www.revistaft.com.br

RevistaFT | ISSN 1678-0817 | v.30, n. 160, 2026 | DOI: 10.69849/6vjdy872

Protecting SAP cloud environments: a risk-based approach to secure enterprise systems

Proteção de ambientes SAP em nuvem: uma abordagem baseada em riscos para a segurança de sistemas empresariais

Thiago Manzaro Serain[1]

Abstract

In recent years, organizations have increasingly migrated enterprise systems to cloud platforms, significantly transforming how operational and financial processes are managed. With the adoption of modern solutions such as SAP S/4HANA, new security challenges emerge, particularly in areas such as access control, identity governance, and monitoring of privileged activities. This article aims to analyze the main security challenges in SAP cloud environments and propose a risk-based approach that integrates governance, access control, and continuous monitoring. The methodology is based on conceptual review and analysis of market practices aligned with international security frameworks. The results indicate that implementing structured governance models enhances organizational resilience against cyber threats while ensuring compliance with global standards. It is concluded that security in SAP cloud environments is essential for protecting critical systems and ensuring business continuity.

Keywords: SAP Security; SAP Cloud; Access Governance; Cybersecurity; Identity Management

Resumo

Nos últimos anos, as organizações têm migrado cada vez mais seus sistemas empresariais para plataformas em nuvem, transformando significativamente a forma como os processos

[1] ORCID: https://orcid.org/0009-0002-1948-1206

operacionais e financeiros são gerenciados. Com a adoção de soluções modernas, como o SAP S/4HANA, surgem novos desafios de segurança, especialmente nas áreas de controle de acesso, governança de identidades e monitoramento de atividades privilegiadas. Este artigo tem como objetivo analisar os principais desafios de segurança em ambientes SAP em nuvem e propor uma abordagem baseada em riscos que integre governança, controle de acesso e monitoramento contínuo. A metodologia baseia-se em revisão conceitual e análise de práticas de mercado alinhadas a estruturas internacionais de segurança da informação. Os resultados indicam que a implementação de modelos estruturados de governança fortalece a resiliência organizacional frente às ameaças cibernéticas, ao mesmo tempo em que assegura a conformidade com padrões internacionais. Conclui-se que a segurança em ambientes SAP em nuvem é essencial para a proteção de sistemas críticos e para a continuidade dos negócios.

Palavras-chave: segurança em SAP; SAP em nuvem; governança de acesso; cibersegurança; gestão de identidades.

Introduction

Enterprise resource planning (ERP) systems have become fundamental components of modern organizational infrastructure, integrating critical functions such as financial management, supply chain, and compliance processes. Among these solutions, SAP platforms stand out, widely adopted by large organizations due to their ability to support complex operations and high transaction volumes.

With the advancement of digital transformation, many companies have migrated their SAP environments to cloud infrastructures, including hybrid and distributed architectures. While this evolution provides scalability and operational efficiency, it also expands the attack surface and introduces new security challenges.

In this context, this article aims to analyze the security challenges in SAP cloud environments and propose a risk-based approach to protecting these systems.

Literature review

Literature on ERP systems highlights their relevance in integrating organizational processes and improving operational efficiency. However, these systems are also critical targets of cyber threats due to the high value of the data they store.

Security in SAP environments involves practices such as access control, segregation of duties (SoD), identity governance, and monitoring of privileged activities. With migration to the cloud, these challenges become more complex, requiring new governance approaches.

International frameworks such as NIST, ISO/IEC 27001, and COBIT provide guidelines for risk management, access control, and continuous monitoring, and are widely used to strengthen the security of corporate systems.

Methodology

This study adopts a qualitative approach based on conceptual review and analysis of market practices. International information security frameworks were considered, as well as technological solutions used in SAP environments.

The analysis focuses on identifying the main risks associated with SAP cloud environments and proposing a risk-based governance model, integrating access control, identity management, and continuous monitoring.

Results and discussion

The results indicate that the main vulnerability in SAP cloud environments is related to inadequate identity and access management. In large organizations, the complexity increases due to the high number of users, integrated systems, and distributed processes.

The absence of adequate controls can result in the accumulation of privileges, conflicts over the segregation of duties, and risks of unauthorized access to sensitive data.

Adopting a risk-based approach allows for prioritizing the most critical controls, aligning security with business impact. This model integrates:

* governance and compliance

Identity management

* access control

* continuous monitoring

Furthermore, strengthening security in SAP systems directly contributes to the protection of critical infrastructure, including supply chains, financial operations, and industrial processes.

Conclusion

Migrating SAP systems to cloud environments represents a significant evolution in how organizations operate. However, this transformation brings new security challenges that require structured and integrated approaches.

Implementing a risk-based security model strengthens control over SAP environments, reducing vulnerabilities and increasing organizational resilience.

In conclusion, security in SAP environments is not just a technical necessity, but a strategic factor in ensuring business continuity and protecting critical systems in the context of the digital economy.

References

Basel Committee on Banking Supervision. (2018). Cyber resilience: Range of practices.

ENISA. (2020). Cloud security guidelines.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives.

ISO/IEC. (2022). ISO/IEC 27001: Information Security Management Systems.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

NIST. (2020). Security and Privacy Controls for Information Systems (SP 800-53).

SAP SE. (2023). SAP Security Guide for SAP S/4HANA.