Encuentro de Comunicación, Investigación, Docencia y Extensión

2017

Calbo, Vicente

Encuentro de comunicación, investigación, docencia y extensión / Vicente Calbo ; María Cecilia Baldo. - 1a ed compendiada. - La Rioja : Suyay, 2021.

Libro digital, PDF

Archivo Digital: descarga y online

ISBN 978-987-48010-1-2

1. Actas de Congresos. I. Baldo, María Cecilia. II. Título.

CDD 507.2

IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE LA UTN FACULTAD REGIONAL LA RIOJA

Lucero, Emilce Beatriz [(1)] **– Garbozo, Ana Carolina** [(2)]

[(1)] Departamento Ingeniería Electrónica
[(2)] Ministerio de Planeamiento e Industria – Gobierno de la Provincia de La Rioja

bealucero@yahoo.com.ar
caroge87@gmail.com

Resumen: En la actualidad las actividades cotidianas de las empresas, de las distintas Administraciones Públicas y de muchas otras instituciones u organizaciones, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y en especial de su seguridad.

Introducción: La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el *hacking* o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

La seguridad informática es la protección que se debe dar a la información para que esta no sea tratada de forma indebida, como el ser revelada, modificada, o destruida de manera accidental o intencional, a través de las normas o medidas que son necesarias para dar la protección adecuada para que no exista el acceso no autorizado, la interferencia accidental o intencionada con operaciones normales.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) es una decisión estratégica de negocio, que se ve influenciada por las necesidades, objetivos, requisitos de seguridad y los procesos de la organización.

Estado actual de conocimiento: Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad (medidas conocidas como su acrónimo "CIA" en inglés "Confidentiality, Integrity, Availability"), así como de los sistemas implicados en su tratamiento, dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Objetivo: Implementar un sistema de Gestión de la Seguridad de la información para la intranet de la UTN –FRLR con el fin de lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos.

Metodología de Trabajo: Para ello se toma como base la norma ISO 27001, se realiza un análisis preventivo y correctivo en la mejora de la administración y gestión de la intranet, identificando las vulnerabilidades presentes en la organización. El proyecto consta de los siguientes pasos o etapas:

Etapa 1: Análisis de la situación de la intranet de la UTN-FRLR

Etapa 2: Definir el alcance de SIGSI

Etapa 3: Identificación, Análisis y Evaluación de Vulnerabilidades en la Intranet

Etapa 4: Implementación del SIGSI en la intranet

Etapa 5: Elaboración de la documentación correspondiente

Contribuciones del proyecto: La principal contribución es la generación e implementación de un sistema de gestión de la seguridad en la Facultad, que ayudará a establecer políticas y procedimientos de seguridad en relación a sus objetivos, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia institución ha decidido asumir.