UIDE
Powered by
Arizona State University

Maestría en

# CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

**AUTORES:** Ing. Luis Bayron Guachamin Escorza
Ing. Silvana Estefanía Ortega Ramírez
Ing. Raúl Alejandro Páez Andrade
Ing. Gabriel Andrés Requelme Rodríguez

**DIRECTOR:** Alejandro Cortés López

## Evaluación de la eficiencia de una herramienta SIEM (Security Information and Event Management) en la detección y respuesta de amenazas en la base de datos transaccional de una institución financiera.

QUITO – ECUADOR | 2023

## Resumen

El presente trabajo tiene como objeto evaluar la eficiencia de una herramienta SIEM en la detección y respuesta de amenazas en la base de datos transaccional de una institución financiera. El área de sistemas responsable del manejo de datos tiene la obligación de garantizar que la información cumpla con criterios de confidencialidad, integridad y disponibilidad. Si bien hasta el momento, no se han identificado ataques o amenazas a la base de datos transaccional, se requiere incluir en el análisis de seguridad una herramienta que permita la detección de incidentes.

Al no contar con el análisis adecuado de eventos relacionados con la base de datos transaccional, es necesario integrar la herramienta SIEM. Por tanto, surge la necesidad de implementar una gestión automatizada para administrar los eventos y así incrementar los niveles de seguridad.

Para resolver esta necesidad, se realizará un análisis de eficiencia con la herramienta SIEM actual de la entidad financiera. Durante este análisis, se definirán reglas y alertas personalizadas capaces de identificar comportamientos sospechosos en las bases de datos.

Previo a su integración, se realizarán varios simulacros en entornos de prueba para evaluar la eficiencia de la SIEM. Cada evento se documentará debidamente para realizar los ajustes necesarios en la herramienta.

## Abstract

The purpose of this work is to evaluate the efficiency of a SIEM tool in detecting and responding to threats in the transactional database of a financial institution. Within the financial institution, the systems area is responsible for data management, therefore, it is its obligation to guarantee that the information meets confidentiality, integrity, and availability criteria. So far, no attacks or threats to the transactional database have been identified, but it is necessary to include a tool in the security analysis that allows the detection of incidents.

Lacking adequate analysis of events related to the transactional database, it is necessary to integrate the SIEM tool. Therefore, the need arises to implement automated management to manage events and thus increase security levels.

To resolve this need, an efficiency analysis will be carried out with the financial institution's current SIEM tool. During this analysis, custom rules and alerts will be defined capable of identifying suspicious behavior in the databases.

Prior to its integration, several simulations will be carried out in test environments to evaluate the efficiency of the SIEM. Each event will be properly documented to make the necessary adjustments to the tool.