PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002

Mauricio Baldeón Garzón[1], Christian Coronel Guerrero[2]

1 UTIC, ESPE, Ecuador, mjbaldeon@espe.edu.ec

2 UTIC, ESPE, Ecuador, cacoronel@espe.edu.ec

RESUMEN: *La Seguridad de la Información (S-I) es algo más que un antivirus, cortafuego o cifrado de datos, la S-I es el resultado de operaciones realizadas por personas y que son soportadas por la tecnología (Gonzalo Álvarez Marañon, Pedro Pablo Pérez García, 2004); bajo este contexto, la Escuela Politécnica del Ejército (ESPE) desde el año 2010 ha realizado adquisiciones considerables de equipamiento de seguridad perimetral y software de altas prestaciones, requiriéndose definir políticas, normas, procedimientos y controles que permitan gestionar correctamente los principios de la S-I (integridad, disponibilidad y confiabilidad).*

El objetivo principal de esta investigación es presentar una propuesta formal para implementar políticas y controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 enfocado a dos procesos de la UTIC: Base de Datos y Redes y Comunicaciones. Se pretende entregar una guía flexible, coherente e integral que permitirá minimizar o eliminar los ataques, vulnerabilidades, desastres naturales o disturbios sociales que destruyan la información, poniendo en peligro inminente a la Institución. Se propone un acercamiento a la metodología OCTAVE para gestionar el riesgo y a la norma de seguridad ISO/IEC 27002. Se realizó un estudio real de las políticas, procesos, controles, planes y manuales existentes en la UTIC, para culminar con el Plan Maestro de Seguridad Informática con lineamientos de la norma ISO/IEC 27002. La utilización de estas políticas y controles permitirán ofrecer servicios de tecnología de calidad acorde a las exigencias Institucionales y tendencias Mundiales.

Palabras clave: Seguridad de la Información (S-I), OCTAVE, ISO/IEC 27002, UTIC.

ABSTRACT: *Information Security (I-S) is more than one antivirus, firewall and data encryption, the I-S is the result of operations carried out by people and that are supported by technology (Gonzalo Álvarez Marañón, Pedro Pablo Pérez García, 2004), in this context, the Army Polytechnic School (ESPE) since 2010 has made substantial purchases of perimeter security equipment and high-performance software, requiring define policies, standards, procedures and controls to manage properly the principles of SI (integrity, availability and reliability).*

The main objective of this research is to present a formal proposal to implement policies and controls best practices recommended by the ISO/IEC 27002 to two processes UTIC: Database and Networking and Communications. It attempts to provide a flexible, consistent and comprehensive which will minimize or eliminate attacks, vulnerabilities, natural disasters or civil unrest destroy information, imminently endangering the institution. We propose an approach to the OCTAVE methodology for managing risk and safety standard ISO / IEC 27002. Secondly, a real study of the policies, processes, controls, plans and manuals in UTIC, culminating in the Master Plan guidelines I-S with ISO/IEC 27002. The use of these policies and controls allow technology to offer quality services in line with Institutional requirements and Global trends.

Keywords: Information Security (I-S), OCTAVE, ISO/IEC 27002, UTIC.

I. Introducción

Las actividades de administrativas, de docencia, investigación y vinculación con la colectividad que se realizan en la ESPE dependen en mayor medida de las Tecnologías de la Información (TI). Esto se da porque se obedece directamente a una sociedad moderna cada vez más exigente de

conocimientos, habilidades y desafíos científicos. Teniendo en cuenta los siguientes escenarios: el entorno de TI actual, el aumento de normas y estándares de TI, y el enfoque de posicionar a la ESPE entre las mejores universidades del Ecuador y de Latinoamérica, el objetivo principal de esta investigación desemboca en poner en manifiesto el gran valor de la aplicación de las mejores prácticas de TI basadas en políticas y controles, con el fin de lograr la alineación de la seguridad de la información con los requerimientos del negocio. En este contexto, la UTIC de la ESPE ha sido gestor de proyectos estratégicos ambiciosos que han logrado alcanzar una adecuada infraestructura tecnológica, la cual permite que el interés institucional y de la comunidad politécnica estén a la vanguardia del país, razón por la cual se requiere de un cuerpo debidamente estructurado de normas reguladoras, procedimientos, reglas y buenas prácticas que garanticen plenamente la disponibilidad, integridad y confiabilidad de la Información. La UTIC, actualmente dispone de procedimientos dispersos referente a seguridad informática entre las diferentes unidades de la UTIC, en un esfuerzo por minimizar el impacto tecnológico ante la falta de una política institucional.

Por tanto, esta investigación se enfoca en el uso de los controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 para fortalecer la S-I en la ESPE con el fin de coordinar y armonizar el trabajo de las diferentes unidades de la UTIC hacia el logro de un objetivo exclusivo que es: "la entrega de servicios de TI con calidad y excelencia".

II. Metodología

Las mejores prácticas de TI y el uso de políticas y controles son muy importantes dentro de las organizaciones, ya que no sólo mejoran la gestión de las TI, lo cual es esencial para alcanzar objetivos estratégicos institucionales, sino también que permiten una gestión eficaz de las actividades que realiza el personal de TI. Para poder generar un plan maestro de S-I bajo el estándar ISO/IEC 27002 para la UTIC, esta investigación se alineo en las siguientes etapas:

A. Definir la Seguridad de la Información

La seguridad informática concierne a la protección de la información que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema (CYBSEC S.A., 2011). La S-I se enmarca en 3 principios fundamentales "Integridad-Confidencialidad-Disponibilidad", los mismos que son un conjunto de políticas y mecanismos que permiten garantizar los recursos de los sistemas. Se puede definir entonces, que la misión de la S-I es garantizar la protección de sus activos y su información sensible y crítica que la integran e interactúan, para ofrecer servicios que permiten la gestión del negocio y las operaciones de una manera oportuna, confiable y segura, y que redunda en calidad para sus clientes, proveedores y empleados.

Lamentablemente, los problemas experimentados por motivos de seguridad van desde ataques externos, hasta incidencias en el interior de la propia organización, como aquellas provocadas por empleados que borran archivos críticos o acceden a información confidencial. En ese contexto, la seguridad información resulta vital en las organizaciones, mientras que la materialización de los riesgos y vulnerabilidades pueden significar millonarias pérdidas y comprometer su continuidad.

Hoy en día las unidades educativas no están libres de estos ataques informáticos, como lo muestra un análisis al sitio web www.zone-h.org donde se realiza una investigación estadística que muestra un total de 308 ataques exitosos realizados a páginas web de instituciones académicas desde el 2002. Como objeto de este estudio, en la Figura 1 se visualiza que la pagina web de la ESPE fue atacada el 15 de Abril del 2012. Zone-h es una organización en la que se puede visualizar las "hackeadas" que han tenido los sitios web de las organizaciones.

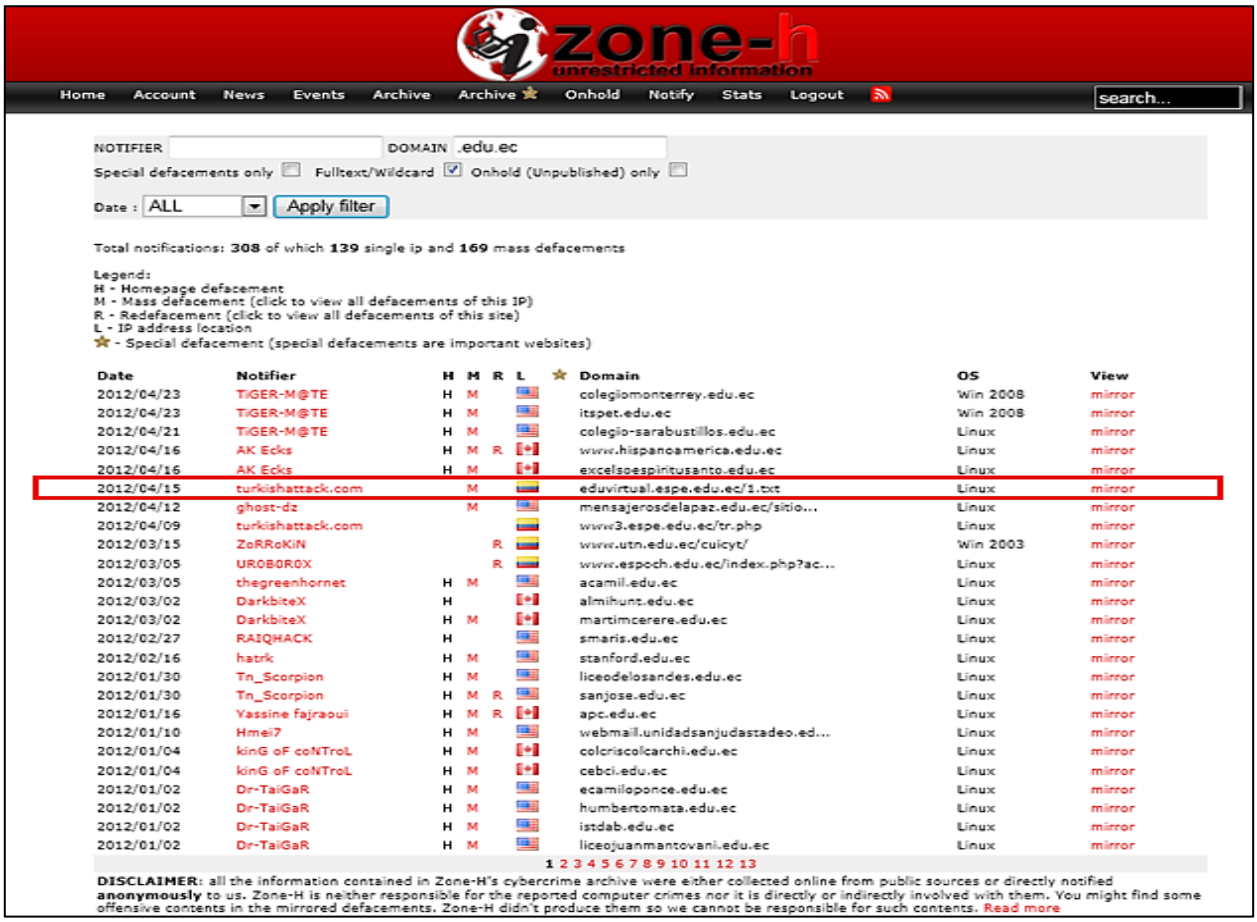

Figura 1: Páginas educativas del Ecuador atacadas (www.zone-h.org)

B. Definir el Riesgo

La norma ISO/IEC TR 13335-1, define al Riesgo como: "El potencial de que una amenaza dada explote las vulnerabilidades causando pérdida o daño a un activo o grupos de activos, y en consecuencia de esto directa o indirectamente a la organización".

a. Análisis del Riesgo

Para minimizar el riesgo se realiza un análisis y administración del mismo aplicando efectivamente medidas de seguridad según las amenazas, vulnerabilidades y el valor de los activos a ser protegidos. Del análisis realizado se puede entonces identificar, cuantificar y evaluar el posible daño que estos pueden causar en una organización y justificar las medidas de seguridad que deben implementarse en la misma.

b. Gestión del Riesgo

Luego de que los riesgos sean identificados y catalogados; se puede tomar las siguientes alternativas: aceptarlo, transferirlo, mitigarlo (implementando políticas de seguridad) y evitarlo eventualmente., estas alternativas serán determinadas por la relación costo/riesgo.

c. Metodología OCTAVE

Es una metodología para la búsqueda de la S-I basada en el análisis estratégico del riesgo y la planeación de una técnica para su implementación. El Método OCTAVE utiliza un enfoque de tres fases para examinar aspectos organizacionales y de tecnología como lo muestra la Figura 2.

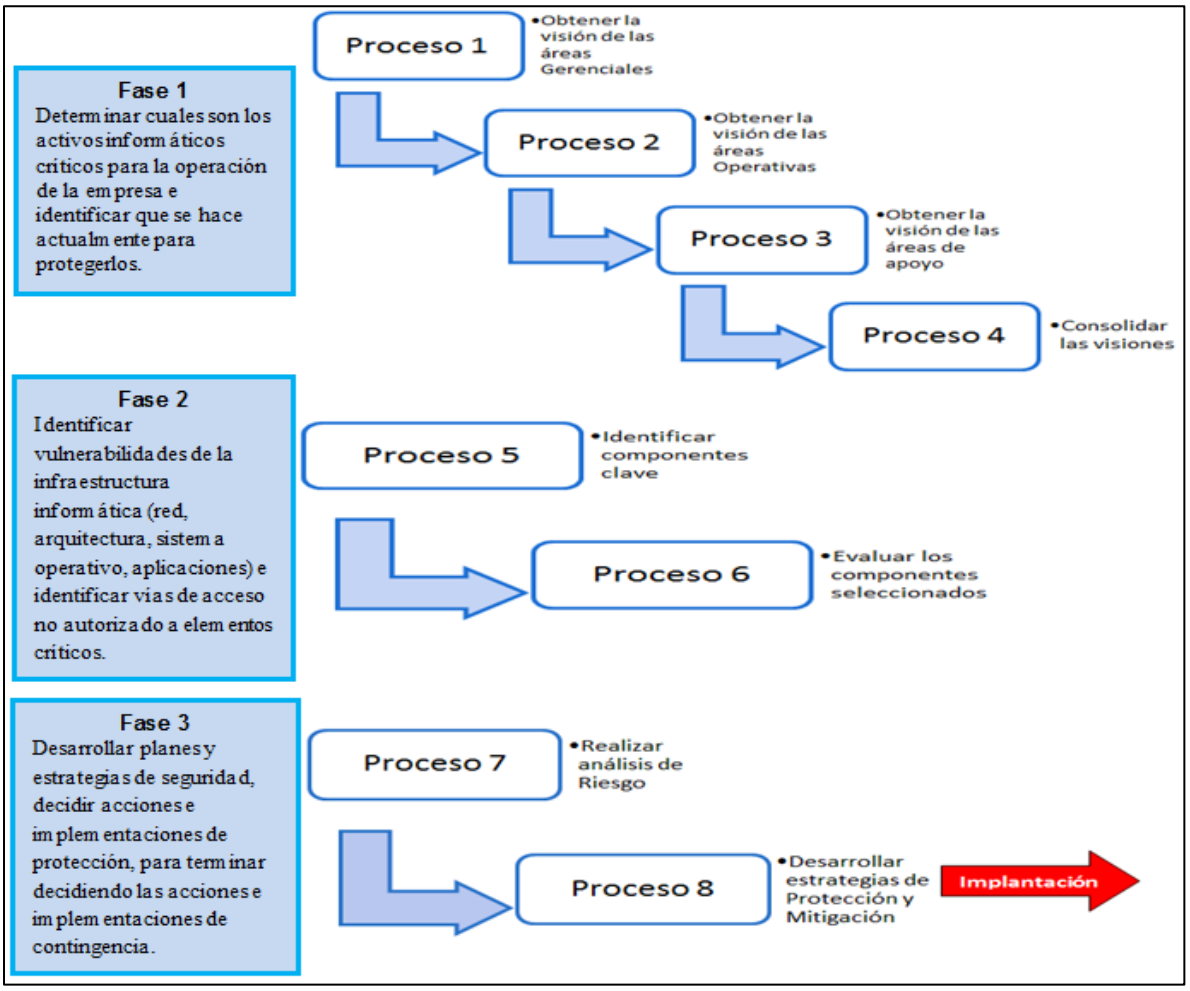

Figura 2: Fases de la Metodología OCTAVE (resumen de la metodología)

Para llegar a la fase de implantación, OCTAVE recomienda una serie de talleres que llevan a su ejecución mediante un equipo de análisis interdisciplinario de tres a cinco personas que trabajen en la organización. El método aprovecha el conocimiento de múltiples niveles de la organización para lograr los siguientes resultados:

- Asegurar la continuidad de la operación de la Institución.
- Identificar y definir los riesgos.
- Establecer estrategias para mitigar el riesgo.
- Enfocarse en la conservación de la información (no de los activos).
- Intervención de todos los departamentos o unidades de la empresa.

C. Alineación a la Norma ISO/IEC 27002

La Serie ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la S-I utilizable para cualquier tipo de organización o institución. La serie ISO/IEC 27000 contiene las mejores prácticas recomendadas en S-I para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Esta investigación se sustenta en una de la norma ISO/IEC 27002, la cual pertenece a la serie ISO 27000. La ISO/IEC, llamada anteriormente ISO/IEC 17799, fue publicada en el año 2.000 y traducida al español desde el año 2.006, es una guía de buenas prácticas que describe los controles recomendables en cuanto a S-I, esta norma no es certificable y contiene 11 dominios, 39 objetivos de control y 133 controles. Es relevante indicar que para una Institución que no posee ninguna norma de S-I, no es imprescindible implementar todos los objetivos de control de la norma si no los

más trascendentales para la misma, por lo tanto en la Tabla 1 se encuentran marcados con color azul los dominios considerados para la ejecución de esta investigación, los cuales hacen referencia a los 2 procesos de UTIC (Base de Datos y Redes y Comunicaciones):

TABLA 1: Resumen de la Norma ISO/IEC 27002

DOMINIO (11)	OBJETIVOS DE CONTROL (39)	CONTROLES (133)
POLÍTICA DE SEGURIDAD	Política de seguridad de la información	2
ASPECTOS ORGANIZATIVOS DE LA SI	Organización Interna	7
	Seguridad en los accesos a Terceros	3
GESTIÓN DE ACTIVOS	Responsabilidad sobre los activos	3
	Clasificación de la información	2
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	Seguridad antes del empleo	3
	Durante el empleo	2
	Finalización del empleo o cambio de puesto de trabajo	3
SEGURIDAD FÍSICA Y DEL ENTORNO	Áreas seguras	6
	Seguridad de los equipos	7
GESTIÓN DE COMUNICACIONES Y OPERACIONES	Procedimientos y responsabilidad de operación	4
	Gestión de servicios externos	3
	Planificación y aceptación del sistema	2
	Protección contra software malicioso	2
	Gestión de respaldo y recuperación	1
	Gestión de la seguridad de redes	2
	Utilización de los medios de información	4
	Intercambio de información	5
	Servicios de comercio electrónico	3
	Monitoreo	6
CONTROL DE ACCESOS	Requisitos de negocio para el control de accesos	1
	Gestión de acceso de usuarios	4
	Responsabilidades de los usuarios	3
	Control de acceso a la red	7
	Control de acceso al sistema operativo	6
	Control de acceso a las aplicaciones y a la información	2
	Ordenadores portátiles y teletrabajo	2
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Requisitos de seguridad de los sistemas	1
	Seguridad de las aplicaciones del sistema	4
	Controles criptográficos	2
	Seguridad de los archivos del sistema	3
	Seguridad en los procesos de desarrollo y soporte	5
	Gestión de la vulnerabilidad técnica	1
GESTIÓN DE INCIDENTES EN LA S-I	Notificación de eventos y debilidades de la S-I	2
	Gestión de incidentes y mejoras en la S-I	3
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Aspectos de la gestión de la continuidad del negocio	5
CUMPLIMIENTO	Cumplimiento de los requisitos legales	6
	Cumplimiento de la políticas y normas de seguridad	2
	Consideraciones sobre la auditoría de sistemas	2

Dominios usados en esta investigación, procesos: Base de Datos - Redes y Comunicaciones

D. Definir la situación actual de la UTIC

La universidad ESPE tiene aproximadamente 25.000 estudiantes en 6 sedes descentralizadas y dirige sus esfuerzos al mejoramiento de las condiciones de vida del país y a impulsar su desarrollo. Como parte fundamental de la universidad esta la UTIC (Unidad de Tecnologías de la Información y Comunicaciones) quien administra los recursos tecnológicos requeridos por la Institución para el manejo de la información amparado en una adecuada comunicación, tal como lo demuestra su

Catálogo de Servicios en la Tabla 2. Por lo tanto, la razón de ser la UTIC es asegurar la disponibilidad, actualización tecnológica, innovación y operación de los recursos y servicios TIC´s, para alcanzar un alto nivel de Tecnología y con estándares de calidad.

TABLA 2: Catálogo de Servicios vigente de la UTIC - ESPE

CATÁLOGO DE SERVICIOS DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN		
ORD	DESCRIPCIÓN	ÁREA RESPONSABLE
1	Sistema de Gestión Académica de Pregrados	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
2	Sistema de Gestión Académica de Postgrados	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
3	Sistema de Gestión Administrativa Financiero	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
4	Sistema de Gestión Investigaciones	ADMINISTRACIÓN DE APLICATIVOS Y BASES DE DATOS
5	Asistencia/Asesoría Técnica en Desarrollo de Redes y Comunicación	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
6	Red LAN	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
7	Red WAN	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
8	Red Inalámbrica	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
9	Acceso Internet	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
10	Acceso Internet Avanzado (CEDIA)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
11	Correo Electrónico	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
12	Administración de Usuarios	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
13	Comunicaciones de voz (VoIP / Mode)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
14	Repositorio de Archivos (FTP)	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
15	Videoconferencias	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
16	Housing	ADMINISTRACIÓN DE SERVICIOS DE REDES Y COMUNICACIONES
17	Asistencia/Asesoría Técnica en Desarrollo de Sistemas de Información	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
18	Portal de Servicios Institucionales (MIESPE)	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
19	Portal Web Institucional / Micrositios	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
20	Desarrollo de Sistemas y Aplicaciones Institucionales	DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE APLICATIVOS
21	Asistencia/Asesoría Técnica Primer Nivel / Gestión de incidencias	GESTIÓN DE SOPORTE TÉCNICO
22	Mantenimiento Preventivo de equipos informáticos de la ESPE	GESTIÓN DE SOPORTE TÉCNICO
23	Mantenimiento Correctivo de equipos informáticos de la ESPE	GESTIÓN DE SOPORTE TÉCNICO
24	Asesoría Técnica en Adquisiciones de equipos TIC´s	GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Servicios que brinda la UTIC correspondientes a los procesos: Base de Datos y Redes y Comunicaciones

III. Evaluación de resultados y discusión

Luego del análisis de la información disponible en la UTIC, se evidencia la necesidad de implementar una normatividad formal que regule los procedimientos y el uso correcto de los sistemas críticos de comunicación y de bases de datos en lo referente a S-I, en virtud que las funciones operativas y de soporte se basan en un alto grado de confianza del conocimiento de los técnicos de TI a fin de solventar incidentes y problemas, los cuales han venido afectando claramente con los principios básicos de la S-I (disponibilidad, integridad y confiabilidad). La carencia de un marco de trabajo controlado bajo una norma, es causal de que los errores e interrupciones tengan una alta probabilidad de ocurrencia. Así lo indica el 85% del personal de la UTIC que desconoce de un documento formal de Políticas de S-I que haya sido aprobado o comunicado en la Institución, o como lo muestran los resultados obtenidos, el bajo porcentaje de cumplimiento en controles de S-I plasmados en la Figura 3.

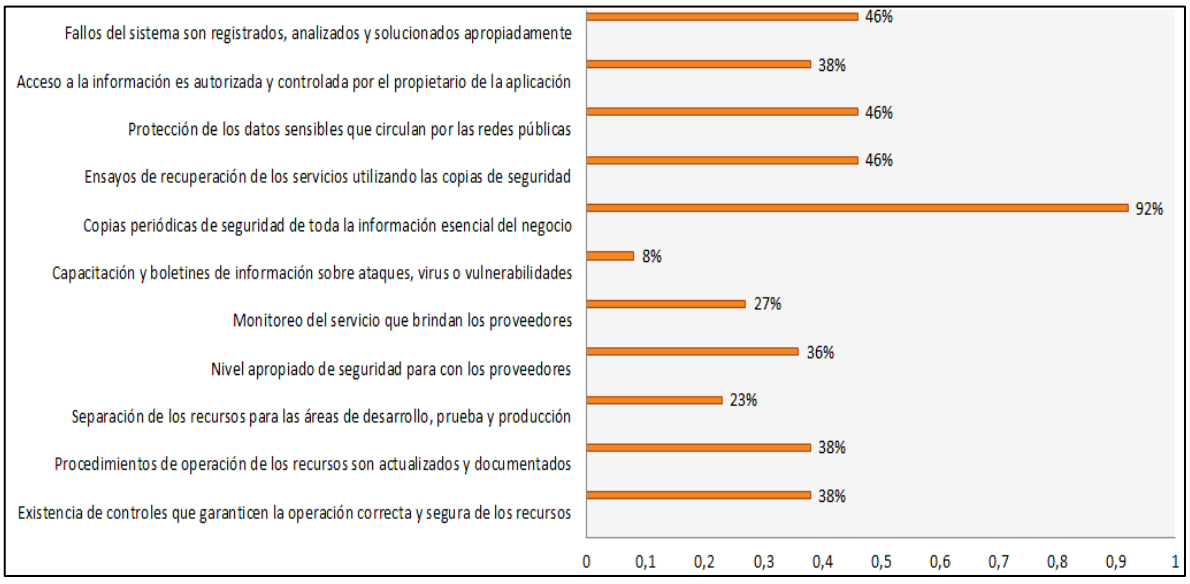

Figura 3: Cumplimiento de controles aplicados a la Gestión de Comunicaciones y Operaciones

IV. Diseño e Implementación

El plan maestro de S-I para la UTIC con lineamientos de la norma ISO/IEC 27002 esta diseñada para que las políticas y controles sean utilizados eficientemente, con el fin de que el personal de TI entienda ¿qué hacer?, ¿cómo hacerlo? y ¿por qué es importante la S-I?, garantizando un lenguaje común entre toda la comunidad y encaminado hacia las necesidades reales de la Institución.

Lógicamente, si se quiere implementar exitosamente un estándar o norma internacional es preferible contar con la ayuda de una consultora externa que conozca a profundidad la misma y que supervise todos los pasos para que la certificación se obtenga sin complicaciones. Solo de esta manera se podrá alcanzar los máximos parámetros de S-I en los sistemas de la Institución. Sin embargo, en un contexto general, para poder implementar la norma en la UTIC, el proceso resumido se indica en la Figura 4.

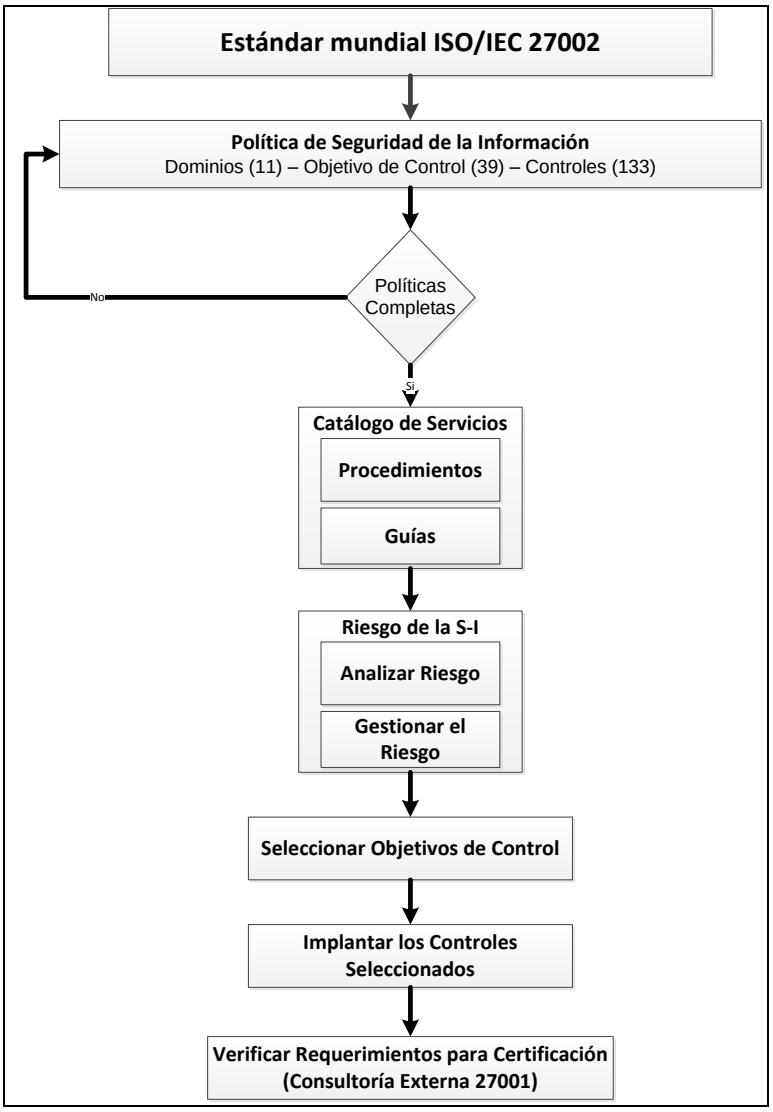

Figura 4: Proceso para implementar la norma ISO/IEC 27002 en la UTIC-ESPE (resumen creado)

V. Trabajos relacionados

Dentro de las líneas de investigación de TIC's y Seguridad Informática, actualmente en la Institución no existen trabajos de tesis de pregrado o postgrado relacionados con la generación de un plan maestro de S-I alineado a una norma o estándar Internacional.

VI. Conclusiones y trabajo futuro

Certificarse en una norma de S-I constituye para la ESPE una apuesta de futuro, que además de una garantía de calidad en la gestión de TI supone una ventaja competitiva respecto a aquellas instituciones que no lo han hecho, esta sería la principal proyección o reto a lograr. Adicionalmente

se debería analizar la factibilidad de crear un proceso que controle y regule las actividades de la S-I en la ESPE. La impresión final de esta investigación se plasma en las siguientes conclusiones:

- La ESPE requiere de políticas y controles de S-I que se encuentren amparadas en una norma internacional. Las normativas y procedimientos vigentes en la UTIC, han sido desarrolladas en función de las experiencias de los técnicos de TI.
- La investigación analítica realizada a través del cuestionario de S-I, demuestra que el 15% de los técnicos de la UTIC hacen referencia a la existencia de un Manual de Políticas y Plan de Seguridad de Informática, sin embargo desconocen la ubicación física y la frecuencia de actualización del mismo.
- La investigación realizada permite entregar una guía flexible, coherente e integral en el uso de políticas y controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 para fortalecer la S-I en la ESPE, coordinando y armonizando el trabajo de las diferentes unidades de la UTIC.
- La ESPE requiere un Sistema de Gestión de la S-I que establezca políticas y procedimientos relacionados con los requerimientos del negocio, a fin de mantener un nivel mínimo de riesgo que pueda asumirse.
- Cumpliendo con el alcance planteado en este proyecto de investigación, se analizaron las políticas para los siguientes dominios:
    - Dominio (1): Política de Seguridad
    - Dominio (6): Gestión de Comunicaciones y Operaciones
    - Dominio (8): Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
    - Dominio (10): Gestión de la Continuidad del Negocio

  Es importante para la UTIC, analizar la posibilidad de continuar y concluir con el desarrollo de los dominios que recomienda la ISO/IEC 27002 que no han sido objeto de la presente investigación. El cumplimiento de este literal tendrá como fin de fortalecimiento de los procesos internos de la UTIC, mejorando la calidad del servicio entregado a la Comunidad Politécnicas. Los dominios faltantes se detallan a continuación:
    - Dominio (2): Aspectos Organizativos de la Seguridad de la Información.
    - Dominio (3): Gestión de Activos
    - Dominio (4): Seguridad Ligada a los Recursos Humanos
    - Dominio (5): Seguridad Física y del Entorno
    - Dominio (7): Control de Acceso
    - Dominio (9): Gestión de Incidentes en la Seguridad de la Información
    - Dominio (11): Cumplimiento.
- En función al dominio (6): Gestión de Comunicaciones y Operaciones, el 92% de los ingenieros que respondieron el cuestionario, manifestaron que se realizan copias de seguridad de toda la información crítica regularmente, este control es el que más porcentaje de cumplimiento tiene la UTIC.
- El dominio (7): Adquisición, desarrollo y mantenimiento de Sistemas de Información, se videncia que un 62% de los profesionales conocen que para evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones de la Institución; se verifican los datos de referencia, tablas de parámetros, entradas duplicadas, valores fuera de rango, caracteres inválidos, definición de responsabilidades de los implicados en el proceso de ingreso de datos.
- Se requiere impulsar en la Comunicad Politécnica una cultura que proteja la S-I, principal activo de la ESPE, para lo cual se debe promover jornadas de orientación y capacitación para los usuarios internos, externos y terceros.
- Las posibles limitaciones que se pueden generar en el proceso de implementación de la norma es creer que el responsable de la S-I es solamente un nombre en un papel y no de cada usuario de la ESPE que tiene acceso a la tecnología.

- Como se muestra en la figura 4 del presente Artículo Técnico, una vez terminadas las políticas de los 11 dominios de la ISO/IEC 27002, se procede con la elaboración de las guías y procedimientos de los servicios de TI que ofrece la UTIC, para posteriormente realizar el análisis y la gestión de riesgos que puedan afectar con su normal funcionamiento. Finalmente, se debe considerar una asesoría externa que permita la elaboración de requerimientos para la certificación en la norma ISO 27001, la misma que es certificable.

VII. Agradecimiento

Al personal de UTIC, por su participación efectiva en la realización de la presente investigación, en la búsqueda de mejora continua y comprometida con la calidad total.

VIII. Referencias Bibliográficas

- Antonio Baquero, Luis Joyanes. (s.f.). *Libro Informática, Glosario de Términos y Siglas.* Mc. Graw Hill.
- CERT. (17 de 09 de 2008). *Software Engineering Institute.* Recuperado el 16 de 03 de 2012, de OCTAVE: http://www.cert.org/octave/
- CYBSEC S.A., S. S. (2011). Fundamento de Seguridad Informática. Buenos Aires, Argentina.
- Gonzalo Álvarez Marañon, Pedro Pablo Pérez García. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: McGraw-Hill.
- Guangalango Vega, Ricardo Napoleón; Moscoso Montalvo, Patricio Esteban. (2011). *Evaluación Técnica de la Seguridad Informática del Data Center de la Escuela Politécnica del Ejército.* Sangolqui: ESPE.
- *ISO ORG.* (s.f.). Recuperado el 12 de 03 de 2012, de ISO 27000: www.ISO27000.es
- IT Governance Institute. (2007). *COBIT 4.1.* IL 60008 USA: IT Governance Institute.
- Palma, L. A. (2011). *Introducción Seguridad informática.* México: ITESM.
- SGC. (s.f.). Recuperado el 06 de 03 de 2012, de Mapa de Procesos de SGC de la ESPE: http://sgc.espe.edu.ec/Paginas/mapa.html
- Vieites, Á. G. (2007). *Enciclopedia de la Seguridad Informática.* México D.F.: Alfaomega Grupo Editor, S.A. de C.V.