UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Gabriela Cristina Egüez Cruz
Luis Humberto Gortaire Delgado
María Del Rosario Soria Soria
Nelson Wladimir Trujillo Guerrón
TUTOR: Ing. Jaime Bladimir Ibarra Jiménez

Integración de herramienta SIEM para monitoreo de Bases de Datos No Relacionales en la nube de AWS

Resumen

La tesis se centra en la integración de una herramienta SIEM para monitorear bases de datos no relacionales en la nube de AWS, abordando la necesidad de mejorar la seguridad de la información en un entorno digitalizado. Se plantea como incógnita la efectividad de los SIEM para cumplir con la normativa ISO 27001 y la legislación local sobre protección de datos. La investigación busca desarrollar una solución efectiva para la monitorización y protección de bases de datos en la nube, utilizando herramientas SIEM y cumpliendo con aspectos específicos de la normativa ISO 27001. Se destacan los conceptos fundamentales de seguridad de la información, infraestructura en la nube y sistemas SIEM, así como la importancia de la integración de estos elementos para fortalecer la postura de seguridad de las organizaciones. El proyecto se enfoca en la implementación de la herramienta SIEM Splunk con AWS y MongoDB, con el objetivo de crear reglas y alertas de seguridad para la base de datos. Se propone una metodología de evaluación de riesgos y un plan de proyecto detallado, con consideraciones éticas, sociales, legales y de seguridad. En resumen, la tesis proporciona una guía completa para abordar el problema de seguridad de la información en un entorno cloud, con un enfoque práctico y fundamentado en la teoría.

Abstract

This thesis focuses on the integration of a SIEM tool to monitor non-relational databases in the AWS cloud, addressing the need to enhance information security in a digitalized environment. The effectiveness of SIEM tools in complying with ISO 27001 standards and local legislation on data protection is questioned. The research aims to develop an effective solution for monitoring and protecting databases in the cloud, using SIEM tools and complying with specific aspects of ISO 27001 standards. Fundamental concepts of information security, cloud infrastructure, and SIEM systems are highlighted, emphasizing the importance of integrating these elements to strengthen organizations' security posture. The project focuses on implementing the SIEM tool Splunk with AWS and MongoDB, aiming to create security rules and alerts for the database. A risk assessment methodology and a detailed project plan are proposed, along with ethical, social, legal, and security considerations. In summary, the thesis provides a comprehensive guide to addressing the information security problem in a cloud environment, with a practical approach grounded in theory.