RESUMEN ANÁLITICO ESPECIALIZADO RAE

Tema	Sistema de gestión de seguridad de la información (SGSI).
Titulo	Diseño de un sistema de gestión de seguridad de la información (SGSI) para La Institución Edutec de los Andes Pitalito, argumentada en la norma ISO/IEC 27001.
Autor	Jasmin Emilse Cuellar Castrillón
Director	Anívar Chaves Torres
Año	2.020
Programa	Especialización en Seguridad Informática

Resumen

Las empresas gestionan información importante y sensible que contribuye al correcto funcionamiento y cumplimiento de los objetivos y el desarrollo de sus actividades. Al tiempo, la información se enfrenta a constantes amenazada procedentes de usuarios internos y externos, y con ello el funcionamiento de general de la organización se encuentra en riesgo. De concretarse una amenaza de seguridad de la información, la organización se verá afectada, no solo en sus operaciones, sino también en su reputación y buen nombre.
El Instituto Edutec de los Andes, con sede en Pitalito Huila, presentaba problemas de seguridad, por no contar con las medidas apropiadas para contrarrestar las amenazas. Con el propósito de disminuir los riesgos se diseñó un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001. Para ello, se aplicó la metodología Magerit, se elaboró el inventario de activos informáticos y de información, se realizó el análisis de riesgos y se propuso políticas y controles de seguridad; además, se elaboró el plan de comunicación y cualificación de los usuarios, con el fin de sensibilizar a todos los usuarios que producen y utilizan información.

Palabras clave

Seguridad informática, Sistema de Gestión de Seguridad de la Información, Análisis de riesgo, Políticas y controles de seguridad, Norma ISO/IEC 27001

Contenidos

El documento se compone de seis capítulos en los que se abordan los siguientes temas:

1. Problema de investigación.
2. Marco referencial.
3. Metodología.
4. Resultados.
5. Conclusiones.
6. Recomendaciones

Problema de investigación

El instituto EDUTEC, como todas las empresas, enfrenta una gran cantidad de amenazas y riesgos informáticos que pueden afectar su buen nombre y su funcionamiento. Dichas amenazas se tornan más graves en función de las prácticas y formas de trabajo que se aplican en el instituto.

Entre otras situaciones, se encontró que un mismo equipo puede ser utilizado por varios usuarios, quienes utilizan memorias USB para transportar sus archivos y hacer uso de ellos en diferentes equipos. Esta forma de uso de los equipos y los dispositivos genera un riesgo de seguridad por cuanto en el evento de que un equipo se infecte con un virus, éste se replicará rápidamente a los demás equipos afectando a toda la institución.

Por otra parte, la institución no cuenta con una política de auditoría o evaluación de la seguridad informática; no se ha llevado a cabo un programa de capacitación y sensibilización sobre seguridad informática con los usuarios de los equipos para que hagan uso más seguro de los mismos y no se cuenta con un manual de buenas prácticas o con políticas y controles de seguridad de la información.

Ante las amenazas de virus, pérdida de información importante y sensible como es el caso de matrículas, notas de los estudiantes, informes para Secretaría de Educación y todos los procesos que se llevan a cabo por todos los actores, es una necesidad apremiante para la institución contar con un Sistema de Gestión de Seguridad de la Información (SGSI), que contribuya a disminuir los riesgos de pérdida o daño de los activos informáticos y de información.

Por lo anterior, se formuló el problema de esta forma:

¿Cómo contribuir a mejorar la Seguridad de la información en el Instituto Edutec de los Andes Pitalito, mediante un Sistema de Gestión de Seguridad de la Información (SGSI) diseñado bajo la norma ISO/IEC 27001?

Objetivos

General

Diseñar un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001.

Específicos

1. Elaborar un inventario de activos informáticos y de información.
2. Realizar un análisis de riesgo informático.
3. Proponer políticas y controles de seguridad de la información y los activos informáticos.
4. Diseñar un plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad contempladas en el SGSI.

Metodología

El proyecto se desarrolló en cuatro fases:

1. Elaboración del inventario de activos informáticos y de información
2. Análisis de riesgo informático, mediante la metodología Magerit, con la información y los activos informáticos, para proceder a identificar las vulnerabilidades y riesgos.
3. Proposición de políticas y controles de seguridad, una vez priorizados los riesgos y con base en la norma ISO 27001, se definieron las políticas de seguridad y los controles a implementar para gestionar los riesgos, teniendo en cuenta el código de buenas prácticas para la gestión de la seguridad norma ISO 27002.
4. Elaboración del plan de comunicación.

Principales Referentes Teóricos y conceptuales

ISO/IEC 27001: Norma que abarca todos los requisitos pertinentes que se deben tener en cuenta en el sistema de gestión de seguridad de la información. Cuenta con el anexo A, que detalla de manera resumida los objetivos de los dominios.
Riesgo: Es la posibilidad de que una amenaza pueda explotar una vulnerabilidad en particular.
Sistema de gestión de seguridad de la información: Principal concepto sobre el que se conforma la norma ISO 27001 en donde se establecen políticas, procedimientos y controles que permite conocer, gestionar y minimizar los posibles riesgos que atentan contra la seguridad de la información.

Resultados

Del 100% de las vulnerabilidades que presenta la metodología Magerit en el catálogo de amenazas que atentan contra los activos del sistema de información, se identificaron 38 vulnerabilidades, con un porcentaje del 42% en el nivel muy alto o catastrófico, un 24% de alto nivel o crítico, 16% medio y 18% bajo, el grupo de amenazas catalogadas así: 16 muy alto, 9 alto, 7 medio, 6 bajo. Se puede evidenciar que es necesario implantar medidas correctivas y preventivas en pro del buen funcionamiento e imagen de la Institución y se recomienda la implementación de un plan de seguridad adecuado.
se propuso políticas y controles de seguridad, se elaboró documento que describe de forma detallada el Plan de comunicación y cualificación de los usuarios, sobre las políticas de seguridad informática contempladas en el sistema de gestión de seguridad de la información (SGSI), para que todos los usuarios las conozcan y las observen.

Conclusiones

Los virus informáticos constituyen una amenaza a tener en cuenta en todas las organizaciones. Sin embargo, en Edutec, ninguna área utiliza un sistema de antivirus con licencia, que cubra las necesidades de seguridad.
El instituto no cuenta con instalación eléctrica regulada ni con sistemas de alimentación ininterrumpida (UPS), lo que implica un alto riesgo para los equipos de cómputo que podrán verse afectados por algún evento relacionado con el suministro eléctrico.

Como resultado del presente proyecto se proporciona al instituto un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2003, es necesario que las directivas lleven a cabo el plan de comunicación y se aseguren de que el SGSI sea implementado.

Recomendaciones

Se recomienda al director de la Institución revisar el Sistema de Gestión de Seguridad que se propone, hacerle los ajustes que consideren necesarios, y proceder a implementarlo.
Se sugiere realizar capacitaciones periódicas a todo el personal sobre las políticas y controles de seguridad. De igual manera, brindar capacitación a personas que se vinculen a la institución.
Estudiar la viabilidad de contratar los servicios de un DLP (Data Loss Prevention) y adquirir un antivirus con licencia, que ofrezcan mayor protección frente a las amenazas.

Fuentes bibliográficas

CISCO. Reporte Anual de Ciberseguridad de Cisco 2018. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018espan.pdf.

ESCRIVÁ, Gema; ROMERO, Rosa y RAMADA, David. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A. Disponible en: http://www.ebrary.com

GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3), IC Editorial, 2014. Disponible en: ProQuest Ebook Central, https://ebookcentral-proquestcom.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=4184155.

GÓMEZ FERNÁNDEZ, Luis y ÁLVAREZ, Ana Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, AENOR - Asociación Española de Normalización y Certificación, 2012. ProQuest Ebook Central, Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3205110.

GÓMEZ FERNÁNDEZ, Luis y RIVERO PEDRO, Pablo Fernández. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2018. Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=5486388.