INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

MELHORES PRÁTICAS DE SEGURANÇA CIBERNÉTICA NO SUPORTE TÉCNICO DE SISTEMAS SAP: PREVENÇÃO DE VULNERABILIDADES NA ESTAÇÃO DE TRABALHO

https://doi.org/10.56238/isevmjv2n1-021

Recebimento dos originais: 10/01/2023 **Aceitação para publicação:** 29/01/2023

Roberto de Carvalho Silva

RESUMO

A segurança cibernética no suporte técnico de sistemas SAP é uma preocupação fundamental para as empresas devido à crescente complexidade das ameaças cibernéticas e ao papel crucial que os aplicativos SAP desempenham nas operações de negócios. As estações de trabalho utilizadas no suporte técnico representam vetores de ataque significativos, principalmente durante os procedimentos de instalação, atualizações e manutenção. Essas vulnerabilidades, se não forem gerenciadas adequadamente, podem levar a acesso não autorizado, violações de dados e interrupções operacionais. Garantir uma segurança robusta em ambientes de suporte técnico SAP requer uma abordagem proativa que integre controle de acesso, gerenciamento de patches, proteção de endpoint e medidas de segurança de dados.

Este estudo explora as melhores práticas de segurança cibernética para suporte técnico do sistema SAP, com foco na mitigação de vulnerabilidades da estação de trabalho. As principais recomendações incluem a implementação de autenticação multifator (MFA) e controle de acesso baseado em função (RBAC) para restringir o acesso não autorizado. O estudo destaca a necessidade de sistemas automatizados de gerenciamento de patches para reduzir a exposição a ataques baseados em exploits e a importância de estratégias de proteção de endpoint, como soluções antivírus de última geração e ferramentas de detecção e resposta de endpoint (EDR). Além disso, técnicas de criptografia e tecnologias de prevenção de perda de dados (DLP) são identificadas como medidas cruciais para proteger dados comerciais confidenciais.

Uma revisão da literatura recente apóia essas descobertas, demonstrando como as organizações que adotam monitoramento de segurança orientado por IA e arquiteturas de confiança zero alcançam maior resiliência de segurança cibernética. Estudos enfatizam que as soluções de segurança tradicionais são inadequadas para lidar com ameaças cibernéticas modernas, defendendo a integração da detecção de ameaças baseada em comportamento e avaliações contínuas de segurança.

Em conclusão, as empresas devem adotar uma abordagem de segurança em várias camadas, combinando soluções técnicas avançadas com treinamento contínuo de funcionários e monitoramento proativo de ameaças. Ao promover uma cultura de segurança em primeiro lugar e refinar as estruturas de segurança em resposta a ameaças emergentes, as organizações podem proteger efetivamente seus ambientes SAP contra riscos cibernéticos e manter a integridade operacional.

Palavras-chave: Cibersegurança. Sistemas SAP. Segurança da estação de trabalho. Suporte técnico.

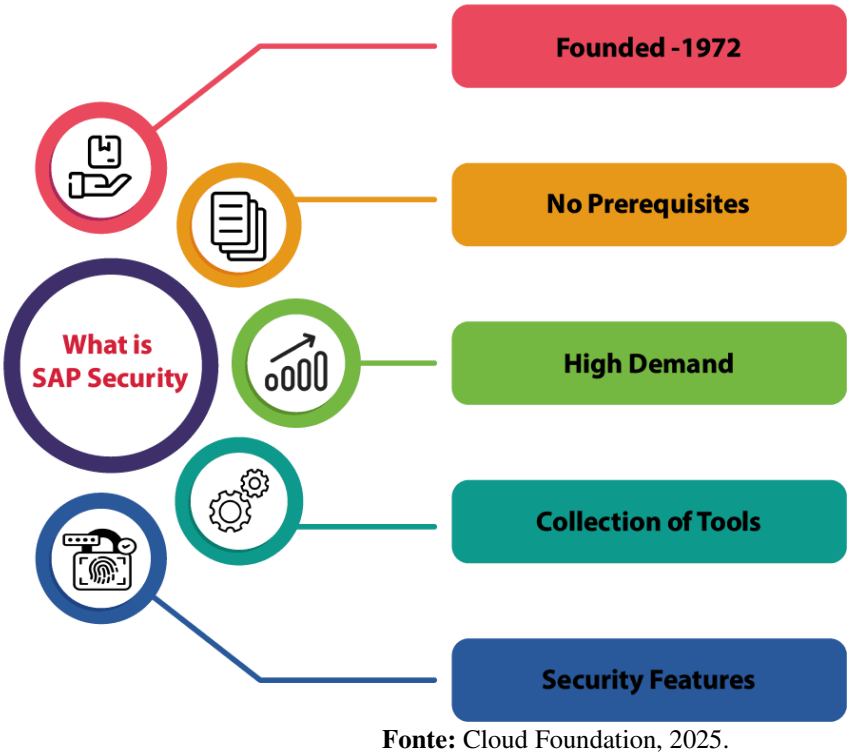
INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

1 INTRODUÇÃO

A segurança cibernética no suporte técnico de sistemas SAP é um aspecto crítico do gerenciamento de TI empresarial. A crescente complexidade das ameaças cibernéticas e o papel crucial que os aplicativos SAP desempenham nas operações de negócios exigem medidas de segurança rigorosas. As estações de trabalho usadas no ambiente de suporte técnico representam um vetor de ataque significativo, principalmente durante os processos de instalação, atualização e manutenção. Qualquer vulnerabilidade de segurança nesses processos pode potencialmente expor dados comerciais confidenciais, interromper operações e levar a perdas financeiras. O cenário de ameaças está em constante evolução, tornando essencial que as organizações implementem protocolos de segurança robustos para mitigar os riscos de forma eficaz.

O sistema SAP Security consiste em vários componentes, sendo a autorização do sistema um elemento crítico. Em sua essência, ele se concentra na definição de funções e permissões de usuário dentro da hierarquia do sistema. Essa estrutura garante que os indivíduos recebam níveis variados de acesso, permitindo que os administradores apliquem medidas de segurança e mantenham as práticas recomendadas por meio de regras e processos relacionados à autorização do sistema.

Figura 1: Segurança do SAP.



Fonte: Cloud Foundation, 2025.

As equipes de suporte técnico responsáveis pelos sistemas SAP geralmente operam em ambientes de alta pressão, onde são necessárias soluções rápidas de problemas e resolução de problemas do sistema. No entanto, a urgência de resolver problemas não deve ser feita à custa da segurança. Os cibercriminosos frequentemente exploram erros humanos, software desatualizado e controles de acesso fracos para obter acesso não autorizado a sistemas corporativos. Ao aplicar fortes medidas de segurança, as organizações podem garantir que suas operações de suporte técnico permaneçam resilientes contra ameaças cibernéticas. Este artigo discute as melhores práticas em segurança cibernética para evitar vulnerabilidades em ambientes de suporte técnico SAP, com foco na proteção de estações de trabalho e na mitigação de riscos durante as atividades de manutenção.

Um aspecto fundamental da segurança cibernética no suporte SAP é o controle de acesso. O acesso privilegiado deve ser limitado estritamente ao pessoal autorizado, e a autenticação multifator (MFA) deve ser imposta para evitar logins não autorizados. Além disso, o RBAC (controle de acesso baseado em função) deve ser usado para garantir que a equipe de suporte tenha apenas as permissões mínimas necessárias para executar suas tarefas. Mecanismos de registro e monitoramento devem estar em vigor para rastrear as atividades do usuário e detectar anomalias em tempo real.

O gerenciamento de patches é outro elemento crucial para proteger as estações de trabalho de suporte SAP. A aplicação oportuna de patches de segurança é essencial para mitigar vulnerabilidades que podem ser exploradas por cibercriminosos. As soluções automatizadas de gerenciamento de patches devem ser integradas aos ambientes de suporte SAP para garantir que as atualizações sejam implementadas de forma consistente em todos os sistemas relevantes. Além disso, essas atualizações devem ser exaustivamente testadas em um ambiente controlado antes da implantação em sistemas de produção para evitar interrupções.

As estratégias de proteção de endpoint são vitais para proteger as estações de trabalho usadas no suporte SAP. Essas estratégias incluem a implantação de soluções antivírus de última geração, ferramentas de detecção e resposta de endpoint (EDR) e firewalls baseados em host. As políticas de segurança devem impor controles de execução rígidos para evitar instalações de software não autorizadas que possam introduzir malware. Além disso, as estações de trabalho devem ser configuradas para limitar a execução de scripts e macros que possam ser explorados em ataques cibernéticos.

Medidas de proteção de dados devem ser implementadas para proteger informações comerciais e de clientes confidenciais. A criptografia deve ser usada para proteger os dados em

trânsito e em repouso, enquanto políticas rígidas de acesso a dados devem ser aplicadas. As tecnologias de prevenção contra perda de dados (DLP) podem ajudar a monitorar e controlar os fluxos de dados, evitando acessos não autorizados ou vazamentos. Auditorias de segurança regulares devem ser realizadas para garantir a conformidade com os requisitos corporativos e regulamentares de proteção de dados. O objetivo deste trabalho é analisar e propor medidas eficazes de segurança cibernética que as equipes de suporte técnico possam adotar para aumentar a segurança dos ambientes SAP, garantindo a conformidade com os padrões da indústria e minimizando a exposição a riscos cibernéticos.

Estudos recentes destacam a importância da segurança cibernética em ambientes de suporte a sistemas SAP. Johnson e Smith (2020) enfatizam o papel da segurança de endpoint na mitigação de riscos cibernéticos, demonstrando como as soluções avançadas de EDR podem identificar e neutralizar proativamente ameaças direcionadas às estações de trabalho de suporte SAP. Seu estudo fornece evidências empíricas mostrando que as empresas que investem em tecnologias EDR experimentam uma redução significativa nas taxas de sucesso de ataques. Eles argumentam que o software antivírus tradicional não é mais suficiente contra ameaças sofisticadas e que as organizações devem adotar métodos de detecção mais avançados e baseados em comportamento para proteger as estações de trabalho SAP.

A segurança cibernética no suporte técnico de sistemas SAP é uma preocupação crítica para as empresas que contam com essa plataforma para gerenciamento de processos de negócios. Com a constante evolução das ameaças cibernéticas e o papel central que os sistemas SAP desempenham nas operações de negócios, é essencial implementar medidas de segurança robustas. As estações de trabalho utilizadas pelas equipes de suporte técnico são pontos críticos, principalmente durante os processos de instalação, atualização e manutenção. Vulnerabilidades nessas áreas podem expor dados confidenciais e causar interrupções operacionais significativas. Portanto, fortalecer a segurança em torno dessas estações de trabalho torna-se um aspecto crucial na mitigação dos riscos de ataques cibernéticos.

O gerenciamento de patches é fundamental para proteger os sistemas SAP contra vulnerabilidades conhecidas. Nagy (2021) enfatiza que os ataques cibernéticos geralmente exploram falhas que já foram identificadas no software, especialmente quando os patches não são aplicados em tempo hábil. O gerenciamento eficaz de patches envolve a automação do processo para garantir que todas as atualizações de segurança sejam implementadas de forma consistente. Além disso, é crucial testar essas atualizações em ambientes controlados antes de aplicá-las aos sistemas de produção para evitar impactos inesperados. Sem uma abordagem estruturada para o

gerenciamento de patches, a superfície de ataque dos sistemas SAP aumenta, tornando-os alvos fáceis para os cibercriminosos.

O controle de acesso e a autenticação também são essenciais para garantir que apenas usuários autorizados possam acessar dados e processos críticos. Bosch (2023) destaca a importância de um sistema de controle de acesso baseado em função (RBAC) que atribui permissões específicas com base nas responsabilidades dos usuários. A implementação da autenticação multifator (MFA) adiciona uma camada extra de segurança, exigindo várias formas de autenticação além de apenas uma senha. Essas práticas reduzem significativamente o risco de acesso não autorizado e fortalecem as defesas contra ataques cibernéticos.

O monitoramento contínuo das atividades nos sistemas SAP é essencial para detectar e responder a atividades suspeitas. Ramo (2023) enfatiza que as ferramentas de detecção de ameaças e análise comportamental podem identificar padrões incomuns de acesso ou uso de dados. A detecção precoce de atividades maliciosas permite uma resposta rápida, minimizando o impacto de possíveis violações. Investir em sistemas avançados de monitoramento é vital para proteger dados confidenciais e manter a integridade do sistema.

A criptografia é uma das principais defesas para proteger dados em sistemas SAP. Garantir que os dados sejam protegidos em trânsito e em repouso é essencial para evitar o acesso não autorizado. Ramo (2023) destaca que a criptografia garante que apenas partes autorizadas possam acessar ou descriptografar informações confidenciais. A implementação de práticas eficazes de criptografia é fundamental para a proteção de dados e a manutenção da confiança do cliente.

Configurações inadequadas ou manutenção de configurações padrão podem aumentar a vulnerabilidade dos sistemas SAP. Mosley (2024) recomenda seguir as diretrizes de segurança fornecidas pelo SAP, desativar serviços desnecessários e aplicar as configurações de segurança apropriadas. A proteção do sistema, que envolve a aplicação estrita de políticas de segurança, deve ser uma prática contínua. Essas medidas ajudam a minimizar a exposição a ameaças e proteger dados confidenciais.

A análise contínua de códigos personalizados é vital para identificar e resolver vulnerabilidades introduzidas durante o desenvolvimento. Schneider-Simon (2022) sugere que auditorias regulares do código-fonte, juntamente com práticas de desenvolvimento seguro, devem ser parte integrante da estratégia de segurança. As ferramentas automatizadas de análise de código podem ajudar a identificar possíveis vulnerabilidades, garantindo que os desenvolvedores sigam as melhores práticas de segurança.

A educação contínua dos funcionários é crucial para prevenir incidentes de segurança. Nagy (2021) destaca que muitos incidentes são causados por erros humanos, como manuseio incorreto de senhas ou interação com e-mails de phishing. A implementação de programas de treinamento que abrangem práticas de segurança, identificação de ameaças e uso adequado de ferramentas de segurança pode reduzir significativamente esses riscos. Funcionários bem informados são uma linha crítica de defesa contra ataques cibernéticos.

O gerenciamento de acesso privilegiado é fundamental para garantir que apenas pessoal autorizado possa executar tarefas críticas. Bosch (2023) usa o Microsoft Entra Privileged Identity Management (PIM) para gerenciar e atribuir funções a usuários e grupos, permitindo que eles executem ações privilegiadas somente quando necessário. Essas práticas reduzem o risco de abuso de privilégios e fortalecem a segurança geral do sistema.

Em conclusão, garantir a segurança cibernética no suporte técnico de sistemas SAP requer uma abordagem multifacetada que inclui controle de acesso, gerenciamento de patches, proteção de endpoint e segurança de dados. A implementação de práticas recomendadas e o aproveitamento de tecnologias de segurança modernas podem mitigar significativamente as vulnerabilidades nas estações de trabalho usadas para tarefas de suporte SAP. Dada a natureza evolutiva das ameaças cibernéticas, as organizações devem avaliar e aprimorar continuamente suas estruturas de segurança para proteger seus ambientes SAP de forma eficaz.

Além disso, a segurança cibernética no suporte técnico SAP deve ser tratada como um processo contínuo, e não como uma implementação única. As organizações devem investir em programas de treinamento contínuo de funcionários para aumentar a conscientização sobre segurança entre o pessoal de suporte. Além disso, os planos de resposta a incidentes devem ser atualizados regularmente para garantir uma reação rápida e coordenada às violações de segurança. Ao promover uma cultura de segurança em primeiro lugar e adotar uma abordagem proativa, as empresas podem reduzir significativamente sua exposição a riscos cibernéticos e proteger a integridade de seus ambientes SAP.

REFERÊNCIAS

ANTONIO, S. L. Inovações tecnológicas e desafios geomecânicos na perfuração da bacia de Midland. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 3, e78097, 2025. DOI: 10.34117/bjdv11n3-005.

BOSCH. Segurança em sistemas SAP: como a Bosch usa as melhores práticas para proteger seus dados. Média, 2023. Disponível em: https://medium.com/@boschtechbr/security-in-sap-systems-how-bosch-uses-best-practices-to-protect-its-data-ff7fe0975e7f. Acesso em: 31 mar. 2025.

CLOUDFOUNDATION. O que é segurança SAP? 2025. Disponível em: https://cloudfoundation.com/blog/what-is-sap-security/. Acesso em: 31 mar. 2025.

DELCI, C. A. M. A eficácia do Last Planner System (LPS) no gerenciamento de projetos de infraestrutura. Revista Sistemática, v. 15, n. 2, p. 133–139, 2025. DOI: 10.56238/rcsv15n2-009.

FILHO, W. L. R. O papel da arquitetura Zero Trust na segurança cibernética moderna: integração com IAM e tecnologias emergentes. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 1, e76836, 2025. DOI: 10.34117/bjdv11n1-060.

FILHO, W. L. R. O papel da IA no aprimoramento dos sistemas de gerenciamento de identidade e acesso. Sete Revistas Internacionais de Multidisciplinaridade, v. 1, n. 2, 2025. DOI: 10.56238/isevmjv1n2-011.

FREITAS, G. B.; RABELO, E. M.; PESSOA, E. G. Projeto modular com reaproveitamento de container marítimo. Brazilian Journal of Development, Curitiba, v. 9, n. 10, p. 28303–28339, 2023. DOI: 10.34117/bjdv9n10-057.

GARCIA, A. G. O impacto das práticas sustentáveis no bem-estar dos funcionários e no sucesso organizacional. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 3, e78599, 2025. DOI: 10.34117/bjdv11n3-054.

MOREIRA, C. A. Monitoramento digital de equipamentos pesados: avançando na otimização de custos e eficiência operacional. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 2, e77294, 2025. DOI: 10.34117/bjdv11n2-011.

MOSLEY, R. Defesa contra ameaças cibernéticas: melhores práticas de segurança cibernética da SAP. Esfera SAP, 2024. Disponível em: https://www.sapsphere.com/defending-cyber-threats-sap-cybersecurity. Acesso em: 31 mar. 2025.

NAGY, C. As 10 principais vulnerabilidades no SAP. Jornal de Política Cibernética, 2021. Disponível em: https://www.journalofcyberpolicy.com/top-10-vulnerabilities-in-sap. Acesso em: 31 mar. 2025.

OLIVEIRA, C. E. C. de. Gentrificação, revitalização urbana e equidade social: desafios e soluções. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 2, e77293, 2025. DOI: 10.34117/bjdv11n2-010.

PESSOA, E. G.; FEITOSA, L. M.; PÁDUA, V. P.; PEREIRA, A. G. Estudo dos recalques primários em um aterro executado sobre a argila mole do Sarapuí. Brazilian Journal of Development, Curitiba, v. 9, n. 10, p. 28352–28375, 2023. DOI: 10.34117/bjdv9n10-059.

PESSOA, E. G.; FEITOSA, L. M.; PEREIRA, A. G.; PÁDUA, V. P. Efeitos de espécies de alna e eficiência de coagulação, Al residual e propriedade dos flocos no tratamento de águas superficiais. Brazilian Journal of Health Review, v. 6, n. 5, p. 24814–24826, 2023. DOI: 10.34119/bjhrv6n5-523.

RAMO. Segurança de dados em sistemas SAP: melhores práticas e desafios. Ramo Consultoria, 2023. Disponível em: https://www.ramo.com/blog/data-security-sap-systems. Acesso em: 31 mar. 2025.

ROJAS, L.; PEÑA, Á.; GARCIA, J. Manutenção preditiva orientada por IA na mineração: uma revisão sistemática da literatura sobre detecção de falhas, gêmeos digitais e gerenciamento inteligente de ativos. Ciências Aplicadas, v. 15, n. 6, 3337, 2025. DOI: 10.3390/app15063337.

SANTOS, H.; PESSOA, E. G. Impactos da digitalização na eficiência e qualidade dos serviços públicos: a comprehensive analysis. Lumen et Virtus, v. 15, n. 40, p. 4409–4414, 2024. DOI: 10.56238/levv15n40-024.

SCHNEIDER-SIMON, J. 12 práticas recomendadas de proteção contra vírus para sistemas SAP. Ponte de Proa, 2022. Disponível em: https://explore.bowbridge.net/blog/12-virus-protection-best-practices-sap. Acesso em: 31 mar. 2025.

TURATTI, R. C. Aplicação de inteligência artificial na previsão de comportamento e tendências do consumidor no e-commerce. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 3, e78442, 2025. DOI: 10.34117/bjdv11n3-039.

VENTURINI, R. E. Inovações tecnológicas na agricultura: a aplicação de Blockchain e Inteligência Artificial para rastreabilidade e proteção de grãos. Revista Brasileira de Desenvolvimento, Curitiba, v. 11, n. 3, e78100, 2025. DOI: 10.34117/bjdv11n3-007.