Resumen

La Cultura de Ciberseguridad se ha convertido en un elemento clave para la gestión de riesgos informáticos a nivel organizacional. El siguiente resumen destaca los puntos críticos, las tácticas empleadas y los beneficios de la creación de este modelo, ofreciendo una perspectiva general del camino hacia una cultura de ciberseguridad sólida y adaptable. En este estudio se elaboró un modelo de la cultura de ciberseguridad aplicable a Instituciones de Educación Superior. La metodología consistió en una extensa revisión bibliográfica de nueve modelos de madurez de ciberseguridad, y a su vez se aplicó el método ecléctico, el cual consiste en la combinación de elementos de diversas fuentes. A partir de esto se definen siete componentes principales: gobernabilidad y controles organizacionales, capacitación y concienciación en habilidades de ciberseguridad, marco jurídico y normativo de la estrategia de ciberseguridad, gestión de activos tecnológicos, gestión de usuarios y accesos, estrategias de gestión de riesgos y amenazas, protección de la información y procedimientos. Estos componentes abarcan controles relacionados a los distintos grupos ocupacionales dentro de una Institución de Educación Superior. Para el modelo se definen también los niveles de madurez, que se obtienen mediante la misma metodología, entonces se tienen seis niveles, empezando con el nivel 0– Cultura inexistente, nivel 1–inicial, nivel 2–Planificado, nivel 3– Establecido, nivel 4–Certificado y nivel 5–Innovado, siendo el nivel 0 el más bajo y el indicativo de una cultura de ciberseguridad deficiente o casi inexistente; y el nivel 5, el nivel de madurez más alto, que representa una cultura bien cimentada, definida, y en proceso de mejora continua.

Palabras clave: Ciberseguridad, Modelo de Madurez, ISO 27001, Cultura de Ciberseguridad, Institución de Educación Superior.

Abstract

Cybersecurity Culture has become a key element in managing IT risk at the organizational level. The following summary highlights the critical points, tactics employed, and benefits of creating this model, providing an overview of the path to a robust and adaptive cybersecurity culture. This study developed a model of cybersecurity culture applicable to Higher Education Institutions (HEIs). The methodology consisted of an extensive literature review of nine models on the topic of cybersecurity maturity models, and in turn the eclectic method was applied, which consists of combining elements from various sources, from this seven main components are defined: Organizational governance and controls, Cybersecurity skills training and awareness, Legal and regulatory framework of the cybersecurity strategy, Technology asset management, User and access management, Risk and threat management strategies, Information protection and procedures. These components cover controls related to the different occupational groups within a Higher Education Institution. For the model, the maturity levels are also defined, which are obtained through the same methodology, so there are six levels, starting with Level 0 - non-existent culture, Level 1 - initial, Level 2 - planned, Level 3 - established, Level 4 - certified and Level 5 - innovated, with Level 0 being the lowest level of maturity and indicative of a deficient or almost non-existent cybersecurity culture; and Level 5, the highest maturity level, representing a culture that is well established, defined, and in the process of continuous improvement.

Keywords: Cybersecurity, Maturity Model, ISO 27001, Cybersecurity Culture, Higher Education Institution.