UNIVERSIDAD ABIERTA PARA ADULTOS

(UAPA)

DIRECCION ACADEMICA DE POSGRADO

MAESTRÍA EN CIBERSEGURIDAD

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD BASADO EN LA NORMA ISO 27001, PARA LA PROTECCIÓN DE LA INFORMACIÓN EN EL CENTRO MÉDICO SIGLO 21 EN EL PERIODO SEPTIEMBRE-DICIEMBRE, 2022

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR POR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD

POR:

VICTOR MANUEL BRITO PEREZ 2021-02700

JOSÉ FERMÍN FRANCISCO FERRERAS 2021-02787

ASESOR(A):

AMERICO VELOZ

SANTIAGO DE LOS CABALLEROS

REPÚBLICA DOMINICANA

DICIEMBRE 2022

INDICE

RESUMEN

El presente trabajo de tesis consiste en la implementación de un sistema de gestión de la seguridad para la protección de la información de la empresa Centro Médico Siglo 21 basado en la norma ISO/IEC 27001 donde se plantea la problemática asociada a la falta de formalización, documentación de las medidas de seguridad y debilidades de los activos de información. En base a esto, se plantearon como objetivos el diseño, ejecución y validación del sistema de gestión de seguridad basado en la norma ISO/IEC 27001 con el propósito de mejorar la seguridad de la información en la empresa.

El desarrollo de este trabajo de tesis corresponde al tipo de investigación cualitativo con un diseño de investigación-acción. En esa misma línea se empleó el método inductivo para la investigación, para la recolección datos se emplearon como instrumentos la entrevista, cuestionarios y la observación directa con apoyo de listas de verificación.
Se tomaron en cuenta los conceptos desarrollados en el primer capítulo, donde se describieron las bases teóricas que sustentan las actividades, procedimientos y conclusiones de la investigación. Luego en el cuarto capítulo podemos ver la descripción de la propuesta donde se realizó la descripción del contexto y la planificación; se definieron los objetivos, el alcance y la estructura de dicha propuesta.

Ya en el cuarto capítulo que lleva por título, Validación de la Propuesta, podemos ver como se desarrolló la ejecución de dicha propuesta empleando el ciclo de mejora continua, donde en la fase de planificación se describió el contexto de la organización, se realizó un inventario de activos y un análisis de riesgo en el cual se encontró un conjunto de debilidades en los activos que en base a las amenazas identificadas suponen riesgos para la seguridad de la información. En esta misma etapa se definió también el plan para el tratamiento de los riesgos identificados.

En la etapa de ejecución, se crearon las políticas de seguridad y se implementaron controles orientados al tratamiento de los riesgos encontrados. Luego en la fase de verificación se realizó una evaluación a las políticas y controles implementados para determinar su nivel de efectividad, todo esto junto a una auditoría interna en donde se elaboró una declaración de aplicabilidad para determinar el estado actual de las políticas y los controles detallados en el anexo A de la norma ISO/IEC 27001:2022.

En la fase de acciones correctivas se desarrolló la estrategia para el tratamiento de los problemas identificados en la verificación, se realizó un programa de capacitación al personal. Luego en la fase de validación de la propuesta se hizo la presentación formal del trabajo realizado a la dirección y a los mandos medios, la cual se encuestó para obtener la valoración por parte de esta. Junto a esto se solicitó la validación de la propuesta por parte de un experto en seguridad de la información.

Como resultado final se obtuvo una valoración bastante positiva por parte de la dirección logrando su interés en participar en los procesos de mejora y continuidad del SGSI. Por otro lado, el experto que fue consultado validó la propuesta indicando que cumple con los requisitos de la norma y de la empresa, esto luego de haber sugerido unos cuantos cambios en base oportunidades de mejora encontradas las cuales fueron tomadas en cuenta realizando las debidas correcciones.

CONCLUSIONES

Después de haber seguido los pasos de la metodología utilizada en este proyecto de investigación y siguiendo un proceso orientado al cumplimiento de los objetivos propuestos, donde se describe, se ejecuta y se valida la propuesta empleando como sustento las bases teóricas, se ha llegado a las siguientes conclusiones:

El diseño del Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001:2022 se ha llevado a cabo satisfactoriamente. Se ha realizado una correcta planificación, definiendo claramente el contexto de la organización describiendo claramente dicho contexto, lo cual permitió conocer los objetivos de negocio; el inventario de activos en el que se identificaron los activos críticos de información; un análisis de riesgos que permitió identificar y clasificar los riesgos para luego definir el plan para el tratamiento de los riesgos encontrados.

Para la ejecución del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022, se tomó en cuenta el plan de tratamiento de riesgos, se desarrollaron un conjunto de políticas y procedimientos y se implementaron controles que asisten al cumplimiento de dichas políticas y a la mejora de la seguridad de la información mitigando los riesgos identificados. Siendo esta la fase más laboriosa, se logró poner en marcha el SGSI obteniendo resultados apreciables y adecuados para una etapa inicial.

En cuanto a la validación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022, se informó a la directiva sobre los procesos realizados, los beneficios esperados y la importancia del SGSI. Finalmente, se obtuvo una valoración bastante positiva por parte de los directivos, logrando un gran nivel de expectativas e interés por colaborar con el proceso de mejora del sistema de seguridad de la información. También se contactó un experto en el área de seguridad de la información para evaluar la adecuación del proyecto a los requisitos seguridad de la empresa y de la norma ISO/IEC 27001:2022 logrando obtener una valoración positiva y la debida validación. Por lo tanto, podemos concluir que se obtuvo una validación satisfactoria del Sistema de Gestión de Seguridad de la Información.

BIBLIOGRAFÍAS

Alcamí, R. L., Devence, C., & Guiral, J. (2016). Introducción a la gestión de sistemas de información en la empresa. D - Universitat Jaume I. Severi de comunicació. Obtenido de https://elibro.net/es/ereader/uapa/51689

Arias, F. (2012). El proyecto de Investigación. Caracas, Venezuela: Editorial Episteme, C.A.

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encina, L. (2020). Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas.

Baca Urbina, g. (2016). Introducción a la Ciberseguridad. Grupo Editorial Patria. Obtenido de https://elibro.net/es/ereader/uapa/40458?page=281

Blasco Mira, J. E., & Pérez Turpin, J. A. (2007). Metodologías de investigación en educación física y deportes: ampliando horizontes. Alicante, España: Editorial Club Universitario.

Brito Pérez, V. M., Mendoza Fernández, J., & Peña Antigua, M. Y. (2018). Auditoría de Seguridad Informática Bajo la Norma ISO/IEC 27002 caso Centro Médico Siglo 21, San Francisco de Macorís en el año 2018. San Francisco de Macorís.

Chicano Tejada, E. (2015). Gestión de Incidentes de Seguridad Informatica, 1ra Ed. Málaga, España: IC Editorial.

Cobarsi-Morales, J. (2011). Sistemas de información en la empresa. Barcelona: Editorial UOC.

Costas Santos, J. (2015). Seguridad informática. Madrid, España: RA-MA Editorioal.

Cruz del Castillo, C., & Olivares Orozco, S. (2014). Metodología de la investigación. México D.F.: Grupo Editorial Patria.

Enrrique Gillermo, B. (2019). Implementación de un Sistema de Seguridad de la Información de acuerdo con la Norma ISO/IEC27001. Caso de Estudio: Unidad de Gestión Educativa Local 01. Pimentel, Perú. Obtenido de

https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6400/Llanos%20Guill%C3%A9n%20Enrique%20Guillermo.pdf?sequence=1&isAllowed=y

Escrivá Gascó, G. (2013). Seguridad informática. Madrid, España: Macmillan Iberia, S.A.

Fernández Gómez, L. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid, España: AENOR - Asociación Española de Normalización y Certificación.

Flores Sanchez, B. B. (2017). Diseño de un Sistema de Gestion de Seguridad de la Información para la empresa Coop-Aspire basado en la norma ISO 27001. Obtenido de https://repositorio.unphu.edu.do/bitstream/handle/123456789/4625/Dise%C3%B1o%20de%20un%20sistema%20de%20gesti%C3%B3n%20de%20seguridad%20de%20la%20informaci%C3%B3n%20para%20la%20empresa%20Coop-Aspire.pdf?sequence=1

García García, J., Reding Bernal, A., & López Alvarenga, J. C. (12 de 2013). https://www.redalyc.org/. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/3497/349733226007.pdf

Gómez Férnandez, L., & Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. Génova, Madrid: AENOR International, S.A.U. Obtenido de https://elibro.net/es/ereader/uapa/53624

Gómez Vieites, Á. (2015). Seguridad en Equipos Informáticos. Madrid, España: RA-MA Editorial.

Gui, S. G. (2020). Implantación de un sistema de gestión de la seguridad de la ifnormacion (SGSI). Barcelona, España: FUOC. Obtenido de https://openaccess.uoc.edu/bitstream/10609/142807/3/M%C3%B3dulo%203_Implantaci%C3%B3n%20de%20un%20sistema%20de%20gesti%C3%B3n%20de%20la%20seguridad%20de%20la%20informaci%C3%B3n%20%28SGSI%29.pdf

Hurtado de Barrera, J. (2010). El proyecto de investigacion :Compresion holística de la metodología y la inevestigación, 6ta Ed. Caracas, Venezuela: Ediciones Quirón.

Kljuÿnikov, A., Mura, L., & Sklenár, D. (2019). Gestión de la Seguridad de la Información en las PYMES. Entrepreneurship and Sustainability Issues, 1,9,11. Obtenido de https://www.researchgate.net/profile/Aleksandr-Kljucnikov/publication/333885503_Information_security_management_in_SMEs_factors_of_success/links/5d0c8010458515c11ceaf543/Information-security-management-in-SMEs-factors-of-success.pdf

Law Insider. (s.f.). lawinsider.com. Obtenido de lawinsider.com: https://www.lawinsider.com/dictionary/electronic-security-system

Menéndez Arantes, S. (2022). Auditoría de Seguridad Informática. RA-MA Editorial. Obtenido de https://elibro.net/es/ereader/uapa/222672?page=11

Monroy Mejía, M., & Nava Sanchezllanes, N. (2018). Metodología de la Investigación. Grupo Editorial Exodo. Obtenido de https://elibro.net/es/ereader/uapa/172512

Mora Garciía, J. (2016). Planificación de Proyectos de Implantación de NIfraestrucutras de Redes Telemáticas. IC Editorial. Obtenido de https://elibro.net/es/ereader/uapa/44148

Nieles, M., Dempsey, K., & Yan Pillitteri, V. (2017). Una Introducción a la Seguridad de la Información. Computer Security División NIST. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Organización Internacional de Normalizació. (2018). ISO 31000:2018 Gestión de Riesgo. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Organización Internacional de Normalización. (2013). Seguridad de la Información (ISO/IEC 27001). Obtenido de https://www.iso.org/isoiec-27001-information-security.html

Organización Internacional de Normalización. (2017). Guía de Implementación ISO/IEC 27003. Obtenido de https://www.iso.org/standard/63417.html

Organización Internacional de Normalización. (2018). ISO/IEC 27000. ISO/IEC. Obtenido de https://www.iso.org/standard/73906.html

Palacios, F. G. (2017). Diseño de un Sistema de Gesión de Seguridad de la Información ajustado a las necesidades de la Corporación Médica Clínica Vidade Quibdó. Medellín, Colombia.

Postigo Palacios, P. (2020). Seguridad Informática 1ra Edición. Madrid, España: Paraninfo.

Real Academia Española. (23 de 09 de 2022). Real Academia Español Enlinea. Obtenido de https://dle.rae.es/antecedente

Sampieri, R. H. (2014). Metodología de la Investigación,6ta ed. México D.F.: McGraw-Hill.

INSTRUCCIONES PARA LA CONSULTA DEL TEXTO COMPLETO:

Para consultar a texto completo esta tesis solicite en este formulario (https://forms.gle/vx5iLzv1pAMyN3d59 como hipervínculo) o dirigirse a la Sala Digital del Departamento de Biblioteca de la Universidad Abierta para Adultos, UAPA.

Dirección

Biblioteca de la Sede – Santiago

Av. Hispanoamericana #100, Thomén, Santiago, República Dominicana

809-724-0266, ext. 276; biblioteca@uapa.edu.do

Biblioteca del Recinto Santo Domingo Oriental

Calle 5-W Esq. 2W, Urbanización Lucerna, Santo Domingo Este, República Dominicana.

Tel.: 809-483-0100, ext. 245. biblioteca@uapa.edu.do

Biblioteca del Recinto Cibao Oriental, Nagua

Calle 1ra, Urb Alfonso Alonso, Nagua, República Dominicana.

809-584-7021, ext. 230. biblioteca@uapa.edu.do