UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ibujés Marcelo

Larrea John

Maldonado Daniela

Matute Ronald

TUTOR: Ing. Ronie Stalin Martínez Gordon, Mtr.

"Evaluación de SIEM en el Cumplimiento Normativo: Un Enfoque Integral en Ciberseguridad Empresarial"

Resumen

En el presente proyecto de titulación "Evaluación de SIEM en el Cumplimiento Normativo: Un Enfoque Integral en Ciberseguridad Empresarial", buscamos investigar y validar la efectividad de las herramientas SIEM (SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD) en el contexto actual de las amenazas cibernéticas y crecientes exigencias normativas, que para el caso de nuestro estudio hemos tomado la ISO 27001 y la nueva Ley Orgánica de Protección de Datos Personales del Ecuador.

Esta investigación aborda el entorno relacionado con la protección de datos y la confidencialidad de la información, destacando la eficacia de las tecnologías SIEM en el campo normativo y la salvaguarda de datos confidenciales; evaluando reglas, teorías, conceptos y prácticas asociadas con esta tecnología.

El enfoque metodológico incluye el análisis de un ambiente en producción, la revisión de literatura y consultas a entendidos en el manejo de estas herramientas y lo que constituye la seguridad de la información. Nuestra investigación busca proporcionar visibilidad de las herramientas para poder fortalecer la postura de las organizaciones frente a amenazas cibernéticas y requisitos normativos en evolución constante. En última instancia, se espera que los resultados obtenidos en este trabajo aporten a la mejora continua de las estrategias de seguridad de la información en el ámbito organizacional de las empresas y en especial para nuestro colaborador ITSISTEMAS.

Palabras clave: implementación del SIEM, Wazuh, ISO 27001, LOPDP

Abstract

In this degree project "Evaluation of SIEM in Regulatory Compliance: A Comprehensive Approach to Business Cybersecurity", we seek to investigate and validate the effectiveness of SIEM tools (SECURITY INFORMATION SYSTEMS AND EVENTS) in the current context of cyber threats, and increasing regulatory demands, which in the case of our study we have taken ISO 27001 and the recent Organic Ley Orgánica de Protección de Datos Personales del Ecuador.

This research addresses the environment related to data protection and information confidentiality, highlighting the effectiveness of SIEM technologies in the regulatory field and the safeguarding of confidential data; evaluating rules, theories, concepts and practices associated with this technology.

The methodological approach includes the analysis of a production environment, the review of literature and consultations with experts in the management of these tools and what constitutes information security. Our research seeks to provide visibility into tools to strengthen organizations' posture against cyber threats and evolving regulatory requirements. Ultimately, it is expected that the results obtained in this work will contribute to the continuous improvement of information security strategies in the organizational field of companies and especially for our collaborator ITSISTEMAS.

KEYWORDS: SIEM implementation, wazuh, ISO 27001, LOPDP