Tekhne e Logos, Botucatu, SP, v.16, n.1, maio, 2025.
ISSN 2176 – 4808

OS BENEFÍCIOS AMBIENTAIS NA GESTÃO DE CREDENCIAIS PRIVILEGIADAS (PAM)

ENVIRONMENTAL BENEFITS OF PRIVILEGED ACCESS MANAGEMENT (PAM))

Wesley de Andrade Santos[1] João Emmanuel D Alkimin Neves[2]

Resumo

O artigo explora a importância do *Privileged Access Management* (PAM) no contexto da segurança cibernética, conformidade regulatória e proteção de infraestruturas críticas, considerando o potencial impacto ambiental. Ademais, o presente trabalho objetiva demonstrar, além do papel crucial na gestão de acesso privilegiado, os possíveis benefícios ao meio ambiente da solução. O artigo adotou uma abordagem qualitativa exploratória, baseada na revisão da literatura acadêmica e normas relacionadas ao PAM. Também considerou estudos de caso e referências a regulamentos. A pesquisa explorou as funcionalidades da solução, bem como sua importância na conformidade com regulamentações ambientais e sua aplicação na proteção de infraestruturas críticas. O PAM desempenha um papel multifacetado na proteção de dados, na conformidade regulatória e na segurança de infraestruturas críticas, como usinas nucleares. A implementação eficaz desse software reduz o risco de violações de segurança e contribui para a preservação do meio ambiente, protegendo informações ambientais sensíveis. Em resumo, o PAM é essencial para garantir a segurança e a conformidade dos dados sensíveis, contribuindo para a proteção ambiental e proteção das infraestruturas críticas.
Palavras-chave: conformidade regulatória, impacto ambiental, infraestruturas críticas, segurança cibernética.

Abstract

This paper explores the importance of Privileged Access Management (PAM) in the context of cybersecurity, regulatory compliance and the protection of critical infrastructures, considering the potential environmental impact. It aims to demonstrate, beyond its crucial role in privileged access management, the possible environmental benefits of the solution. A qualitative exploratory approach was considered, based on the review of academic literature and standards related to PAM. It also considered case studies and references to regulations. The research delved into the functionalities of the solution, as well as its importance in compliance with environmental regulations and its application in protection of critical infrastructures. PAM plays a multifaceted role in data protection, regulatory compliance, and the security of critical infrastructures such as nuclear power plants. Effective implementation of this software reduces the risk of security breaches and contributes to environmental preservation by safeguarding sensitive environmental information. PAM is essential for ensuring the security and compliance of sensitive data, thereby contributing to environmental protection and the safeguarding of critical infrastructures.

Keywords: critical infrastructures, cybersecurity, environmental impact, regulatory compliance.
.

[1] Graduando em Segurança da Informação Industrial pela Faculdade de Tecnologia de São Paulo – Campus Araraquara Prof Jose Arana Varela.
[2] Professor titular da Fatec Americana. R. Emílio de Menezes, S/N - Gleba B, Americana - SP, 13469-111. e-mail: joao.neves11@fatec.sp.gov.br.

Recebido em fevereiro de 2024 e aceito em dezembro de 2024.

Tekhne e Logos, Botucatu, SP, v.16, n.1, maio, 2025.
ISSN 2176 – 4808

1. INTRODUÇÃO

O gerenciamento de acesso privilegiado (PAM) desempenha um papel fundamental na segurança cibernética e no controle de acesso, sendo uma tecnologia essencial para organizações que buscam proteger seus ativos mais críticos. De acordo com Gonçalves (2023), PAM é baseado no princípio do menor privilégio, que constata que utilizadores, aplicações e sistemas devem ter apenas acesso às permissões necessárias para executarem a sua função. Essa abordagem garante que cada elemento do sistema possua apenas o nível de acesso necessário para cumprir suas funções, reduzindo a superfície de ataque. O controle de acesso é amplamente discutido em normas de segurança, como a ISO/IEC 27000/2018, que define que Controle de Acesso é o processo de garantir que os recursos de processamento da informação e da informação da organização sejam acessados somente por pessoas autorizadas e de forma autorizada. Esse princípio reflete a necessidade de autenticação rigorosa e autorizações bem definidas, características centrais das soluções PAM.

Conforme Sindiren e Ciylan (2018), o gerenciamento de contas privilegiadas inclui componentes como distribuição de tarefas, segurança de senhas, treinamento, monitoramento e auditoria para garantir o cumprimento das políticas de segurança. Esses elementos constituem um processo robusto que previne abusos de poder e falhas de segurança em ambientes críticos. A arquitetura do PAM, por sua vez, é composta por elementos integrados que asseguram uma gestão eficiente. Gonçalves (2022) destaca que a arquitetura PAM inclui um servidor PAM, agentes PAM, um repositório de credenciais, e módulos de autenticação, autorização, auditoria e sessão para controle e auditoria do acesso privilegiado. Essa estrutura possibilita não apenas o controle de acessos, mas também a rastreabilidade e a responsabilização das ações realizadas. Além disso, a escolha de provedores confiáveis é essencial para a implementação de tecnologias PAM eficazes.

No contexto regulatório, a transparência e a proteção de informações são cruciais. A Lei Federal 10.650/2003 assegura que qualquer indivíduo terá acesso às informações dos estudos ligados ao meio ambiente, desde que não as utilize para fins comerciais ou não cite as fontes do estudo, protegendo a privacidade dos envolvidos (Brasil, 2003). Nesse cenário, as soluções PAM se destacam por viabilizarem o cumprimento de requisitos legais enquanto resguardam dados sensíveis.

Por fim, a crescente sofisticação dos ataques cibernéticos ressalta a importância de tecnologias como o PAM. Conforme Sofaer e Goodman (2001), na Era da Informação, os ataques em infraestruturas críticas são predominantemente cibernéticos, e a sofisticação desses

ataques está crescendo a taxas alarmantes, representando riscos significativos". Essa realidade reforça a necessidade de estratégias avançadas para proteger ativos críticos e prevenir incidentes de grande impacto.

2. DESENVOLVIMENTO DO ASSUNTO

O PAM conforme com Tomaz, Oliveira e Gualberto (2024) tem por objetivo focar no gerenciamento de contas de usuários que representam um maior risco para a organização, seja de usuários com funções de administradores que têm o papel de adicionar, alterar e remover outras contas, ou fazer alterações de configuração em sistemas operacionais e aplicações, ou mesmo usuários que acessam o ambiente corporativo a partir de redes não confiáveis. Segundo Gonçalves (2023) existem aspectos importantes inerentes à área de PAM como a implementação do princípio do menor privilégio, controlos de acesso baseado em funções, automação e monitorização das atividades das contas privilegiadas, entre outros (Figura 1). PAM é baseado no princípio do menor privilégio, que constata que utilizadores, aplicações e sistemas devem ter apenas acesso às permissões necessárias para executarem a sua função (Gonçalves, D. 2023). Como descrito por Branco (2021) implementação de qualquer modelo básico de controle de acesso, é necessário compreender os elementos que possibilitam a avaliação de diferentes formas de controle automatizado de acesso, importante salientar que as normas da família ISO/IEC 27000 (ISO/IEC 27000 *et al*., 2018) definem os seguintes conceitos fundamentais (Leal; Branco, 2017, 2021):

Identificação: métodos para prover um sujeito (entidade que solicita acessos) com uma identidade reconhecível (por exemplo uma conta de usuário, passaporte, etc.).

Autenticação: métodos para assegurar que um sujeito é quem ele diz ser (senha, token, impressão digital, etc).

Autorização: métodos para controlar quais ações um sujeito pode realizar em um objeto (por exemplo, lista de permissões do sujeito e lista de permissões do objeto).

Consoante Sindiren e Ciylan (2018) os seis componentes do processo de gerenciamento dos acessos privilegiados; esses componentes são:

Distribuição e limitação de tarefas e autorizações: consiste em definir as responsabilidades e os níveis de acesso dos usuários, evitando a concentração de poder e a violação do princípio do menor privilégio.

Classificação dos ativos de TI: consiste em identificar e categorizar os ativos de TI de acordo com seu valor e criticidade, aplicando medidas de proteção adequadas para cada classe.

Gerenciamento de identidade digital: consiste em criar e manter as identidades digitais dos usuários, garantindo a autenticidade, integridade e confidencialidade dos dados pessoais.

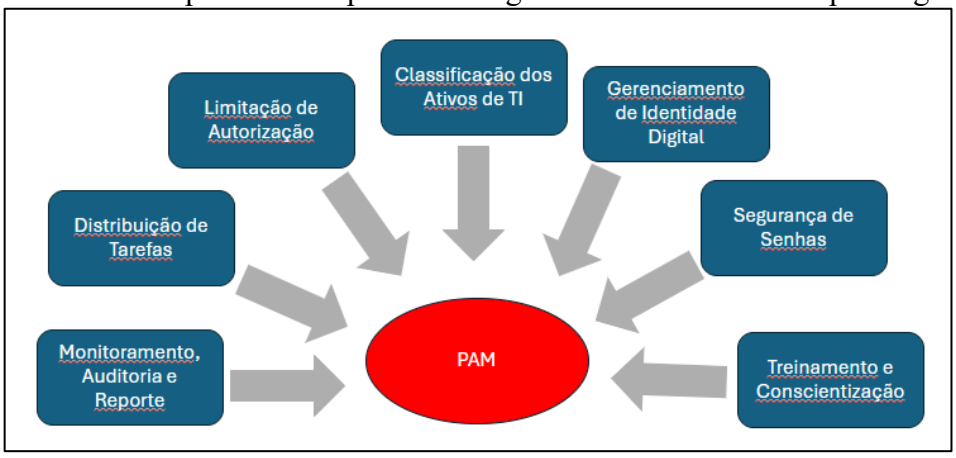
Segurança de senhas: consiste em definir e seguir políticas de senhas fortes, complexas e únicas, utilizando mecanismos de criptografia, armazenamento seguro e rotação periódica.

Treinamento e conscientização: consiste em educar e sensibilizar os usuários sobre as boas práticas de segurança cibernética, prevenindo comportamentos negligentes ou maliciosos que possam comprometer as contas privilegiadas.

Monitoramento, auditoria e relatório: consiste em acompanhar e registrar as atividades realizadas pelas contas privilegiadas, detectando e respondendo a possíveis incidentes ou ameaças cibernéticas.

A imagem a seguir ilustra os componentes que circulam o processo de implementação da tecnologia PAM.

Figura 1 - Os componentes do processo de gerenciamento de contas privilegiadas.

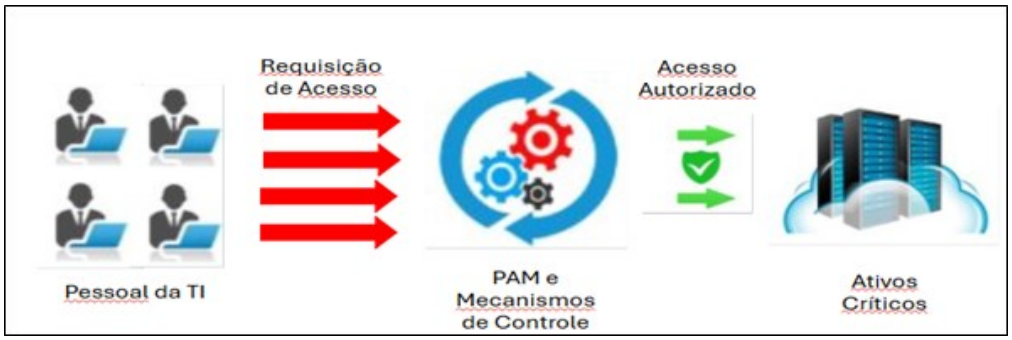


Fonte: Sindiren e Ciylan, 2018

De acordo com Gonçalves (2022), a arquitetura PAM é composta por diversos componentes que trabalham em conjunto para fornecer uma solução completa de gerenciamento de acesso privilegiado. Estes componentes incluem um servidor PAM, agentes PAM, um repositório de credenciais, um módulo de autenticação, um módulo de autorização, um módulo de auditoria e um módulo de sessão. Oliveira (2022), destaca que a arquitetura PAM também inclui um módulo de aprovação. Gonçalves (2022) também destaca que o PAM atua como um *gatekeeper*, controlando e auditando todo o acesso privilegiado aos sistemas e aplicações da organização. A Figura 2, ilustra o posicionamento do PAM como uma camada intermediária entre os usuários e os ativos de TI, atuando como um controlador de acesso

privilegiado. Posição que permite que o PAM gerencie e monitore todas as interações entre usuários e recursos críticos da organização.

Figura 2 - Posição do gerenciamento de contas privilegiadas e do mecanismo de controle em uma infraestrutura de TI.



Fonte: Sindire e Ciylan. 2018

2.1. Conformidade no regulamento ambiental

Os estudos de licenciamento ambiental têm como objetivo atender ao interesse público, ao buscar identificar e avaliar os impactos ambientais, potenciais ou reais, de um empreendimento ou atividade sobre o meio ambiente e a sociedade. Essa análise fundamenta a necessidade de se verificar a viabilidade ambiental, locacional e tecnológica do projeto. O processo também tem como objetivo determinar a adoção de medidas de mitigação e compensação (Lemos; Basso, 2023). É senso comum que a busca pelo desenvolvimento tecnológico e econômico está alinhada com questões ambientais. Um caso famoso recente à escrita deste artigo foi a perfuração da Foz do Rio Amazonas, em que o Ibama, instituto ligado ao Ministério do Meio Ambiente, emitiu um parecer técnico desfavorável à concessão de licença ao requerente, neste caso, a Petrobrás, ligada ao Ministério de Minas e Energia, argumentando inconsistências no parecer técnico e falta de avaliação preliminar dos impactos ambientais (FOLHA, 2023). Um caso público e notório como o exemplificado, expõe as partes interessadas devido à repercussão do tema supracitado. Em contrapartida, como a gestão do PAM poderia auxiliar na conformidade no regulamento ambiental?

Algumas regulamentações ambientais podem exigir medidas de segurança de TI específicas para proteger informações relacionadas ao meio ambiente, como dados ou informações de conformidade ambiental. A implementação de PAM ajuda a garantir o cumprimento dessas regulamentações e a proteger informações ambientais sensíveis. De acordo com Brasil (2003), qualquer indivíduo, independentemente da comprovação de interesse específico, terá acesso às informações dos estudos ligados ao meio ambiente, bem como os de

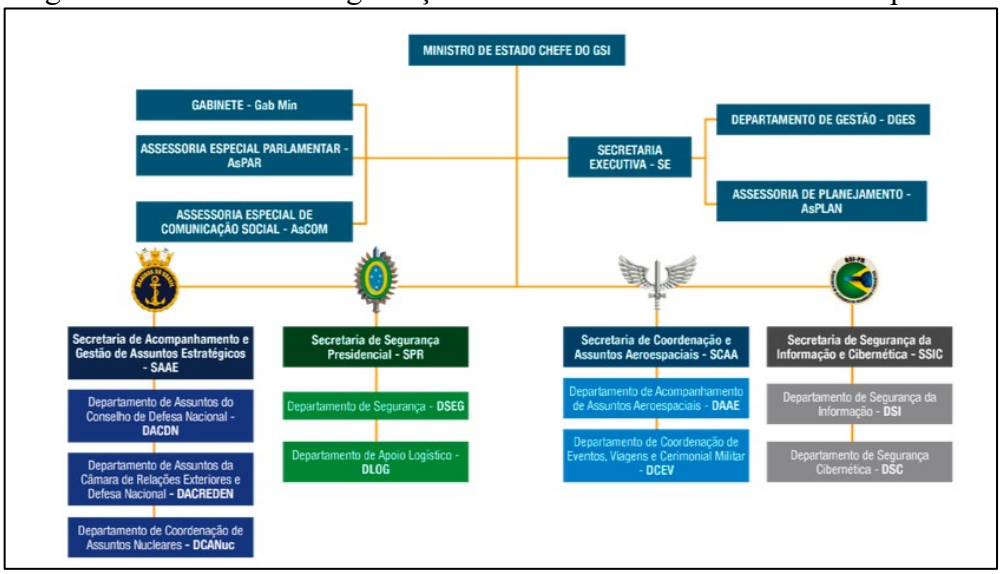
licenciamento ambiental, desde que não as utilize para fins comerciais ou não cite as fontes do estudo, como os dados pessoais dos técnicos e os entrevistados envolvidos.

Conforme já apresentado neste artigo, uma solução de PAM provê monitoramento, auditoria e relatório a partir da autenticação do usuário, acompanhando e registrando as atividades realizadas pelas contas privilegiadas (Sindiren e Ciylan; 2018). Dessa forma, qualquer solicitação dos resultados de um determinado estudo de licenciamento ambiental, independentemente do interesse ou mérito de um solicitante por meio de um sistema público que armazene tais informações, estará resguardada pelo princípio do não-repúdio e autenticidade, e as responsabilizações legais expressas na Lei Federal 10.650/2003 poderão, se necessário, ser devidamente aplicadas, além de proteger principalmente os dados dos envolvidos em estudos de licenciamento ambiental.

2.2 Solução PAM para redução de impactos ambientais

De acordo com o DECRETO Nº 9.573, de 2 de 2018, artigo 1º, inciso I, infraestrutura crítica é definida como "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (BRASIL, 2018). Este mesmo decreto aprovou a criação da Política Nacional de Segurança de Infraestruturas Críticas de competência do GSI, que resultou na criação da Secretaria da Segurança da Informação, contando em sua estrutura com o DSC - Departamento de Segurança Cibernética, conforme demonstrado no organograma da Figura 3.

Figura 3 - Gabinete de Segurança Institucional da Presidência da República



Fonte: gov.br, 2023

Segundo Sofaer e Goodman (2001), na Era da Informação, os ataques em infraestruturas críticas são predominantemente cibernéticos. A infraestrutura de informações está progressivamente sob ataque de "cibercriminosos". A quantidade, o custo e a sofisticação dos ataques estão crescendo a taxas alarmantes. Algumas formas infligem, também, uma crescente ameaça às pessoas e infraestruturas nacionais críticas (Sofaer; Goodman, 2001).

Um exemplo de ataque cibernético, foi o incidente ocorrido no Irã nas instalações nucleares de Natanz, em 2010, por meio de um programa de computador conhecido como "*Stuxnet*". Esse ataque resultou no aumento de 40% na velocidade de rotação das centrífugas, causando rachaduras nas mesmas (Araujo, 2020 citado por Clarke, 2015).

No Brasil, existem duas usinas nucleares, Angra I e II, que respondem por aproximadamente 2% da geração de energia elétrica do país (Agência Brasil, 2023). Apesar do potencial de geração de energia ser pequeno em comparação com outras matrizes energéticas, como hidrelétricas, um ciberataque que prejudique as instalações da usina poderia causar impactos ambientais com repercussões imprevisíveis, afetando tanto a vida da população quanto a vida das espécies que compartilham o ambiente marinho. Além disso, a atividade pesqueira, que também depende de licenciamento ambiental para operar, e o turismo seriam prejudicados.

Com isso, como a solução PAM evitaria ataques nas usinas de Angra ou como os que ocorreram na usina nuclear do Irã? Se considerado o princípio do menor privilégio, no qual as responsabilidades e os níveis de acesso dos usuários estão bem definidos, a implementação eficaz de PAM ajudaria a proteger sistemas e dados críticos contra ameaças cibernéticas, incluindo ataques de *hackers* que podem prejudicar a infraestrutura tecnológica e causar impactos ambientais indiretos. Ao evitar violações de segurança — violações que podem permitir ao atacante ter acesso aos controles da usina — também se evita a interrupção de serviços e sistemas, ou até mesmo o comprometimento das estruturas do complexo nuclear, o que pode ser catastrófico para o meio ambiente.

2.3 PAM e sua relação com a conformidade regulatória ambiental e a proteção de infraestruturas críticas

A pesquisa sobre essas relações revelou insights significativos sobre a importância dessa tecnologia na mitigação de riscos cibernéticos e na proteção de dados sensíveis. O estudo de Gonçalves (2023) destaca que o PAM é fundamentado no princípio do menor privilégio, que assegura que usuários, aplicações e sistemas tenham acesso apenas às permissões necessárias

para desempenhar suas funções, prevenindo acessos não autorizados e potenciais violações de segurança. De acordo com Sindiren e Ciylan (2018), o gerenciamento de acessos privilegiados envolve seis componentes principais: distribuição e limitação de autorizações, que define responsabilidades e níveis de acesso, evitando a concentração de poder; classificação dos ativos de TI, identificando e categorizando ativos de TI conforme seu valor e criticidade; gerenciamento de identidade digital, mantendo identidades digitais dos usuários, garantindo autenticidade e integridade; segurança de senhas, implementando políticas de senhas fortes e seguras; treinamento e conscientização, educando os usuários sobre boas práticas de segurança cibernética; e monitoramento e auditoria, registrando atividades realizadas por contas privilegiadas para detectar incidentes.

O licenciamento ambiental é essencial para avaliar os impactos de atividades sobre o meio ambiente. A pesquisa de Lemos e Basso (2023) enfatiza que a análise de viabilidade ambiental é fundamental para garantir o cumprimento de normas que protegem o meio ambiente. Um exemplo notável foi a tentativa da Petrobras de perfurar a foz do Amazonas, onde o Ibama negou a licença devido à falta de avaliação adequada dos impactos.

O Decreto nº 9.573 define infraestruturas críticas como aquelas cuja interrupção pode causar sérios impactos sociais e econômicos (Brasil, 2018). A implementação de PAM é crucial para proteger essas infraestruturas contra-ataques cibernéticos, como evidenciado pelo ataque *Stuxnet* em 2010, que afetou instalações nucleares no Irã. A proteção de usinas nucleares no Brasil, como Angra I e II, é vital para evitar consequências ambientais catastróficas. A pesquisa utilizou uma abordagem qualitativa exploratória, revisando literatura acadêmica, normas e regulamentos relevantes. As fontes consultadas incluíram normas da ISO/IEC 27000, que definem conceitos de controle de acesso e, estudos acadêmicos sobre PAM, como os de Sindiren e Ciylan (2018), que abordam a prevenção de ataques cibernéticos.

3. CONSIDERAÇÕES FINAIS

O PAM desempenha um papel importante na conformidade com regulamentações de proteção de dados, garantindo que informações ambientais confidenciais, no contexto do estudo de licenciamento ambiental, estejam adequadamente protegidas. No âmbito das infraestruturas críticas, como usinas nucleares, o PAM pode desempenhar um papel crucial na prevenção de ataques cibernéticos que podem causar impactos ambientais devastadores. Através da implementação eficaz do PAM, é possível restringir o acesso não autorizado a sistemas de controle, protegendo assim a integridade e a segurança dessas instalações vitais.

Por fim, foi possível concluir que a gestão de acesso privilegiado desempenha um papel multifacetado na proteção de dados, na conformidade regulatória e na segurança de infraestruturas críticas. A implementação adequada do PAM não só reduz o risco de violações de segurança, mas também contribui para a preservação do meio ambiente e para a segurança de instalações que desempenham um papel vital em nossa sociedade.

Referencias

AGÊNCIA BRASIL. **Especialistas divergem sobre uso da energia nuclear no Brasil.** Agência Brasil, 8 mar. 2023. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/especialistas-divergem-sobre-uso-da-energia-nuclear-no-brasil#:~:text=A%20Ag%C3%AAncia%20Brasil%20ouviu%20especialistas,energia%20el%C3%A9trica%20produzida%20no%20pa%C3%ADs.. Acesso em: 8 out. 2023.

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. 2020. 28f. Monografia (Especialização em Altos Estudos em Defesa) – Escola Superior de Guerra, Brasília, 2020. Disponível em: https://repositorio.esg.br/handle/123456789/1258. Acesso em: 7 out. 2024.

BRASIL. **Decreto nº 9.573**, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Brasília, DF, 23 nov. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/decreto/D9573.htm. Acesso em: 2 out. 2024. BRASIL. Lei nº 10.650, de 16 de abril de 2003. Dispõe sobre o acesso público aos dados e informações existentes nos órgãos e entidades integrantes do Sisnama. Diário Oficial da União, Brasília, DF, 17 abr. 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.650.htm. Acesso em: 5 out. 2024. 9

BRANCO, Marcus Diego de Oliveira Castelo. **Implementação de gerenciamento de identidade e acessos aplicado a ambientes baseados em GNU/Linux**. 2021. 67 f. Trabalho de Conclusão de Curso (Especialização em Gestão e Qualidade em Tecnologia da Informação e Comunicação) – Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco, Campus Jaboatão dos Guararapes, Jaboatão dos Guararapes, 2021. Disponível em: [https://repositorio.ifpe.edu.br/xmlui/bitstream/handle/123456789/285/Implementa%C3%A7%C3%A3o%20de%20gerenciamento%20de%20identidade%20e%20acesso-v10-final.pdf?sequence=1]. Acesso em: 5 out. 2024. 9

FOLHA DE S.PAULO. **Entenda a discussão sobre a tentativa da Petrobras de perfurar a foz do Amazonas.** Folha de S.Paulo, São Paulo, 5 maio 2023. Ambiente. Disponível em: https://www1.folha.uol.com.br/ambiente/2023/05/entenda-a-discussao-sobre-a-tentativa-da-petrobras-de-perfurar-a-foz-do-amazonas.shtml. Acesso em: 1 out. 2023.

GONÇALVES, Daniel Filipe Ribeiro. **Gestão de acesso privilegiado: abordagem com a solução CyberArk.** 2023. 97f. Dissertação (Mestrado em Engenharia Informática) – Instituto Superior Politécnico Gaya, Escola Superior de Ciência e Tecnologia, Portugal, 2023. Disponível em: https://comum.rcaap.pt/handle/10400.26/49761. Acesso em: 9 jul. 2024.

LEMOS, Patrícia Faga Iglecias; BASSO, Ana Paula. O licenciamento ambiental como instrumento da política nacional sobre mudança do clima. **Revista de Direito Público**, Londrina, v. 16, n. 1, p. 27-46, jan./abr. 2023. Disponível em: https://www.scielo.br/j/rdp/a/vwftczDQHZ8tgzNJGWGGXXw/. Acesso em: 2 out. 2024.

SINDIREN, Erhan; CIYLAN, Bünyamin. Abordagem de gerenciamento de contas privilegiadas para prevenir ataques internos. International **Journal of Computer Science and Network Security**, v. 18, n. 1, p. 33-42, 2018. Disponível em: https://www.researchgate.net/profile/ErhanSindiren/publication/341464060_Privileged_Account_Management_Approach_for_Preventing_Insider_Attacks/links/5ec2f2db299bf1c09ac8ec5b/Privileged-Account- Management-Approach-for-Preventing-Insider-Attacks.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19. Acesso em: 2 out. 2024.

SOFAER, Abraham D.; GOODMAN, Seymour E. (ed.). **The transnational dimension of cybercrime and terrorism**. Stanford, CA: Hoover Institution Press, 2001. 292 p.

OLIVEIRA, Tiago. **Privileged Access Management: Implementação numa Organização.** 2022. Dissertação (Mestrado em Engenharia Informática) - Faculdade de Engenharia, Universidade do Porto, Porto, 2022. Disponível em: https://repositorio-aberto.up.pt/handle/10216/156455. Acesso em: 9 jul. 2024.

TOMAZ, Lídia Bononi P.; OLIVEIRA, Patrícia Araújo de; GUALBERTO, Éder Souza. Investigação da ferramenta Keycloak na mitigação de incidentes cibernéticos: uma abordagem integrada com o Programa de Privacidade e Segurança da Informação (PPSI). In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSeg 2024), 24., 2024, São José dos Campos. **Anais Estendidos** [...]. São Paulo: Sociedade Brasileira de Computação, 2024. p. 201–204. DOI: 10.5753/sbseg_estendido.2024.243301. Disponível em: https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/30137. Acesso em: 7 jul. 2024.