

Resumen

Este proyecto se enfocó en la minería de procesos relacionados con la seguridad de la información. El objetivo fue realizar una Minería de Procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el Servicio de Acceso a Internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000. La minería de procesos se llevará a cabo utilizando la metodología ProM. La investigación se enfocará en una empresa que ofrece servicios de acceso a internet. Aunque tanto los usuarios como los proveedores de servicios son conscientes de la importancia de la seguridad de la información, los proveedores hacen esfuerzos para minimizar las amenazas. Sin embargo, las estrategias implementadas no siempre están alineadas con una norma internacional. Por eso, la minería de procesos propuesta se basará en el estándar ISO-27001, lo que permitirá una mejor aplicación de las estrategias mencionadas. Para los proveedores de servicios de acceso a internet, es crucial minimizar los impactos de los ataques informáticos. Sin embargo, no cuentan con procesos específicos para reducir estos impactos. Por ello, es necesario establecer procesos prácticos basados en una normativa internacional. El modelado para descubrir, mejorar y controlar procesos se convierte en una herramienta esencial para la toma de decisiones en todos los niveles de gestión.

Palabras clave: ciberseguridad, minería de datos, ataques Informáticos, minería de procesos

Abstract

This project focused on data mining related to information security. The objective was to perform process mining applied to cybersecurity—specifically regarding attack incidents—at a company that provides Internet access services, using the ProM tool and in accordance with the ISO 27000 standard. The process mining will be carried out using the ProM methodology. The research will focus on a company that provides internet access services. Although both users and service providers are aware of the importance of information security, providers make efforts to minimize threats. However, the strategies implemented are not always aligned with an international standard. Therefore, the proposed process mining will be based on the ISO-27001 standard, which will allow for better implementation of the aforementioned strategies. For internet access service providers, it is crucial to minimize the impacts of cyberattacks. However, they lack specific processes to reduce these impacts. Therefore, it is necessary to establish practical processes based on an international standard. Modeling to discover, improve, and control processes becomes an essential tool for decision-making at all management levels.

Keywords: cybersecurity, data mining, computer attacks, process mining