SATHIRÍ Sembrador

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

INFORMATION SECURITY POLICIES REGARDING TO STATAL POLYTECHNIC OF CARCHI UNIVERSITY

Recibido: 13/09/2020 - Aceptado: 25/05/2021

JUAN PABLO LÓPEZ GOYEZ

Máster en Ingeniería de Software y Sistemas Informáticos
Universidad Internacional de la Rioja - UNIR

juan.lopez@upec.edu.ec
https://orcid.org/0000-0003-2873-2185

VIVIANA LUCÍA PROAÑO BARRO

Máster en Ingeniería de Software y Sistemas Informáticos
Universidad Internacional de la Rioja - UNIR

vivi03lu@gmail.com

WILSON ANDRÉS ZABALA VILLARREAL

Director de TIC de la Universidad Politécnica Estatal del Carchi
Tulcán - Ecuador

Magíster en Ingeniería de Software
Universidad Técnica del Norte

andres.zabala@upec.edu.ec
https://orcid.org/0000-0003-0713-9876

Cómo citar este artículo:

López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2022). Políticas de seguridad de la información para la Universidad Politécnica Estatal del Carchi. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Resumen

El presente trabajo está enmarcado en el desarrollo de políticas de seguridad de la información para la Universidad Politécnica Estatal del Carchi (UPEC), como un requisito para el establecimiento del Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma técnica ecuatoriana INEN-ISO/IEC-27001. El propósito de la elaboración de dichas políticas es disponer de la documentación necesaria que permita definir los procedimientos para salvaguardar la información y garantizar la continuidad en las operaciones de los servicios informáticos institucionales. Se utilizó la metodología propuesta por el EGSI y la ISO/IEC 27001 que establecen los requisitos y objetivos de control necesarios para la gestión de la seguridad de la información.

Se realizó el levantamiento de información en las unidades de la Dirección de TIC de la UPEC para conocer a detalle el portafolio de servicios informáticos que se ofrecen a la comunidad universitaria. Con la información obtenida se realizó un estudio de los controles establecidos en el EGSI y se relacionó cada uno de ellos con la finalidad de conocer el nivel de cumplimiento y madurez de la Institución.

Se elaboró y evaluó las políticas de seguridad de información tomando como punto de partida los trece apartados del EGSI que corresponden a: seguridad de activos, desarrollo de software seguro, control de acceso a sistemas informáticos, seguridad en redes, gestión de riesgos y continuidad de operaciones; acciones que permiten promover la mejora continua en los procesos de continuidad y gestión de incidentes.

Palabras claves: EGSI, ISO, controles, políticas, seguridad

Abstract

This work is framed in the development of information security policies for the Carchi State Polytechnic University (UPEC), as a requirement for the establishment of the Government Information Security Scheme (EGSI) based on the Ecuadorian technical standard INEN ISO/IEC 27001. The purpose of the elaboration of the information security policies for this institution is to have the necessary documentation to define the procedures to safeguard the information and modify the continuity in the operations of the institutional computer services. The methodology proposed by the EGSI and the ISO/IEC 27001 standard that establishes the requirements and controls for the necessary objectives for adequate management of security information were used.

Information was collected from the team work of the IT department of the UPEC University to know in detail the portfolio information of the technological services offered to the university community. With the obtained information, a study of the controls established in the EGSI was carried out and each of them was related to the way of knowing the level of compliance and maturity of the Institution.

The security Information policies were elaborated and evaluated taking as a starting point the EGSI sections that correspond to: asset security, secure software development, access control to computer systems, data network security, risk management and continuity of operations; actions that allow promoting continuous improvement in the continuity and incident management processes.

Keywords: EGSI, ISO, controls, policies, security

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Introducción

Los pilares fundamentales de la seguridad de la información en toda organización están basados en el establecimiento de políticas de seguridad de la organización, implantación de sistemas de gestión de seguridad de la información (SGSI) y de procesos correctamente definidos para el ciclo de vida de desarrollo de software seguro (S-SDCL), con la finalidad de garantizar la eficiencia y eficacia en los sistemas de información y la confidencialidad, integridad y disponibilidad en la información (Technical-Committee ISO/IEC, 2013).

En el Ecuador, se promueve la implementación de políticas de seguridad de la información con la finalidad de proteger la información como activo fundamental para la ejecución de los procesos institucionales que ofrecen las instituciones públicas (Santorum, 2014) . Por ello, se han definido lineamientos necesarios que permitan la elaboración de políticas de seguridad de la información mediante el esquema gubernamental de seguridad de la información (EGSI) que busca normalizar y exigir el uso de políticas de seguridad en las instituciones públicas de acuerdo con el ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la Información (Subsecretaría de Gobierno Electrónico del Ecuador, 2019).

La UPEC es una Institución de Educación Superior (IES) en el Ecuador, catalogada como universidad pública y que con 15 años de vida Institucional ha logrado posicionarse entre las mejores universidades del norte del país, brindando calidad en sus procesos administrativos y académicos.

En su corta existencia institucional ha superado varios procesos de evaluación y a pesar de contar con bajo presupuesto anual, gestiona sus recursos para realizar sus actividades institucionales con calidad, respeto y responsabilidad. Frente a esto existen muchas necesidades y específicamente en el área de tecnologías de la información y comunicación, en donde se está trabajando en conjunto con las autoridades de la Institución con la finalidad de recibir mayor presupuesto y poder adquirir equipamiento que soporte y permita una transformación en la infraestructura tecnológica actual.

La UPEC dispone actualmente en sus repositorios digitales de la siguiente información: catálogos de servicios, normativas, reglamentos y procedimientos vigentes relacionados a los servicios y gobierno de tecnologías de la información y comunicación; el reglamento de buen uso de internet y de equipos informáticos es una de las bases sobre las que se construirá las políticas de seguridad de la información, ya que abarca puntos relacionados a la protección, buen uso de contraseñas, administración de usuarios de redes e internet y buen uso de correo electrónico (Políticas TIC UPEC, 2017).

Las necesidades actuales en el área de tecnologías de la información y comunicación de la UPEC se relacionan directamente al tema de seguridad de la información, tales como: implementar sistemas de respaldo y contingencia para garantizar la disponibilidad de la información frente a vulnerabilidades que pueden afectar la continuidad de los servicios informáticos, entre otras la disponibilidad de políticas que regulen los procesos y permitan definir controles y objetivos de control.

La implementación del EGSI en la UPEC permitirá definir las políticas de seguridad de la información y también promover la propuesta para implementar procesos de gestión de seguridad de la información enfocados a garantizar la continuidad de los servicios institucionales a la comunidad universitaria (Baldecchi, 2014; ISO Tools Excellence, 2017).

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Por tal razón, se busca elaborar las políticas de la UPEC basadas en prácticas recomendadas por la legislación ecuatoriana y también por normativa internacional vigente como la norma ISO/IEC 27001 que establece los debidos lineamientos para su realización.

Antecedentes

La seguridad de la información en instituciones públicas de educación superior es una prioridad para el gobierno ecuatoriano debido a la fuerte demanda de usuarios que requieren el uso de los servicios informáticos para realizar labores académicas y administrativas, y que acceden desde diversos dispositivos y equipos tecnológicos a Internet. Para el caso de la Universidad Técnica Particular de Loja (UTPL, 2011), la universidad elaboró y estableció un SGSI para garantizar el control de sus procesos relacionados a las tecnologías de la información y comunicación y la seguridad de la información. En el año 2017, se presentó un alto porcentaje de ciberataques, especialmente en universidades públicas de Manabí debido al incremento en el uso de nuevas herramientas tecnológicas, la migración de servicios tradicionales a servicios digitales que dependen del uso de internet provocando que exista incidencias de malware, tráfico de cifrado malicioso, por lo que se implementó controles y políticas para mitigar este tipo de incidentes (Avellán & Zambrano, 2018).

En el país se busca es incorporar una cultura de prevención y protección frente a amenazas y vulnerabilidades a la seguridad de la información que pueden violentar los principios básicos y la reputación de las instituciones de educación superior (Baldeón Gutiérrez & Guanopatín Safla, 2015). Además, se busca la implementación de medidas preventivas y correctivas por parte de los responsables de las unidades de TIC (Santorum, 2014), las mismas que permitan mitigar el impacto de posibles riesgos que puedan afectar el normal desempeño de la infraestructura tecnológica y de los sistemas informáticos, como se menciona en el estudio realizado para la implementación de un sistema de protección de la red de datos en la Escuela Superior Politécnica de Chimborazo-Espoch (Quezada, 2017).

Materiales y métodos

La investigación científica utilizada para el desarrollo de las políticas de la UPEC se centró en el concepto básico que relaciona la revisión del estado del arte, el levantamiento de información, recopilación y análisis de datos; así como las conclusiones de la investigación realizada.

Identificación de requisitos y metodologías. La identificación y levantamiento de requisitos permitió analizar la situación actual de la UPEC, esto es conocer la información necesaria para establecer un punto de partida en el desarrollo de las políticas de seguridad. Los requisitos se describen a continuación:

- Contexto de la Institución
- Misión y visión UPEC
- Estructura orgánica funcional Institucional
- Estructura orgánica Dirección de TIC
- Políticas institucionales
- Portafolio de servicios informáticos

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Descripción de las metodologías. La subsecretaria de Gobierno Electrónico establece el lineamiento para la definición de políticas de seguridad de la información para implementar un EGSI, bajo normativa nacional e internacional con la finalidad de cumplir con los estándares alineados a cuidar los activos tecnológicos y proteger la información (Cáceres & Mena, 2015). Para cumplir con este fin, se proponen metodologías que fueron empleadas para el desarrollo de este trabajo, las cuales se presentan a continuación:

- Estándar INEN ISO/IEC 27001 basado en el estándar internacional ISO/IEC 27001:2013.
-
- Esquema gubernamental de seguridad de la información (EGSI) de aplicación obligatoria para las instituciones públicas que dependen directamente del gobierno central del Ecuador.

Estándar ISO/IEC 27001:2013. Es una normativa que especifica los requisitos indispensables para lograr el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo el contexto de una institución, o empresa interesada en implementar un sistema de seguridad sin importar su tamaño, naturaleza o contexto (Gualotuña & Quilumbaqui, 2016). De igual manera establece los requisitos para implementar políticas de seguridad de la información, así como el tratamiento de riesgos asociadas a la seguridad de la información de las organizaciones (Technical-Committee ISO/IEC, 2013).

La implantación de un sistema de gestión de seguridad de la información se realiza mediante el ciclo PDCA de mejora continua de Deming, que define las actividades y el ciclo de vida del SGSI, el ciclo se describe en la Figura 1.

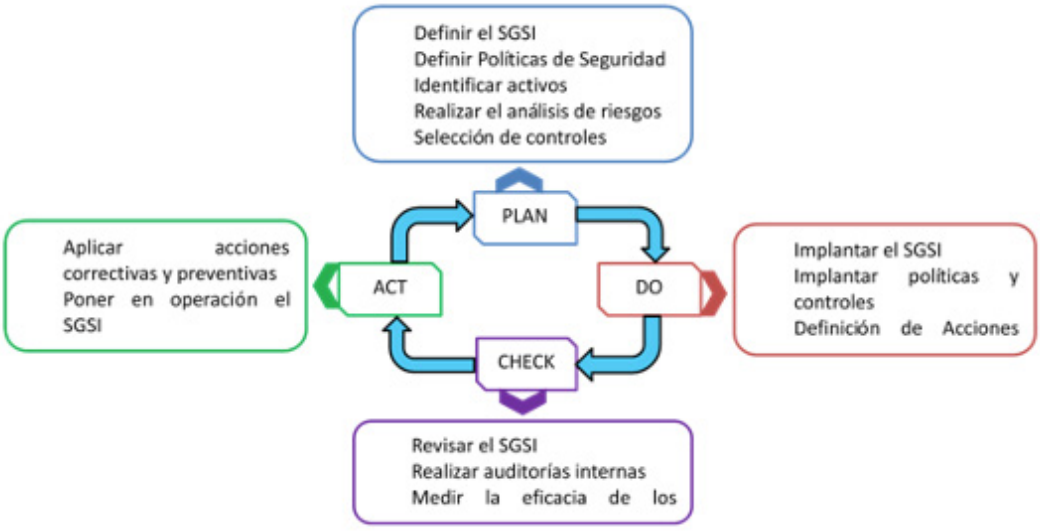

Figura 1. SGSI – Ciclo PDCA

Esquema gubernamental de seguridad de la información. El esquema gubernamental de seguridad de la información EGSI es un marco basado y fundamentado en la normativa ecuatoriana NTE INEN-ISO/IEC 27000 para la gestión de la seguridad de la información (Peñaherrera, 2013). El EGSI presenta lineamientos e hitos de control que deben ser cumplidos mediante la

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

implementación de un sistema de gestión de seguridad de la información que busca garantizar la definición de procesos y procedimientos para salvaguardar la información y activos informáticos de las Instituciones Públicas en el Ecuador (Peñaherrera, 2013).

Figura 2. Modelo EGSI v1.0 Ecuador
Fuente: (Gobierno Electrónico del Ecuador, 2013)

Análisis de la situación actual y aplicación de las metodologías. Determinación de un SGSI. La organización debe vincular los requisitos para el establecimiento de SGSI bajo el criterio de la mejora continua, los requisitos PDCA se presentan a continuación:

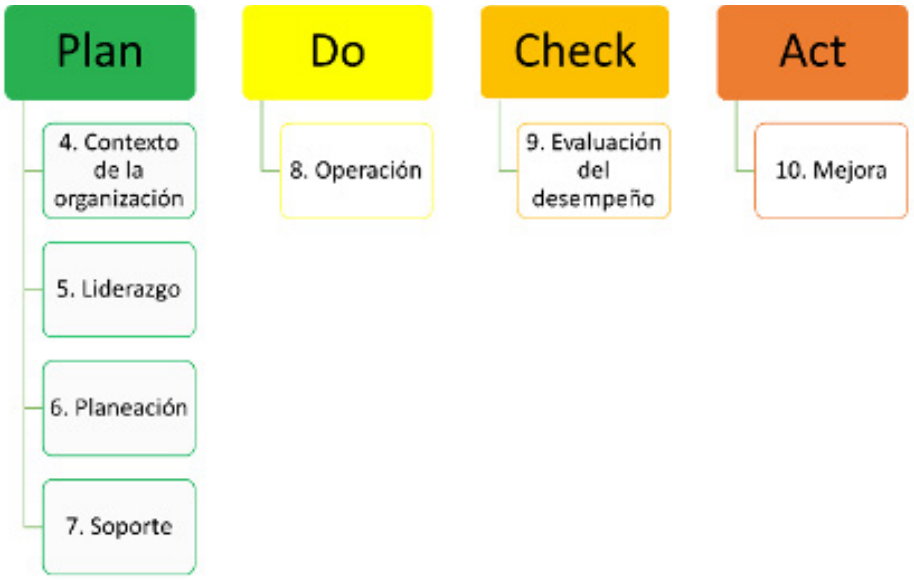

Figura 3. Ciclo de mejora continua para la norma ISO/IEC 27001:2013

Para determinar la necesidad de implantar un SGSI en una organización, se empleó la normativa ISO/IEC 27001:2013 para conocer el nivel de cumplimiento con cada uno de los apartados y requisitos (Technical-Committee ISO/IEC, 2013), mismos que se presentan en la Figura 4.

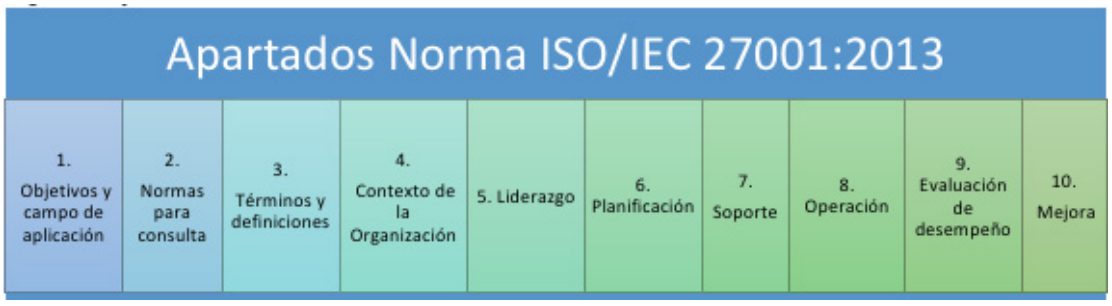

Figura 4. Apartados de la norma ISO/IEC 27001:2013

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Cada apartado de la normativa ISO/IEC 27001:2013 se relaciona con el cumplimiento de requisitos que permiten determinar si una organización requiere implementar políticas de seguridad de la información y un SGSI.(Ver Tabla 1).

Tabla 1.
Requisitos normativa ISO/IEC 27001

ISO/IEC 27001:2013	Dominios	Requisitos
Apartado 4	Contexto de la organización	5
Apartado 5	Liderazgo	3
Apartado 6	Planificación	4
Apartado 7	Soporte	7
Apartado 8	Operación	3
Apartado 9	Evaluación del desempeño	3
Apartado 10	Mejora	2
	TOTAL	**27**

Fuente: (Technical-Committee ISO/IEC, 2013)

Para medir el nivel de cumplimiento de los requisitos propuestos en la normativa ISO 27001:2013 se determina la siguiente matriz para realizar una valoración cualitativa mediante la técnica de la entrevista que se realizará a las partes interesadas (Baldecchi, 2014). (Ver Tabla 2).

Tabla 2.
Matriz medición requisitos establecidos en ISO/IEC 27001

Nivel de cumplimiento	Descripción
APLICA	La UPEC cumple o se alinea a los requisitos establecidos por la norma
PARCIAL	La UPEC cumple parcialmente los requisitos establecidos por la norma
NO APLICA	La UPEC no cumple los requisitos establecidos por la norma o se encuentra en procesos de implementación

Elaboración de políticas de seguridad y objetivos de control. Los dominios y objetivos de control del EGSI v1.0 parten de la normativa ISO 27001 y pueden ser empleados para la elaboración de políticas de seguridad de información (Baldeón Gutiérrez & Guanopatín Safla, 2015).

A continuación, se presenta la cantidad de objetivos de control obligatorios que se deben cumplir para poder alinearse a la propuesta del Anexo A1 disponibles en la normativa ISO 27001:2013 y que se relacionan con los hitos de control de seguridad de información propuestos en el EGSI del Gobierno Electrónico del Ecuador (Sangoluisa, 2012)(Ver Tabla 3).

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Tabla 3.
Dominios y objetivos de control establecidos en normativa ISO 27001

	Dominio	Objetivos obligatorios
1.	Políticas de seguridad de la Información	4
2.	Organización de la seguridad de la información	10
3.	Gestión de activos	19
4.	Confidencialidad de la información para el talento humano	3
5.	Seguridad física y del entorno	8
6.	Seguridad en las comunicaciones y operaciones	25
7.	Seguridad en el control de acceso a los sistemas informáticos	27
8.	Seguridad para la adquisición, desarrollo y mantenimiento de los sistemas informáticos	2
9.	Gestión de incidentes de la seguridad de la información	12
10.	Continuidad de los servicios informáticos	0
11.	Cumplimiento	0
TOTAL		110

Resultados y discusión

Aplicación matriz medición requisitos establecidos en ISO/IEC 27001. Al aplicar la matriz de valoración para medir el nivel de cumplimiento de la UPEC frente a los requisitos establecidos en la normativa ISO 27001 presentados en la Figura 4 y Tabla 1 respectivamente, se pudo determinar lo siguiente: se cumple con el 40,74 % de requisitos, mismos que se alinean con los procesos de la UPEC. Por otro lado, el 29,63 % de requisitos corresponde a un cumplimiento parcial y el 29,63 % a un no cumplimiento de procesos desde el punto de vista de gestión de TI, estos resultados se determinaron en la evaluación comprendida entre 2019 y 2021.

Tabla 4.
Matriz medición requisitos establecidos en ISO/IEC 27001

Nivel de cumplimiento	Descripción	Requisitos	Porcentaje
APLICA	La UPEC cumple o se alinea a los requisitos establecidos por la norma	11	40,74 %
PARCIAL	La UPEC cumple parcialmente los requisitos establecidos por la norma	8	29.63 %
NO APLICA	La UPEC no cumple los requisitos establecidos por la norma o se encuentra en procesos de implementación	8	29.63 %
	Total	27	100 %

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Es decir, la UPEC no se alinea con los requisitos propuestos por la normativa, ya que no se cumple con al menos el 60 % de cumplimiento parcial a los indicadores analizados. Con este antecedente se establece como punto inicial la necesidad de elaborar políticas en conjunto con un modelo de gestión de seguridad de información.

El resultado también evidencia las limitaciones presentadas en las instituciones públicas en general por la poca asignación de recursos a temas relacionados a la seguridad de la información, así como la falta de interés en el tema de seguridad informática, Sin embargo, la alineación de la UPEC al modelo de gestión de un SGSI es factible si se aplican instrumentos y metodologías adecuadas procurando la mejora continua.

Desarrollo de las políticas de seguridad de la información. Los planes estratégicos institucionales de la UPEC buscan la mejora continua y la calidad en sus procesos, la Unidad de Planificación y Desarrollo Institucional ha establecido planes y procedimientos orientados al cumplimiento de metas y objetivos, siendo estos: Plan Operativo anual: (POA), plan estratégico y de desarrollo institucional: (PEDI), portafolio de servicios informáticos, manual de procesos y procedimientos y la información obtenida mediante entrevistas al equipo de la Dirección de TIC

Con estos antecedentes, se desarrolló las políticas orientadas al cumplimiento de los 11 ejes transversales del Esquema gubernamental de seguridad de la información, el cuál fue adaptado a las necesidades, servicios y proyecciones de la comunidad universitaria frente a los servicios informáticos y la seguridad de la información. A continuación, se presenta el resumen de políticas de seguridad de información orientadas al contexto organizacional de la UPEC.

Figura 5. Políticas de seguridad de la información de la UPEC

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Aplicabilidad actual de objetivos de control. Los objetivos de control obligatorios propuestos por el EGSI v1.0, ISO 27001:2013 en su Anexo A1, fueron adecuados al contexto organizacional de la UPEC y definidos en función de la propuesta de políticas de seguridad de la información. Se determinó un total de 110 controles que serán revisados, mejorados o implementados en la Institución en una fase inicial.

Al realizar una valoración empleando la herramienta de auditoría de procesos como lo es el checklist, se pudo determinar que ciertos procesos relacionados con los servicios informáticos de la UPEC no están orientados a garantizar la seguridad de la información, la continuidad de las operaciones y la respuesta frente a incidentes o amenazas. A continuación, se presentan de los resultados obtenidos en la evaluación de los dominios y objetivos de control propuestos en las políticas de seguridad de la información.

Tabla 5.
Matriz medición requisitos establecidos en ISO/IEC 27001

	Dominio	Objetivos obligatorios	Objetivos cumplidos
1.	Políticas de seguridad de la Información	4	1
2.	Organización de la seguridad de la información	10	7
3.	Gestión de activos	19	2
4.	Confidencialidad de la información para el talento humano	3	3
5.	Seguridad física y del entorno	8	8
6.	Seguridad en las comunicaciones y operaciones	25	9
7.	Seguridad en el control de acceso a los sistemas informáticos	27	16
8.	Seguridad para la adquisición, desarrollo y mantenimiento de los sistemas informáticos	2	1
9.	Gestión de incidentes de la seguridad de la información	12	0
10.	Continuidad de los servicios informáticos	0	0
11.	Cumplimiento	0	0
	TOTAL	110	**47**

Para el establecimiento de las políticas en la UPEC se requiere del cumplimiento de 110 objetivos de control. Para la fecha actual de la presentación de este artículo, los procesos implementados por las diferentes unidades de trabajo de la Institución permiten el cumplimiento de 47 objetivos, esto representa un 43 % de implementación de las políticas de seguridad propuestas (Ver Figura 6). La Dirección de TIC progresivamente deberá implementar los objetivos de control faltantes con la finalidad de cumplir y garantizar la calidad en el desarrollo y ejecución de los procesos que dependen de los servicios informáticos; así como la seguridad de la información de la UPEC.

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

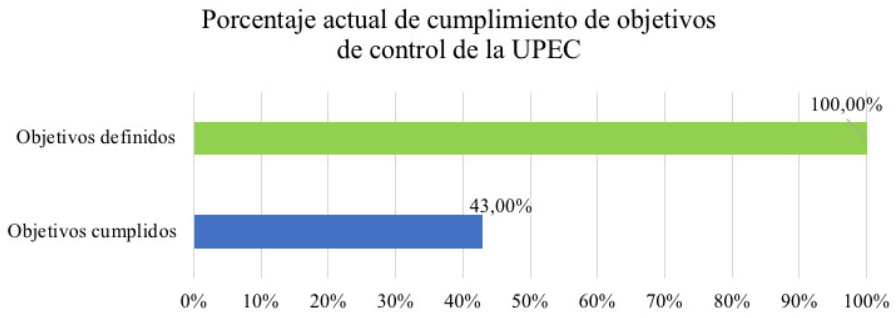

Figura 6. Cumplimiento de objetivos de control en la UPEC

En la Figura 7, se presenta el porcentaje actual de cumplimiento de cada uno de los dominios propuestos en las políticas de la UPEC, siendo el valor de 100 % el que representa el total cumplimiento. Se evidencia que dos dominios: Confidencialidad de la información y seguridad física y del entorno se cumplen al 100 %.

Por otro lado, la aprobación, difusión e implementación de la política de seguridad de la información permitirá que los dominios: Documentación de las políticas de seguridad y la organización de la seguridad de la información con un 25 % y 70 % de cumplimiento respectivamente se cumplan en su totalidad. Sin embargo, los dominios restantes cuya importancia es vital para garantizar el ciclo de vida de los sistemas de gestión de seguridad de la información son inferiores o menores al 50 %; esto debido a que la Institución se encuentra en la fase inicial de implementación.

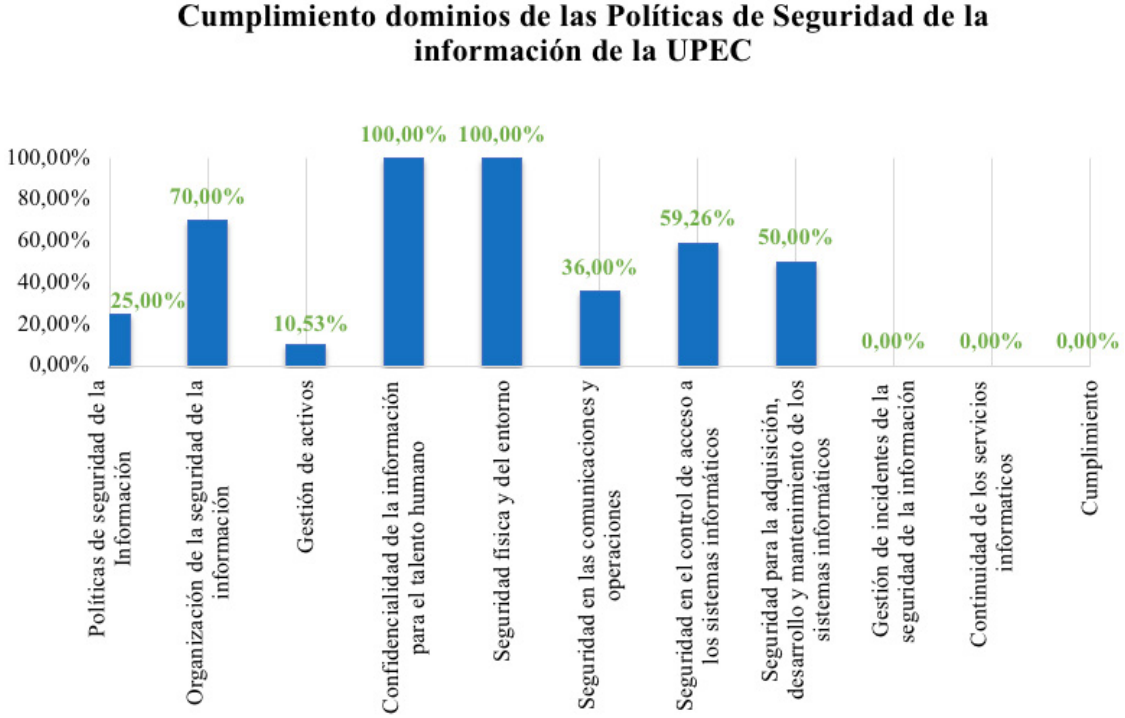

Figura 4. Cumplimiento actual de los dominios establecidos en las políticas de la UPEC

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Conclusiones

Se realizó el análisis de la situación actual de la UPEC mediante levantamiento de información empleando la técnica de entrevista y recopilando información proporcionada por la Dirección de TIC y Procuraduría General, determinando así: la filosofía y organización de la UPEC, los objetivos y planificación institucional, el portafolio de servicios informáticos, la validación de los apartados propuestos por la normativa ISO/IEC 27001; los mismos que permitieron conocer la situación real y actual respecto a la seguridad de la información. Por tal razón, se analizó un total de 27 requisitos propuestos en los apartados de la norma, de los cuales la UPEC cumple únicamente con 11 requisitos que representa el 40,74 %, validando así la necesidad de implementar las políticas de seguridad de la información.

Las políticas desarrolladas para la UPEC se realizaron con base en la normativa ISO/IEC 27001:2013 y bajo los dominios y objetivos de control propuestos por el Esquema Gubernamental de Seguridad de la Información (EGSI), de cumplimiento obligatorio para las instituciones públicas ecuatorianas que dependen de la Administración Pública Central y en general para las demás instituciones del país.

Se definió un total de 11 dominios y 110 objetivos de control en las Políticas de Seguridad de la Información, que se alinean a los servicios informáticos de la UPEC. Los objetivos son el resultado de la adopción de los objetivos propuestos en el EGSI, los cuales a su vez forman parte del Anexo A de la normativa ISO/IEC 27001 y su definición se realizó considerando aspectos como: nivel de cumplimiento, evidencia de documentación de sustentación, definición e implementación de procesos, ámbito legal y aspectos financieros. La UPEC cumplió con 47 objetivos de control que representan el 43 % de cumplimiento.

Se desarrolló las políticas de seguridad de la información de la UPEC bajo las directrices del EGSI, que requieren una adecuada planificación, investigación y trabajo multidisciplinario que involucró las siguientes áreas de la institución: Consejo Superior Universitario Politécnico (CSUP), Dirección de TIC, Procuraduría, Secretaría General, con las cuáles se analizó los 11 dominios propuestos en esta metodología, se definió las políticas y el nivel de cumplimiento para cada uno de ellos; finalmente se definieron objetivos de control que serán implementados en la institución.

Recomendaciones

Se plantea en la institución la implementación, control y monitoreo de 110 objetivos de control propuestos en las políticas de seguridad de la información de la UPEC con la finalidad de cumplir los indicadores del acuerdo Ministerial 166 de la Secretaría de la Administración Pública respecto a la implementación de un Esquema Gubernamental de Seguridad de la Información y garantizar la seguridad de la información en la UPEC como compromiso de la máxima autoridad y las unidades responsables.

Se recomienda implementar los procesos para la gestión de riesgos y elaboración del Plan de Continuidad de los Servicios informáticos de la UPEC, que permita tener un tratamiento y respuestas frente a incidentes de seguridad de la información basado en normativas nacionales e internacionales y marco legal vigente.

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Se propone determinar los niveles de madurez alcanzados por la UPEC respecto a la seguridad de la información, con la finalidad de dar paso a la elaboración del modelo de gestión de seguridad de la información, que será utilizado para instaurar la cultura de mejora continua en los procesos de tecnologías de la información y comunicación; así como los procesos destinados a garantizar la seguridad de la información y de los activos tecnológicos.

La seguridad de la información en las Instituciones Públicas que se encuentran en la zona geográfica y geopolítica de la UPEC y que no dependen directamente de la Administración Central no se encuentra focalizada bajo un marco normativo técnico que permita definir y enmarcar los objetivos institucionales con los de un sistema de gestión de seguridad de la información, se plantea desarrollar investigaciones que permitan determinar la situación actual de las mismas e instaurar políticas de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de la información y a su vez la eficiencia de los sistemas de información.

Referencias

Baldecchi, R. (2014). *Implementación efectiva de un SGSI ISO 27001.* ISACA. https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014 - Exposición 2 CIGRAS ISO 27001 - rbq.pdf

Baldeón Gutiérrez, M. del R., & Guanopatín Safla, J. (2015). *Politicas de Seguridad de Informacion para la Universidad Central del Ecuador Bajo los Estandares iso/IEC 27000 y COBIT 5.* https://repositorio.espe.edu.ec/bitstream/21000/12551/1/T-ESPE-049808.pdf

Cáceres, C., & Mena, C. (2015). *Elaboración de la guía de implantación de las normas prioritarias del esquema gubernamental de seguridad de la información EGSI en las entidades de la administración pública.* https://bibdigital.epn.edu.ec/bitstream/15000/11234/1/CD-6422.pdf

Políticas TIC UPEC, 13 (2017). http://www.upec.edu.ec/index.php?option=com_docman&task=doc_download&gid=5392&Itemid=202

Gobierno Electrónico del Ecuador. (2013). *Esquema Gubernamental de Seguridad de la Información – EGSI.* Ministerio de Telecomunicaciones y de La Sociedad de La Información. https://www.gobiernoelectronico.gob.ec/esquema-gubernamental-de-seguridad-de-la-informacion-egsi/

Gualotuña, H., & Quilumbaqui, G. (2016). *Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del Sistema Nacional de Nivelación y Admisión (SNNA).* http://bibdigital.epn.edu.ec/handle/15000/15191

ISO Tools Excellence. (2017). ISO 27001: P*lan de tratamiento de riesgos de seguridad de la información.* SGSI. https://www.pmg-ssi.com/2017/06/iso-27001-plan-tratamiento-riesgos-seguridad-informacion/

Peñaherrera, C. C. (2013). *EGSI - Acuerdo 166 - Esquema gubernamental de seguridad de la informacion* (pp. 1–47). LEXIS. http://www.regulacionelectrica.gob.ec/esquema-gubernamental-de-seguridad-de-la-informacion-egsi-2/ %0Ahttp://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-InformaciÃ3n.pdf

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117

Sangoluisa, D. (2012). *Definición de las Políticas De Seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basada en las normas ISO 27000.* http://bibdigital.epn.edu.ec/bitstream/15000/14623/1/CD-6793.pdf

Santorum, M. (2014). *Propuesta de políticas de seguridad de la información para la Escuela Politécnica Nacional.* http://bibdigital.epn.edu.ec/handle/15000/8686

Subsecretaría de Gobierno Electrónico del Ecuador. (2019). *Esquema Gubernamental de la Seguridad de la Información.* https://www.gobiernoelectronico.gob.ec/egsi/

Technical-Committee ISO/IEC. (2013). INTERNATIONAL STANDARD ISO / *IEC 27001. In ISO/IEC 27001:2013* (Vols. 2013-10–01, Issue Second Edition).

Cómo citar este artículo:
López, J., Proaño, V. & Zabala, W. (Enero - Junio de 2021). Políticas de Seguridad de la información para la Universidad. *Sathiri* (17)1, 313-326. https://doi.org/10.32645/13906925.1117