DIAGNÓSTICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), EN LA UNIVERSIDAD DE CIENCIAS COMERCIALES UCC - CAMPUS LEÓN 2023.

DIAGNOSIS OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS), AT THE UCC UNIVERSITY OF COMMERCIAL SCIENCES UCC - CAMPUS LEÓN 2023.

Martha Elizabeth Aguinaga Mora
Máster en Ciberseguridad
(elizabeth.aguinaga@ucc.edu.ni)

RESUMEN:
Un Sistema de Gestión de Seguridad de la Información, proporciona las mejores prácticas de seguridad de Información y permite a la organización desarrollar, implementar y medir la práctica eficaz de gestión de la seguridad en todas sus áreas unificadas en sus operaciones (comúnmente el día a día de la organización), con el fin de alinearse al cumplimiento de los objetivos de la misma y para minimizar los riesgos existentes.
PALABRAS CLAVES: seguridad, gestión, información, riesgos

ABSTRACT:
An Information Security Management System provides information security best practices and enables an organization to develop, implement and measure effective security management practices across all of its unified areas of its operations (commonly on a day-to-day basis). day of the organization), to align with the fulfillment of its objectives and minimize the existing risks.
KEYWORDS:
security, management, information, risks

INTRODUCCIÓN

En la actualidad, al hablar de información, se debe considerar que esta es uno de los activos más importantes dentro de cualquier tipo de organización, para mantener sus niveles de competitividad, por lo que es necesario tener en cuenta que la gestión de la misma debe ser adecuada con el fin de preservar su integridad, confidencialidad y disponibilidad.

Partiendo de lo mencionado anteriormente, dentro de la Universidad de Ciencias Comerciales, campus León, es importante considerar la necesidad de crear una cultura de seguridad de la información, mediante la adopción de mecanismos de control, que permitan incorporar un nivel de seguridad adecuado a los activos de información, que son gestionados por el área de Tecnologías de la Información y Comunicación.

A partir de esto, se ha llevado a cabo la presente investigación, la cual consiste en proponer la implementación de un Sistema de Gestión de Seguridad de la Información para la Universidad de Ciencias Comerciales, campus León, que será gestionado por el área de Tecnología de Información y Comunicación (TIC), adaptando los requerimientos de la Norma ISO/IEC 27001:2013 a las actividades y funciones realizadas en la Unidad, para ello se establecen tres fases de desarrollo, las mismas que permiten, mediante el análisis de la situación actual del Campus en cuanto a seguridad de la información, valoración de los activos de información (bajo las dimensiones de: confidencialidad, disponibilidad e integridad), determinación de amenazas y vulnerabilidades asociadas a los activos de información, análisis de riesgos encontrados para los activos de información y determinación de los mecanismos de control necesarios para la mitigación de dichos riesgos a partir del Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2013, que contiene 114 controles, distribuidos en 11 secciones; esquematizar la propuesta de un Manual de Políticas de Seguridad de la Información, destinado a la mitigación de riesgos informáticos y creación de una cultura de

seguridad de la información a nivel institucional, todo ello gestionado por el área de Ciberseguridad y Tecnología de la Información y Comunicación de la Institución.

En el capítulo I del presente documento se realiza el planteamiento de la Investigación, en el que se explica el contexto actual de la Universidad, se establece los objetivos e Hipótesis de la investigación.

En el capítulo II se abordan aspectos relacionados al marco referencial, teorías y conceptos bajo los que está sustentada esta investigación.

El capítulo III explica cada uno de los procedimientos, instrumentos y formas de procesamiento de los datos obtenidos para llevar a cabo esta investigación.

El capítulo IV muestra el análisis de los resultados, en el que se explica y demuestra los resultados que se obtuvieron al aplicar los instrumentos, la interpretación de las entrevistas realizadas y el porcentaje de cumplimiento de los controles aplicados en la UCC que corresponden a la Norma ISO/IEC 27001 mediante una lista de cotejo.

El capítulo V, refleja los aspectos administrativos que se tomaron en cuenta para el desarrollo de esta investigación, tales como el presupuesto y el cronograma de actividades.

El capítulo VI, describe las conclusiones y futuras líneas de investigación que se podrían continuar desarrollando tomando como bases este estudio.

Y por último en el capítulo VII se brindan las recomendaciones para mejorar el proceso de gestión de seguridad de la información en la UCC.

MARCO DE REFERENCIA

Se han consultado varios estudios relacionados a esta investigación, tales como los mencionados a continuación:

-Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Este estudio se llevó a cabo en el año 2016 por Valencia-Duque, y contribuyó en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001.

- Diseño y creación de una política de seguridad de la información (SGSI) basado en la normativa ISO 27000 para la cooperativa construcción, comercio y producción (Año 2016). Se creó una política de seguridad de la información que ayudó a cumplir con los objetivos organizacionales, administrativos y técnicos de la planificación anual.

-Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000, (Año 2015). Se definieron políticas de seguridad de la información a nivel de red y de usuario para el servicio de correo electrónico y de videoconferencia de la Presidencia de la República basadas en un análisis de riesgo previo. Para realizar el análisis previamente se estudió algunas metodologías de análisis de riesgo de la seguridad de la información como, MAGERIT, ISO 27005, FRAAP, OCTAVE-ALLEGRO.

Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Estos son necesarios para que la organización funcione y alcance los objetivos que propone su dirección (Espinoza, 2013).

La seguridad de la información son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (Aguirre Freire & Palacios Cruz, 2014).

Un Sistema de Gestión de Seguridad de Información (SGSI) es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007).

Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables (Montesino Perurena, Baluja Garcia, & Porven Rubier, 2013).

Actualmente en Nicaragua existe una Ley, la cual se aprobó el 27 de octubre del año 2020, conocida como Ley especial de Ciberdelito o Ley 1042, la cual tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.

METODOLOGÍA

El tipo de investigación presentada es de carácter cuantitativo, de corte transversal, descriptiva, no experimental.

El enfoque cuantitativo en este estudio se aplicó debido a que para su realización fue necesaria la recolección de información sobre los diferentes elementos que luego fueron transformados en datos porcentuales para su posterior análisis, logrando medir el nivel de cumplimiento en la Universidad de Ciencias Comerciales UCC, Campus León, de los controles establecidos en la Norma ISO/IEC 27001:2013.

Este estudio es de corte transversal porque las variables en este caso, los dominios de la Norma ISO 27001, fueron analizados durante un determinado período de tiempo. Es descriptiva porque describe cada una de las políticas de seguridad de la información que se aplican en la UCC, campus León en base a criterios establecidos en la Norma antes mencionada.

El estudio es no experimental porque se observa el estado actual en cuanto a niveles de seguridad de la información de la UCC, campus León, para después analizarlos.

El área de estudio es la Universidad de Ciencias Comerciales, UCC, en el campus León, ubicado al costado Oeste del Campus Médico, UNÁN León.

Las unidades de análisis son los activos

informáticos del Campus León.

La población de estudio son todos aquellos colaboradores que de manera directa o indirecta tengan acceso a información sensible o sistemas informáticos implementados en la Institución.

Para la muestra se han seleccionado a dos colaboradores para aplicarle entrevista.

Dada las características del tema a investigar, la información será recolectada mediante fuentes primarias, ya que la obtención de los datos será a través del contacto directo con los sujetos en estudio y los instrumentos por el cual se registrará la información serán entrevistas y lista de cotejo.

Se hará una escala de Likert para medir el nivel de cumplimiento de cada uno de los controles de seguridad de la información que son aplicados en el campus León, y que están establecidos en la Norma ISO 27001:2013.

Teniendo en cuenta los requerimientos establecidos en la norma ISO/IEC 27001:2013 para el diseño del Sistema de Gestión de Seguridad de la Información, se establecieron las siguientes fases para el desarrollo del proyecto: Fase I-Diagnóstico del SGSI, Fase II-Preparación, Fase III-Planificación.

ANÁLISIS DE RESULTADOS

De la entrevista realizada al Máster Ulises Rivera, director del área de Tecnologías de la Información y Comunicación, se ha logrado interpretar que:

-En la Universidad de Ciencias Comerciales, campus León, no existe una política de seguridad de la información como tal, sino que existen normas de uso de los servicios tecnológicos, pero de manera general.

- No se han realizado capacitaciones de concienciación al personal sobre el uso de buenas prácticas para proteger la información frente amenazas internas y externas.

-Se debe mejorar el sistema de cableado estructurado en la institución para prevenir las interferencias en la transmisión de los datos y uso de la red informática.

- Se tiene un doble control de acceso a los sistemas que tiene que ver con la autenticación del equipo desde el cual se hace la conexión a los servidores y la autenticación de los usuarios a los sistemas informáticos con sus respectivas credenciales personales.

- Se realizan respaldos de la información ingresada en los sistemas de manera diaria.

-Se cuenta con poco personal en el área de soporte informático para dar respuesta a la demanda de servicios que deben de darse a las áreas en lo que respecta a mantenimiento de equipos informáticos y acceso a la red.

De la entrevista realizada a la Lic. Grethel Hernández, coordinadora de Registro Académico del campus León, se pudo interpretar que:

-En registro académico existe una normativa interna, sin embargo, no es específicamente para la seguridad de la información, sino que trata de la descripción de los procesos académicos del área.

-A la información que se maneja en Registro Académico, únicamente tiene acceso el personal autorizado.

-No se tiene clasificada la información por grado de criticidad, sin embargo, la información más sensible se tiene resguardada en áreas de acceso restringido.

- La información que se traslada fuera del campus es resguardada en cajas de cartón resistente y es transportada por personal autorizado únicamente.

- Se maneja información física como digital correspondiente a la vida académica de los estudiantes.

- Hay un perímetro de seguridad entre el área a la que puede acceder el público y el área a la que puede acceder solamente personal autorizado.

-A los equipos informáticos se les brinda mantenimiento preventivo y correctivo con cierta frecuencia, pero podría mejorar.

Para determinar el nivel de cumplimiento de los controles de seguridad de la información que implementa actualmente la UCC-Campus León, en base a los objetivos de control establecidos en la Norma ISO/IEC 27001, se ha elaborado una lista de cotejo o de verificación.

La siguiente tabla, refleja las equivalencias de los valores en el campo nivel de cumplimiento.

Tabla 1. Escala de cumplimiento

Cumplimiento	Escala (0-0.5-1)
Si cumple	1
Nivel medio de cumplimiento	0.5
No cumple	0

Fuente: Elaboración propia

El nivel o porcentaje de cumplimiento global se obtuvo de la sumatoria de los valores correspondientes a cada uno de los controles dividido entre el número de ellos y posteriormente se multiplicará por 100.

Para determinar el porcentaje de cumplimiento de los controles se utilizará la siguiente fórmula:

PC=(SC/NC) *100

Donde:

PC= Porcentaje de Cumplimiento

SC= Sumatoria de los controles.

NC= Número de controles

PC= (50.5/114) *100

PC=44.3%

El porcentaje de cumplimiento de los controles que se aplican en la Universidad de Ciencias Comerciales, campus León, basado en Norma ISO/IEC 27001, es del 44.3%.

CONCLUSIONES

1. Se realizó un análisis de cumplimiento de los controles de la ISO/IEC 27001 para determinar la situación actual de la seguridad de la información en la Universidad de Ciencias Comerciales, campus León, encontrándose que existen incumplimientos significativos con respecto a la norma de referencia, sobre todo en los dominios de Organización de la seguridad de la información, Gestión de activos, Seguridad física y ambienta, Gestión de las comunicaciones y las operaciones, Gestión de incidentes de seguridad de la información y Cumplimiento.

2. Aplicando una lista de cotejo se pudo determinar que el nivel de cumplimiento de los controles que se implementan en la Institución respecto a los establecidos en la Norma ISO/IEC 27001 es del 44.3 %.

3. Se definieron las políticas de seguridad de la información, para cada uno de los siguientes dominios de la seguridad de la información: (1) Gestión de activos de información, (2) Seguridad física y del entorno, (3) Gestión de comunicaciones y operaciones, (4) Control de acceso, (5) Adquisición, desarrollo y mantenimiento de sistemas y (6) Cumplimiento.

Futuras Líneas de Investigación

Para dar continuidad a la presente investigación, se podría seguir desarrollando el tema:

-Realizando un análisis sobre los riesgos a los que se encuentra expuesta la información y el impacto que esto generaría en la institución al materializarse estos riesgos o amenazas.

-Puesto que esta investigación solo abarca el diagnóstico y la propuesta de algunas políticas, se podría continuar con la implementación del Sistema de Seguridad de la Información en un futuro estudio o investigación.

-Se puede expandir el alcance del estudio hacia las demás sedes de la Universidad de Ciencias Comerciales, dado que esta investigación fue realizada tomando en cuenta únicamente el campus León.

REFERENCIAS BIBLIOGRÁFICAS

- Bertrán, J., & Francisco, F. (2014). Implementación del modelo de gestión de la seguridad de la información aplicando ISO 27000 en la empresa Coka Tours, Ambato - Ecuador.
- Mata, L. (2017). “El enfoque cuantitativo de investigación”. Obtenido de https://investigaliacr.com/investigacion/el-enfoque-cuantitativo-de-investigacion/?msclkid=9ac683aea56e11ec85b2ce53b6bd11f7
- Montaño Orrego, V. (2011). La gestión en la seguridad de la información. Revista Pensamiento Americano.
- Ochoa Arévalos, P. A. (2015). Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica ESPOL.
- Ramos, Y., Urrutia, O., & Bravo, A. (2013). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. 4to Congreso Internacional AmITIC 2017, Aplicando nuevas tecnologías.
- Rodríguez, J. (2016). Diseño y creación de una política de seguridad de la información (SGSI) basado en la normativa ISO 27000 para la cooperativa construcción, comercio y producción.
- Sangoluisa, D. (2015). Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000.
- Valencia-Duque, F. J. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Iberica de Sistemas y Tecnología de la Información.

ANEXOS

Entrevista a Director de TIC.

Estimado MBa. Ulises Rivera, director de TIC de la Universidad de Ciencias Comerciales. Solicito su colaboración para contestar las siguientes preguntas. Las respuestas a las mismas serán utilizadas únicamente para fines investigativos. Muchas gracias de antemano.

1. ¿Considera usted importante que en la institución exista un conjunto de políticas para la seguridad de la información? ¿por qué?
2. ¿Se ha elaborado un inventario de los activos informáticos y recursos para el tratamiento de la información? ¿estos tienen definido un propietario o responsable que se haga cargo de su uso?
3. ¿Qué procedimiento formal de registro y retirada de usuarios se implementa en la institución, para el control de acceso a la red y sistemas informáticos con la asignación de roles y permisos claramente definidos? Ejemplifique.
4. ¿Qué procedimiento sobre el inicio de sesión a los sistemas informáticos se implementa actualmente en la institución y cómo se gestiona el uso, la protección y la duración de las contraseñas?
5. ¿Qué medidas se implementan para proteger el sistema de cableado estructurado de interferencias o daños?
6. ¿Se realiza mantenimiento preventivo y correctivo a los equipos informáticos? ¿Con qué frecuencia?
7. ¿Qué controles de detección, prevención y recuperación se implementan para la protección contra malware? ¿y qué procedimiento se aplican para la concienciación a los empleados o usuarios de los equipos informáticos respecto a dichos códigos maliciosos?
8. ¿Se realizan copias de seguridad o respaldos de información de los sistemas? ¿Con qué frecuencia se realizan dichos respaldos?
9. ¿Existe un plan de contingencia para dar respuesta a incidentes relacionados con la seguridad de la información?
10. ¿Qué medidas de seguridad de la red se implementan en la institución? Explique.

Entrevista a Coordinadora de Registro Académico.

Estimada Lic. Grethel Hernández, Coordinadora de Registro Académico, de la Universidad de Ciencias Comerciales, campus León. Solicito su colaboración para contestar las siguientes preguntas. Las respuestas a las mismas serán utilizadas únicamente para fines investigativos. Muchas gracias de antemano.

1. ¿Ha escuchado anteriormente el termino Sistema de Gestión de Seguridad de la información (SGSI)?
2. ¿Qué políticas de seguridad de la información se implementan actualmente en la coordinación de registro académico?
3. ¿De qué manera está clasificada la información en registro académico?? Explique
4. ¿Quiénes tiene acceso a la información de

registro académico?

5. ¿Qué medidas se implementan durante el traslado de la información fuera de los límites físicos de la institución?

6. ¿Qué controles de entrada se implementan para proteger las áreas que contienen información sensible?

7. ¿Qué procedimiento implementa para identificar sus activos de información?

8. ¿Qué medidas se implementan para la protección de la información física ante desastres naturales?

9. ¿Se les brinda mantenimiento correctivo y preventivo a los equipos informáticos (actualización de antivirus)? ¿Con qué frecuencia?

10. ¿Qué controles de acceso a los sistemas de información se aplican en la coordinación de registro académico? ¿Se utiliza la misma contraseña para todos los sistemas?

embargo, el 42% es femenino donde lo hacen por una necesidad de compra.

A continuación, se presentan los resultados obtenidos de esta investigación, asociando a las preguntas de la encuesta con los objetivo general y específicos.