18th International Conference - Science, Technology and Innovation
Booklets

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Administrative audit tool as support for the iso 27001 standard towards managing the quality of information in smse, 2021

Authors: RUÍZ-TAPIA, Juan Alberto, RUÍZ-VALDÉS, Susana, CRUZ-SOLÍS, Ivett and ALCÁNTARA-CRUZ, Félix Héctor

Editorial label ECORFAN: 607-8695
BECORFAN Control Number: 2021-01
BECORFAN Classification (2021): 131221-0001

Pages: 12
RNA: 03-2010-032610115700-14

Introducción

La seguridad de la información es un aspecto esencial en las actividades y procesos de las organizaciones por lo que es importante implementar medidas de seguridad para mejorar su eficiencia. Algunas empresas no hacen un adecuado uso y/o manejo de su información, por lo que esto facilita la exposición a su vulnerabilidad. Es necesario identificar los activos de información que tienen un impacto significativo en la Organización; realizar un análisis, evaluar el riesgo y decidir cuáles son las opciones de tratamiento a implementar para minimizar las posibilidades de que las amenazas puedan causar daño a la integridad, confidencialidad y disponibilidad de la información a la organización.

Surgen diferentes riesgos en la seguridad de la información por ello la necesidad de proteger los sistemas de información tanto en software como en hardware. Algunas empresas insertan medidas de seguridad para proteger su información, pero en muchas ocasiones son insuficientes con lo que se ve en la necesidad de seguir normas, como la ISO 27001, para prevenir, medir, evaluar y corregir los posibles riesgos que puedan provocar daños irreversibles.

……. **Introducción**

Hoy en día, las investigaciones en el área de la ingeniería de software se centran en el desarrollo de metodologías que garanticen y controlen la calidad en el software desarrollado.

Se pretende disminuir los riesgos informáticos y proponer un plan de tratamiento de riesgos con la ayuda de un software. El alcance del proyecto está limitado por los objetivos de control que se obtienen directamente de la norma ISO 27001:2013.

Los ataques y amenazas contra la seguridad de la información en la mayoría de las Organizaciones no toman muy en serio el riesgo que implica mantener toda esta información desprotegida y no cuentan con las políticas de seguridad que recomiendan las normas internacionales.

……..Introducción

En esta investigación se parte de la identificación de los riesgos, amenazas o vulnerabilidades en la seguridad de la información a los que está expuesta una Organización y que son causados por diversas situaciones dentro de estas organizaciones, proponiendo medidas, procedimientos y controles, para mantener la integridad, confidencialidad y disponibilidad de la información para un funcionamiento positivo dentro de la Organzación y poder minimizar el impacto negativo dentro de estas.

El objetivo de esta investigación fue realizar una aplicación informática para un sistema de gestión de la calidad para la seguridad de la información (SGCSI) aplicado a Empresas basado en norma ISO 27001 para prevenir vulnerabilidades y amenazas sobre la calidad del sistema de seguridad.

Se levantó y analizó la información de las variables documentando los resultados generando una propuesta para otras organizaciones en situaciones similares.

Metodología

Software existente.

El Software ISOTools Excellence para ISO/IEC 27001:2013 para el Sistema de Gestión de Seguridad de la Información o SGSI se encuentra compuesto por diferentes aplicaciones que, al unirlas, trabajan para que la información que manejan las Organizaciones no pierda ninguna de sus propiedades más importantes: disponibilidad, integridad y confidencialidad.

Se analizaron conceptos, definiciones de software, ingeniería de software, aplicaciones de Software, proceso de desarrollo de software, metodología de desarrollo de software, estándares y las normas de seguridad: ISO 27000 para el ciclo de mejora continua de seguridad Plan – Do – Check – Act, ISO 29119 para pruebas de software, ISO 25010 como modelo de calidad del producto software. PMBOOK para la Gestión de Proyectos de Software. ITIL para el soporte y continuidad de servicio TI para la comprobación de aplicaciones web.

….. Metodología

Normas ISO 27001:2013.
Ésta norma es el estándar internacional para la gestión de la seguridad de la información. Define cómo poner en práctica un sistema de gestión de seguridad de la información evaluado independientemente y certificado. Con esta norma, se puede demostrar compromiso y cumplimiento con la mejor práctica global, demostrando a todos los interesados que la seguridad es esencial para la manera en que la Organización opera.

Ésta norma es aplicable a cualquier organización que cuente con sistemas de información. Al cumplirse con las normas legales de protección de datos, se permite reducir los problemas con los involucrados. Ofrece garantía de continuidad en la Organización basándose en el Plan de Contingencias. Aumenta el valor comercial de la empresa así como una gran mejora en su imagen. Aumenta los niveles de confianza entre todos los involucrados. Es una importante mejora continua del SGSI, mediante la aplicación de la metodología PDCA (Planificar, Hacer, Verificar y Actuar).

….. Metodología

El proyecto se desarrolla con un enfoque cuantitativo, donde se van a cuantificar las diferentes propiedades de las variables que intervienen en el proyecto. Es una investigación de tipo descriptivo porque mide las variables para generar datos.

La investigación es no experimental y transversal, se estudian las variables en un tiempo definido. Se determinó la manera más adecuada de medir dicho conjunto de variables para poder dar una visión general del estado de los controles de seguridad de la información y si estos cumplen con la norma ISO/IEC 27001 de 2013 y conservan la calidad de la información.

….. Metodología

El proyecto se desarrolla con un enfoque cuantitativo, donde se van a cuantificar las diferentes propiedades de las variables que intervienen en el proyecto. Es una investigación de tipo descriptivo porque mide las variables para generar datos.

La investigación es no experimental y transversal, se estudian las variables en un tiempo definido. Se determinó la manera más adecuada de medir dicho conjunto de variables para poder dar una visión general del estado de los controles de seguridad de la información y si estos cumplen con la norma ISO/IEC 27001 de 2013 y conservan la calidad de la información.

…… Metodología

El proyecto se estructura por fases:

a).- Se plantea el problema en el cual se pone de evidencia los inconvenientes que actualmente tienen las organizaciones que no cuentan con un Sistema integral de Calidad en la Seguridad de la Información (SICSI) implementado.

b).- Los objetivos de este sistema a desarrollar.

c).- El marco de referencia a partir del cual se logró medir las dimensiones del proyecto.

d).- El marco teórico a partir del cual se logró medir las dimensiones del proyecto para desarrollarlo para implementarse en una empresa y

e).- La solución tecnológica propuesta.

4- Results

Desarrollo de la aplicación informática.

El software permite el establecimiento de medidas de seguridad de la información en cualquier tipo de Organización. Para ello cuenta con un sistema modular que permite el ingreso de información con la colaboración de directivos, jefes de área y personal de apoyo.

Se retroalimenta de información y le permite al encargado de la seguridad de la información realizar un análisis verás y obtener informes inmediatos que le permitirán tomar medidas adecuadas para minimizar los riesgos a los cuales se exponen los activos críticos de información en las Organizaciones, en los diferentes aspectos en la seguridad de una empresa.

…… Results

Desarrollo de la aplicación informática.

Se cuenta con un manual que proporciona la lógica con la cual se ha diseñado el software y sus componentes tecnológicos sobre los cuales funciona correctamente, así como la adecuada instalación de este.

En la aplicación informática que se desarrolló se pueden subir fotos, videos documentos y notas, por medio de una USB o por el teléfono celular. Los documentos que se pueden obtener son: Políticas, Medidas, Procedimientos, Controles, Riesgos, Sugerencias, un Libro conteniendo información sobre cada punto de la Norma ISO 27001 para aclarar más a detalle cualquier duda sobre ella.

Se pueden dar de alta de documentos para una posible auditoría, se pueden imprimir por separado cada uno de los puntos de control de la Norma ISO 27001, se pueden firmar acuerdos y guardarlos por medio de la unión de la aplicación de Adobe Reader,

Se pueden enviar documentos por medio de correo electrónico por cada uno de los puntos de la Norma, obtener informes sobre proveedores de servicios,

Se pueden obtener reportes para la Dirección de la Organización, se pueden obtener informes de seguimiento faltantes por cada punto de la Norma, los diferentes análisis y reportes permiten tomar decisiones oportuna por las diferentes personas involucradas.

…… Results

Reportes del SW.

Los reportes con que cuenta el software son: Planeación del proyecto, Documento sobre el alcance del SGSI, Diagnóstico Inicial, Diagnostico Cuantitativo de SGSI, Política de seguridad de la información, Políticas de Seguridad de la Información, Roles y Responsabilidades, Gestión de Riegos de SGSI, Software Tratamiento Riesgos (Desarrollo propio para gestionar los riesgos), Documentación, Gestión de Riegos de SGSI, Software Tratamiento Riesgos (Desarrollo propio para gestionar los riesgos), Auditoria, Revisión por la Dirección.

4- Conclusions

El modelo del software presentado para la implantación del SGCSI, es una herramienta que ofrece análisis de riesgos, sugerencias específicas, documentación metodológica, revisión frecuente, manejo de no conformidades. En el software desarrollado se realizaron tareas de recolección de información, análisis de datos, comprensión y aplicación de teorías, entre otros, permitieron el intercambio de conocimientos y destrezas. El producto final constituye un software y herramienta de facilitación y consolidación de metas que describen procesos y pautas para apoyar el proceso de implantación del Sistema de medidas de Seguridad de la Información.

Con la aplicación informática presentada en este documento, se proponen diferentes procedimientos, políticas, tipos de controles, medidas de seguridad para el control de la información y los sistemas que son pieza clave en las organizaciones. Después de analizar los riesgos informáticos con los que actualmente las organizaciones tienen que convivir se lograron los siguientes resultados: proponer políticas, medidas, procedimientos y controles para el uso, control y resguardo para la seguridad de la información de los sistemas en la Institución al momento de implantar una aplicación informática del SGCSI, para proteger los riesgos a que están sometidos y al mismo tiempo proponer soluciones que den seguimiento a los posibles problemas presentes y futuros que se presenten.

ECORFAN®