de datos por error de usuario
Hardware	
1	Falla de hardware
2	Exposición o extravió de equipo, unidades de almacenamiento
3	Pérdida de datos por error hardware
4	Falta de mantenimiento físico y lógico

Datos	
1	Manejo inadecuado de datos críticos
2	Transmisión no cifrada de datos críticos
3	Divulgación
4	Uso no autorizado
Software	
1	Falta actualización, mantenimiento y soporte
2	Virus informáticos
3	Falta de actualización de firewall
Infraestructura	
1	Dependencia a servicio técnico externo
2	Red cableada expuesta para el acceso no autorizado
3	Red inalámbrica
4	Acceso
Políticas	
1	Falta de normas y procedimientos para riesgos
2	Falta de medios de verificación
3	Falta de políticas generales y específicas para la seguridad de la información

Elaboración: Propia

Se tendrá en cuenta además las vulnerabilidades:

Tabla 4. Identificación y clasificación de vulnerabilidades

N°	Vulnerabilidades
Físicas	
1	Desastres naturales
2	Inadecuada prevención contra incendio/detección
3	Desastres provocados por el hombre
4	Abastecimiento de energía eléctrica inestable
5	Abastecimiento de aire
Usuario	
1	Falta de cultura de seguridad
2	Falta de políticas, normas y procedimientos

3	Control inadecuado de selección de personal
4	Falta de capacitaciones
Hardware	
1	Falla de hardware y sus componentes
2	Climatización no adecuada
3	Suministro eléctrico
4	Incompatibilidades de unidades de hardware
5	Falta de mantenimiento no planificado
Datos	
1	Susceptibilidad de daños en almacenamiento de medios
2	Control inadecuado de base de datos
3	Respaldo de datos
4	Abusos de privilegios
5	Autenticación débil
Software	
1	Instalación / desinstalación no controlada
2	Sistemas operativos sin parches o desactualizados
3	Falta de protección contra virus y código malicioso
4	Administración de configuraciones inadecuadas
5	Plugins desactualizados
Infraestructura	
1	Monitoreo insuficiente de medidas de seguridad para infraestructura
2	Mantenimiento a la infraestructura

Una vez realizada la valoración de los riesgos para todos los activos involucrados dentro del alcance del SGSI, se debe precisar el nivel de riesgo aceptable por la universidad. Este nivel sirve como indicador, definiendo que todos los activos con algún riesgo por encima de este valor deben ser tratados de alguna forma para ser mitigados, eliminados o aceptados.

Revisión del SGSI

La Norma ISO 27001 establece la revisión periódica del SGSI, por lo menos una vez al año, para establecer el grado de eficacia y pertinencia del sistema en concordancia con los objetivos

de la IES. Esta revisión permite el análisis del sistema, detección de fortalezas, debilidades y la toma de decisiones en cuanto a planes de mejoras. Para ello, se requiere la siguiente documentación:

- Resultados de auditorías internas o externas e informes de revisiones del SGSI
- Sugerencias y recomendaciones otorgadas por las partes interesadas (estudiantes, administrativos, profesores y personal externo)
- Procesos, procedimientos o técnicas que pudieran ser útiles para mejorar el nivel de eficiencia y eficacia del SGSI
- Informes sobre el estado de acciones preventivas y correctivas realizadas al SGSI
- Registros de vulnerabilidades o amenazas que no se hayan tratado adecuadamente en evaluaciones de riesgos anteriores
- Informesyestadodelasaccionesiniciadascomoproductoderevisionesanterioresal SGSI
- Cambios realizados en la organización y que pueden afectar al SGSI
- Recomendaciones establecidas por otros organismos externos.

Actuar

En esta última fase, se implementan las medidas correctivas y planes de mejora obtenidos como resultado de la verificación del SGSI, algunas de las actividades que se deben realizar en esta etapa corresponden a:

- Mantener y mejorar el SGSI
- Definir planes de acción en cuanto a medidas correctivas, preventivas y planes de contingencia
- Identificar las no conformidades encontrada en el SGSI, producto de las auditorías internas
- Aplicar los planes de mejoramiento al SGSI, propuesto en la fase de verificación
- Realizar análisis y estudio de casos y análisis de causa-efecto
- Implementación de cambios propuestos y ejecución de recursos asignados
- Evaluar la efectividad de los planes de mejora del SGSI, teniendo en cuenta los resultados de acciones implementadas anteriormente
- Comunicar las acciones de mejora del SGSI a las partes interesadas
- Actualizar los planes de seguridad en los sistemas informáticos
- Verificar la correcta implementación de las mejoras propuestas al SGSI

Estarán involucrados en la fase de actuar, los directivos de la UTEQ, así como personal administrativo, profesores y estudiantes.

PROPUESTA

Estructuración de la organización de la seguridad de la información

La UTEQ no cuenta con una estructura adecuada para la implementación del SGSI, la Unidad de TIC tiene problemas en la estructuración de los cargos del departamento como ser auditores de sus propias responsabilidades, lo cual hace evidente la necesidad de contar con un área específica de Seguridad de la Información y la actualización, aprobación y difusión de las políticas específicas de seguridad de la información

Al momento la UTEQ cuenta con una política de seguridad de la información, sin embargo, se requiere su actualización y por otra parte, definir las políticas específicas en materia de seguridad de la información en las siguientes áreas:

1. De equipos
    - Instalación de equipos de computación en los laboratorios
    - Mantenimiento de equipos de computación
    - Reubicación de equipos de computación
2. Control de acceso
    - Acceso a Áreas Críticas
    - Control de acceso al equipo de computación en los laboratorios
    - Control de acceso local a la red
    - Control de acceso remoto
    - Acceso a los sistemas administrativos
3. Utilización de los recursos de la red
    - Administrar, mantener y actualizar la infraestructura de la red
    - Confidencialidad en el uso de los recursos de la red
4. Software
    - Adquisición del software
    - Instalación del software
    - Actualización del software
    - Auditoría de software instalado
    - Software propiedad de la institución
    - Uso de software de la institución
5. Supervisión y Evaluación
    - Auditorías en aspectos de seguridad lógica y física de la red

- Monitorización constante de los servicios de internet e intranet

Plan de Concienciación y Capacitación sobre seguridad de la información

La implementación de un plan de concienciación dirigido a estudiantes, personal académico y/o administrativo, se considera como uno de los aspectos fundamentales, a fin de generar una cultura de seguridad de la información.

El citado plan debe abordar la capacitación en los siguientes aspectos: políticas de seguridad de la información de la IES, Reglamento de Régimen Académico del CES, la Ley Orgánica de Educación Superior del Ecuador y Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas del CACES 2019.

Plan de Continuidad del Negocio

En las instituciones de educación superior, es recomendable poseer un plan de continuidad ante situaciones que no se puedan evitar, el citado plan no puede faltar ya que tiene como objetivo que la IES esté preparada ante situaciones imprevistas, pueda contrarrestar las interrupciones de las actividades normales y esté en condiciones de garantizar su reanudación oportuna.

Un plan de continuidad del negocio debe presentar las siguientes características:

- El plan se enmarcará en un proceso de mejora continua.
- Su orientación será hacia la recuperación de los procesos considerados como críticos por la IES.
- La seguridad de la información debe estar integrada en los sistemas de gestión de la continuidad del negocio de la organización.
- Su diseño deberá estar integrado al resto de elementos de la seguridad.
- Tener un conjunto de tareas planificadas, para actuar en el momento de crisis.

Conclusiones

1. En la actualidad, la UTEQ no cuenta con un SGSI que permita la seguridad de la información, no existen políticas de seguridad definidas para la protección, cuidado y continuidad del negocio en caso de materializarse una catástrofe que conlleve a la pérdida de la información generada a diario por cada una de las áreas académicas y administrativas involucradas.
2. El establecimiento de una metodología de sistema de gestión de seguridad de la información basado en la norma NTE ISO/IEC 2700, proporciona una línea base para garantizar la disponibilidad, integridad y confidencialidad de la información sensible de la IES, a la vez que permite cumplir con los estándares de calidad de la información.

Referencias bibliográficas

Asamblea Nacional. (2008) Constitución de la República del Ecuador. Obtenido de: http://www.estade.org/legislacion/normativa/leyes/constitucion2008.pdf

Bongiovanni, I., (2019).The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security. 86: 350-357

CACES. (2019). Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas. Obtenido de: https://www.caces.gob.ec/documents/20143/714527/3.+Modelo_Eval_UEP_2019_compressed.pdf/486dba29-6d71-f1e0-a3f1-01f6ecdceae8

CES. (2013). Reglamento de Régimen Académico. Ecuador. Obtenido de: http://www.ces.gob.ec/lotaip/2018/Enero/Anexos%20Procu/An-lit-a2-Reglamento%20de%20R%C3%A9gimen%20Acad%C3%A9mico.pdf

CES. (2018). Ley Reformatoria a la Ley Orgánica de Educación Superior. Ecuador

Esquema Gubernamental de la Seguridad de la Información."(2014).

Instituto Ecuatoriano de Normalización. (2016). Obtenido de http://www.normalizacion.gob.ec/wp content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Ley Orgánica de Educación Superior. (2018). Registro Oficial Suplemento 298. Quito, Ecuador. 30p.

Marks, A.A., (2007). Exploring universities' Information Systems Security Awareness in a Changing Higher Education Environment: a Comparative Case Study Research. University of Salford.

Ministerio de Finanzas del Ecuador, (2018) "Acuerdo Ministerial No. 209, Implementación del Plan Estratégico de Desarrollo Institucional UTEQ 2018-2020.

Norma UNE ISO/IEC 27001:2013. (1 de octubre de 2013). Segunda, 30

Okibo, B.W., Ochiche, O.B., (2014). Challenges facing information systems security management in higher learning Institutions: a case study of the catholic university of eastern Africa-Kenya. Int. J.f Manage. Excell. 3 (1), 336–349

Secretaría Nacional de la Administración Pública del Ecuador, "Esquema Gubernamental de Seguridad de la Información EGSI," (2013).

Whitson, G., (2003). Computer security: theory, process and management. J. Comput. Sci. Colleges 18 (6), 57–66.