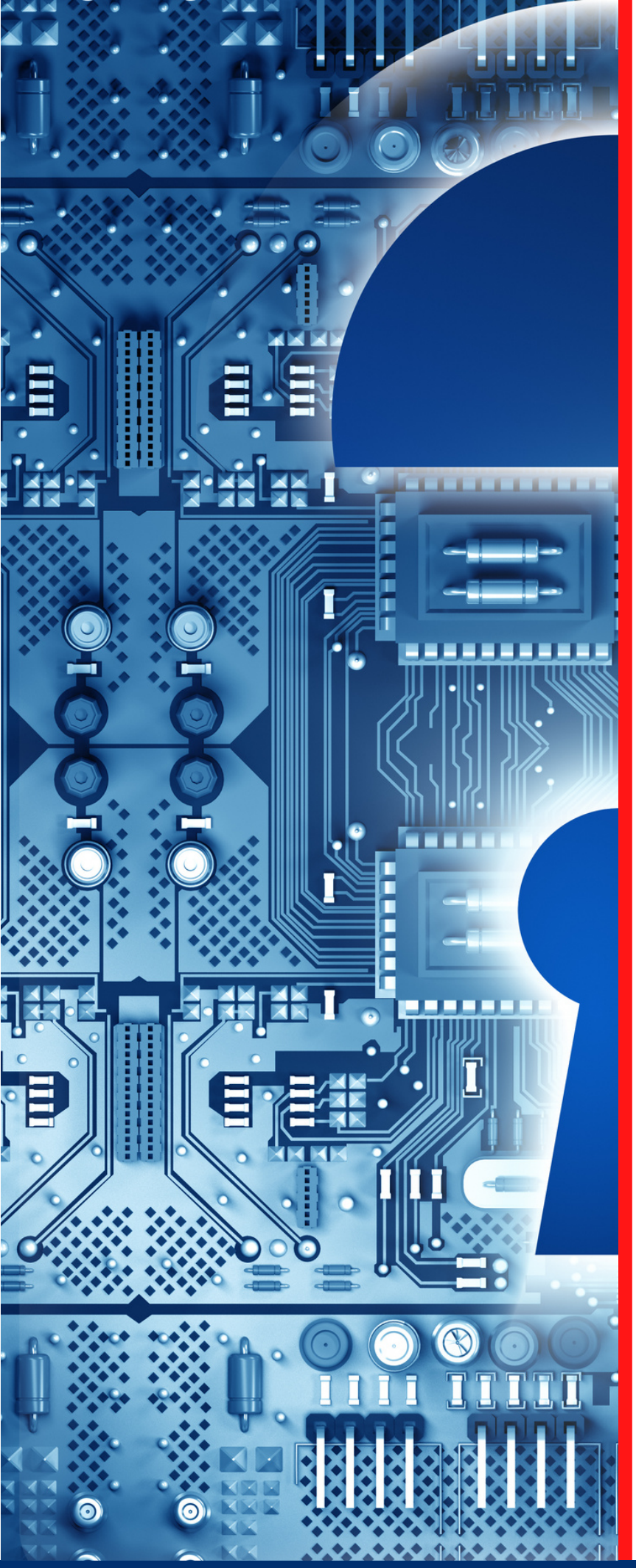


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

09/2023

Gestão de Acesso Privilegiado

(*Privileged Access Management* – PAM)

Parte 2 de 2

Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

PAM (parte 2 de 2)

A segurança do acesso privilegiado é extremamente importante e impacta em outras ações de segurança, pois um invasor no controle de contas com privilégios estabelece condição para comprometer os demais ativos acessíveis com aquelas credenciais, inclusive ferramentas de segurança.

Em face da importância e da complexidade, o tema sobre Gestão de acesso Privilegiado foi proposto em duas edições de Orientação de Segurança da Informação e Cibernética (OSIC). Neste segundo momento, trataremos sobre os riscos, consequências e recomendações aos usuários.

Riscos relacionados à segurança do acesso privilegiado

Alguns dos principais parâmetros que podem ser explorados por adversários e relacionados com a gestão de acesso privilegiado são:

1. **contas órfãs:** contas privilegiadas não mais necessárias e ainda ativas, há muito esquecidas, estão comumente espalhadas pelas organizações. Essas contas órfãs podem fornecer *backdoors* perigosos para invasores, incluindo ex-colaboradores da organização ou de empresas prestadoras de serviços, mas mantiveram o acesso em função da não-remoção ou desativação de suas contas;

2. **nível de privilégios além do necessário:** se os controles de acesso privilegiado forem excessivamente restritivos, eles podem interromper os fluxos de trabalho do usuário, causando frustração e prejudicando a produtividade. Em contrapartida, os usuários finais raramente reclamam de possuir muitos privilégios, por isso, verifica-se a arriscada prática de administradores de rede fornecerem aos usuários finais conjuntos amplos de privilégios, muitos não necessários ao desempenho das atividades daqueles usuários. Além disso, a função de um funcionário geralmente é fluida e pode evoluir de forma que suas responsabilidades sejam alteradas e, em consequência, os privilégios correspondentes, acabando por manter privilégios que não mais necessita (vide Figura 1). Todo esse excesso de privilégio resulta em uma superfície de ataque ampliada;

3. **compartilhamento de credenciais:** muitas equipes de rede compartilham a conta de administrador ou outras credenciais privilegiadas por conveniência, de modo que as cargas de trabalho e as tarefas possam ser ajustadas conforme necessário. No entanto, essa prática dificulta, por vezes inviabiliza, a auditabilidade e a conformidade, além dos óbvios riscos de segurança criados;

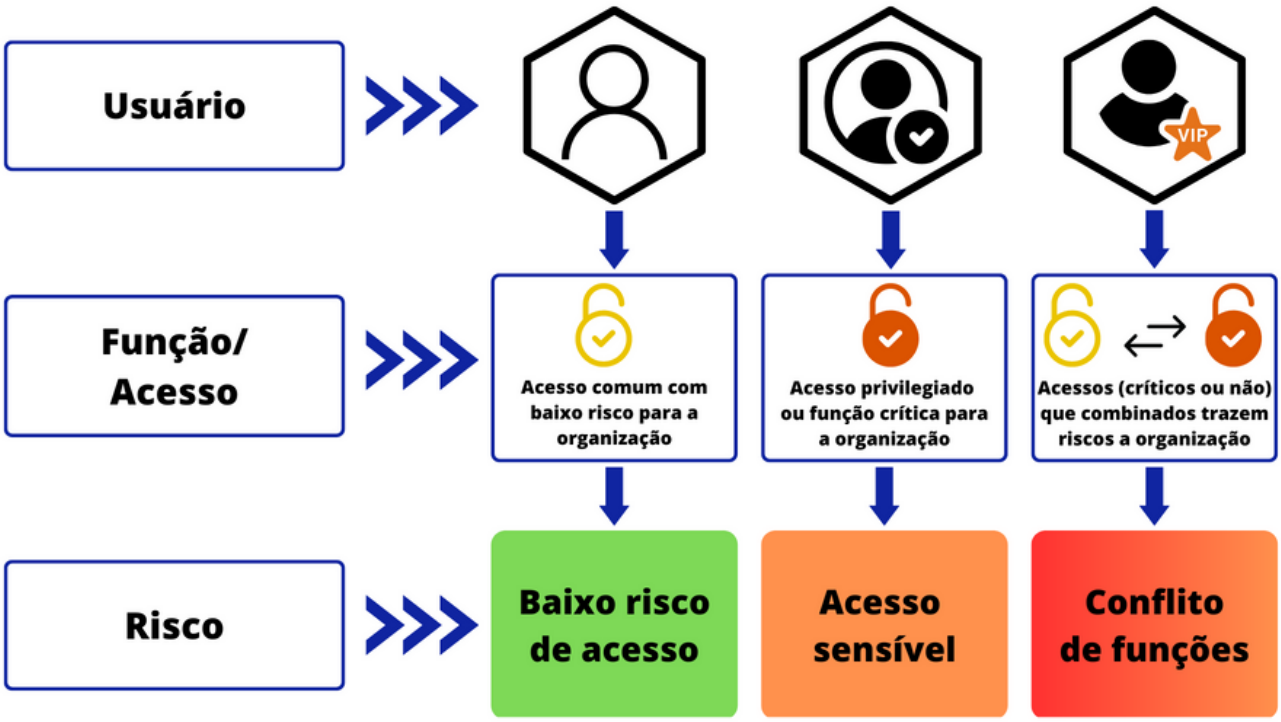


Figura 1

4

credenciais *hardcoded*/**incorporadas** (*embedded*)**.** Credenciais privilegiadas são necessárias para facilitar a autenticação para comunicações e acesso de aplicativo para aplicativo (A2A) e aplicativo para banco de dados (A2D). Aplicativos, sistemas, dispositivos de rede e dispositivos IoT podem ser implantados com as credenciais padrão de fábrica, que geralmente são fáceis de adivinhar ou de obter com em pesquisa de fontes abertas, normalmente no manual do produto, e representam um risco substancial. Além disso, os funcionários costumam codificar as senhas em texto simples, como em um *script*, código ou arquivo, para que seja facilmente acessível quando necessário;

5

gerenciamento manual ou descentralizado de credenciais: os controles de segurança de privilégio geralmente são fracos, com contas e credenciais privilegiadas podendo ser gerenciadas de forma diferente em vários silos organizacionais. Os processos de gerenciamento de privilégios por humanos é praticamente inviável em ambientes de TI onde existem milhares — ou mesmo milhões — de contas, credenciais e ativos privilegiados. Com tantos sistemas e contas para gerenciar, os administradores usam atalhos, como reutilizar credenciais em várias contas e ativos. Neste caso, uma única conta comprometida pode, portanto, comprometer a segurança de outras contas que compartilham as mesmas credenciais;

6

falta de controle dos privilégios de aplicativo ou conta de serviço: aplicativos e contas de serviço geralmente executam automaticamente processos privilegiados para executar ações, bem como para se comunicar com outros aplicativos, serviços, recursos, etc. Além disso, frequentemente possuem direitos de acesso privilegiado excessivos por padrão e outras deficiências de segurança graves;

7 **ferramentas e processos de gerenciamento de identidade em silos:** ambientes de TI modernos geralmente são executados em várias plataformas (Windows, Unix, Linux, etc.) e ambientes (localmente, em nuvem privada, nuvem pública, etc.), cada um mantido e gerenciado separadamente. Essa prática, além de maior complexidade para usuários finais, representa um incremento na superfície de ataque;

8 **consoles e ambientes de administrador de nuvem e virtualização:** provedores de serviços de nuvem fornecem recursos de superusuário, permitindo que estes usuários provisionem, configurem e excluam servidores rapidamente em grande escala. Nesses consoles, os usuários podem criar e gerenciar sem esforço várias máquinas virtuais (cada uma com seu próprio conjunto de privilégios e contas privilegiadas). Isso aumenta a complexidade dos processos que as organizações necessitam utilizar para implementar os controles de segurança corretos de forma a integrar e gerenciar todas essas contas e credenciais privilegiadas recém-criadas em grande escala;

9 **ambientes *DevOps*:** a ênfase do *DevOps* em velocidade, implantações em nuvem e automação apresenta desafios e riscos na gestão de privilégios. A gestão inadequada de credenciais, senhas *hardcoded*, provisionamento excessivo de privilégios e caminhos de acesso inseguros à infraestrutura são alguns riscos comuns em implantações típicas de *DevOps*; e

10 **dispositivos de computação de borda e IoT:** as redes de borda estão se expandindo para fornecer dados mais rapidamente onde eles são necessários. O acesso relacionados a esses dispositivos – bem como os próprios dispositivos (geralmente IoT) – deve ser protegido. Infelizmente, os dispositivos IoT geralmente apresentam graves problemas de segurança, como senhas padrão *hardcoded* e carência no desenvolvimento de *patches* de segurança para o *software* ou raras atualizações do *firmware*. Além disso, a grande maioria dos dispositivos IoT não possuem capacidade de processamento suficiente para executar uma solução *antimalware*.

Ameaças relacionadas à segurança do acesso privilegiado

O roubo ou abuso de credenciais faz uso de vetores muito utilizados para execução de outras formas de ataque. **Os principais vetores utilizados por ameaças para ter controle de contas privilegiadas** são *malwares* específicos para exfiltração de credenciais, fornecedores ou parceiros corporativos com acesso remoto, *insiders* intencionais ou não, e técnicas relacionadas à engenharia social.

Contas privilegiadas são alvos de ameaças para o primeiro acesso ou na busca de escalar privilégios. Os invasores sempre procuram por contas e credenciais privilegiadas desprotegidas, sabendo que, uma vez obtidas, elas fornecem um caminho rápido para os sistemas mais críticos e dados de uma organização. Com credenciais privilegiadas em mãos, um invasor se torna essencialmente um usuário qualquer, com a possibilidade de apagar seus rastros para evitar a detecção enquanto explora o ambiente comprometido.

Ao contrário dos invasores, que são ameaças externas, as ameaças internas – os *insiders* (funcionários, terceirizados, etc.) – estão no ambiente selecionado como alvo, com a grande vantagem de saber onde estão os ativos e dados de interesse. As ameaças internas são de difícil detecção, já que os funcionários e outras pessoas internas geralmente se beneficiam de algum nível de confiança por padrão. O tempo prolongado até ser descoberto também se traduz em maior potencial de dano. Muitas das violações mais relevantes dos últimos anos foram perpetradas por pessoas de dentro da própria organização.

É importante ressaltar que **a obtenção de acesso privilegiado por um invasor é um evento de alto impacto, com uma elevada probabilidade de acontecer** e que está crescendo a uma taxa alarmante em todos os setores. Segundo artigo publicado na revista Forbes, 74% dos ataques de vazamento de dados envolvem o abuso de credenciais privilegiadas (ver: https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/?sh=dcf23473ce45).

Complementarmente, verifica-se no relatório Cost of Data Breach 2022, da IBM (disponível em: https://www.ibm.com/reports/data-breach), que credenciais privilegiadas roubadas ou comprometidas, além de ser a causa mais comum de violação de dados também foram o tipo de problema que mais tempo levou para ser identificado. Esse vetor de ataque custou, em 2022, US$ 150 mil a mais do que o custo médio dos demais incidentes de violação de dados.

Apesar de ser difícil prever ou estimar o possível impacto nos negócios e danos por uma obtenção indevida de acesso privilegiado, cabe destacar que invasores com acesso privilegiado têm efetivamente controle total de todos os ativos e recursos corporativos aos quais tenham obtido acesso, o que concede a eles a capacidade de exfiltrar e divulgar dados confidenciais, interromper ou subverter processos, e quaisquer outras ações danosas que estejam a seu alcance.

Durante muito tempo, o roubo de dados direcionado, para uso próprio ou para terceiros com interesse na organização, foi o principal objetivo dos invasores. No entanto, esse tipo de ataque impunha limites de monetização ao invasor, pois apenas grupos e indivíduos que fossem capazes de monetizar a propriedade intelectual das organizações alvos podiam lucrar com esses ataques. Isso também limitava o número de organizações que seriam alvos vantajosos pois a propriedade intelectual roubada teria de ser de alto valor de mercado e ser de rápida utilização, caso contrário o ganho dos invasores não seria significativo.

Com o advento do *ransomware* o cenário mudou radicalmente e a probabilidade de ocorrência de um ataque por uso indevido de privilégios tornou-se extremamente alta pois os limites de monetização deixaram de existir. Ataques de ransomware são universalmente aplicáveis. Todas as organizações, em qualquer setor, são motivadas financeiramente – no caso do governo, legalmente – a continuar operações ininterruptamente. Atualmente, os ganhos dos invasores são altos e os ataques são extremamente disruptivos para muitas organizações.

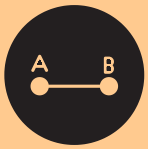
Em 2022, segundo o relatório da IBM, Cost of Data Breach 2022 (ver: https://www.ibm.com/reports/data-breach), a média dos pagamentos realizados foi de US$ 812.360,00, um aumento significativo em relação a anos anteriores.

Princípio do Privilégio Mínimo

Quando se trata do tema PAM, o conceito de privilégio mínimo sempre é citado. Portanto, aplicar o princípio do privilégio mínimo é uma regra geral que deve ser sempre observada.

Para garantir que o usuário, que já provou sua identidade por meio de vários níveis de autenticação, receba apenas os direitos mínimos necessários para executar suas atividades, ressalta-se a importância de impor restrições na amplitude do acesso, além de restrições na duração do acesso, o que significa implementar controles do tipo acesso *just-enough-administration* (JEA) ou acesso *just-in-time* (JIT).

De maneira geral, para impor o Princípio do Privilégio Mínimo (PoLP), devem ser realizadas as seguintes ações:



remover os direitos de administrador nos *endpoints*. Para a maioria dos usuários não há justificativa para ter acesso de administrador em sua máquina local. Além disso, em termos de segurança, as organizações devem ser capazes de exercer controle centralizado sobre o acesso privilegiado. Por esse motivo, deve-se remover os privilégios de administrador nas extremidades, reduzir cada usuário a um usuário padrão e apenas habilitar privilégios elevados para aplicativos e execução de tarefas específicas quando necessário.

aplicar regras de acesso com privilégios mínimos por meio do controle de aplicativos, bem como outras estratégias e tecnologias para:

- remover privilégios desnecessários de aplicativos, processos, dispositivos IoT, ferramentas (*DevOps*, etc.) e outros ativos;
- impor restrições à instalação de *software*, uso e alterações na configuração do sistema operacional;
- limitar os comandos que podem ser executados em sistemas altamente sensíveis/críticos.

remover todos os direitos de acesso *root* **e** *admin* **aos servidores** e utilizar tecnologias PAM que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento.

eliminar privilégios permanentes (privilégios que estão "sempre ativos") sempre que possível. Enquanto o acesso privilegiado para usuários humanos deve sempre expirar, diversos processos, aplicativos, serviços e até equipamentos continuarão a precisar de privilégios persistentes para manter sua atividade. Por esse motivo, deve ser implementado controle como o acesso JEA ou o acesso JIT para elevar os privilégios para aplicativos e tarefas específicas apenas no momento em que forem necessários.

limitar a associação de uma conta privilegiada ao menor número possível de pessoas. Essa regra simples reduz de maneira significativa a superfície de ataque da organização.

minimizar o número de direitos para cada conta privilegiada. Dessa forma, qualquer conta comprometida produzirá um agente de ameaça com apenas um conjunto limitado de privilégios e ajudará a limitar o escopo de uma violação de segurança.

Melhores práticas de PAM

As principais práticas recomendadas de PAM são:

1) antes da delegação do acesso privilegiado:

- **estabelecer e aplicar uma política abrangente de gerenciamento de privilégios**, que deve determinar:
  - como o acesso privilegiado e as contas serão controlados;
  - abordar o inventário e a classificação de identidades e de contas privilegiadas; e
  - aplicar as melhores práticas de segurança e gerenciamento.
- **realizar o levantamento de todos os ativos nas plataformas locais (*on-premises*), remotas, na nuvem e virtuais da organização, classificando-os conforme sua criticidade.** O levantamento deve incluir:

  - todas as plataformas utilizadas (por exemplo, Windows, Unix, Linux, nuvem, local, etc.);
  - diretórios e arquivos críticos;
  - dispositivos de *hardware*; e
  - aplicativos, serviços/*daemons*, *firewalls*, roteadores, etc.
- após a descoberta de ativos, a próxima etapa é **consolidar as contas privilegiadas associadas e as chaves SSH – ou quaisquer entidades de autenticação de usuário que forneçam permissões elevadas, como cartões inteligentes – em um cofre de senhas central seguro.** Este cofre deve ser protegido por várias camadas de criptografia com algoritmos robustos como AES-256 ou RSA-4096. Essa consolidação deve incluir:

  - contas privilegiadas de todos os usuários;
  - contas locais de superusuário;
  - contas de banco de dados;
  - contas de aplicativos e serviços;
  - contas de nuvem e mídia social;
  - chaves SSH;
  - senhas padrão e *hardcoded*; e
  - outras credenciais privilegiadas – incluindo aquelas usadas por terceiros/fornecedores.

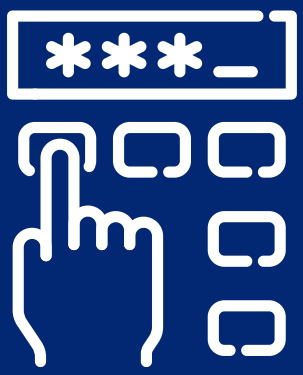
2) durante a delegação do acesso privilegiado, implementar as seguintes medidas:

- **impor privilégios mínimos sobre usuários finais,** *endpoints*, **contas, aplicativos, serviços, sistemas, etc.,** através da eliminação total de privilégios em todos os lugares em que eles existam em seu ambiente (zero *trust*), seguida da aplicação de regras para elevar privilégios conforme necessário para executar ações específicas e revogando privilégios após a conclusão da atividade privilegiada;

- **impor a separação de privilégios e separação de atividades.** As medidas de separação de privilégios incluem a separação das funções de conta administrativa dos requisitos de conta padrão, a separação dos recursos de auditoria/registro nas contas administrativas e a separação das funções do sistema (por exemplo, leitura, edição, gravação, execução, etc.). Quando o privilégio mínimo e a separação de privilégios estiverem em vigor, será possível impor a separação de deveres. Cada conta privilegiada deve ter privilégios ajustados para executar apenas um conjunto distinto de tarefas, com pouca sobreposição entre várias contas;

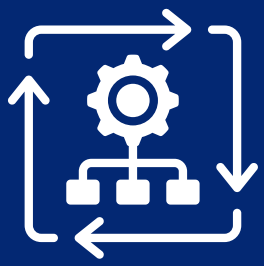
- **segmentar sistemas e redes para separar usuários e processos com base em diferentes níveis de confiança, necessidades e conjuntos de privilégios.** Sistemas e redes que exigem níveis de confiança mais altos devem implementar controles de segurança mais robustos. Quanto maior a segmentação de redes e sistemas, mais fácil é conter qualquer violação potencial de se espalhar além de seu próprio segmento. Sempre que possível, deve ser implementada a **microssegmentação**, uma estratégia chave do **modelo de confiança zero**, insolando recursos através da criação de zonas, o que restringe ainda mais a visibilidade e o acesso aos aplicativos, protegendo contra ataquesações de movimento lateral;

- **impor melhores práticas de segurança para senhas e credenciais.** Isso geralmente implica em:



  - centralizar a segurança e o gerenciamento de todas as credenciais em um cofre de senhas à prova de violação;
  - utilizar certificados efêmeros para autenticar e autorizar sessões privilegiadas. Os certificados efêmeros são gerados e provisionados automaticamente durante o acesso privilegiado para que os usuários não precisem inserir as credenciais durante a conexão e expiram automaticamente após a conclusão da sessão;
  - impor regras que garantam a criação de senhas robustas, que possam resistir a tipos de ataque comuns (por exemplo, força bruta, baseado em dicionário, etc.), aplicando parâmetros de geração de senhas fortes, como complexidade de senha, exclusividade, etc.

- impor o rodízio (alteração) rotineiro de credenciais e senhas, diminuindo os intervalos de alteração proporcionalmente aos privilégios da conta. A prioridade máxima é identificar e alterar rapidamente quaisquer credenciais padrão, pois elas apresentam um enorme risco. Para contas e acessos privilegiados mais confidenciais, deve-se implementar senhas descartáveis (*one-time password* – OTP), que expiram imediatamente após um único uso. Embora a rotação frequente de senhas ajude a evitar muitos tipos de ataques de reutilização de senhas, as senhas OTP podem efetivamente eliminar essa ameaça; e
- impor a criação de *login* exclusivo para cada usuário a fim de garantir uma supervisão clara e uma trilha de auditoria limpa.



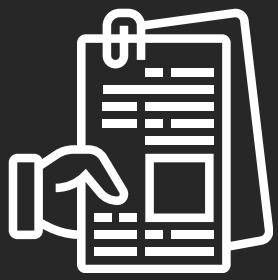
- **bloquear a infraestrutura,** estendendo os princípios da gestão de acesso privilegiado para implementar um gerenciamento robusto de acesso à infraestrutura. O acesso à infraestrutura deve ser feito por *proxy* utilizando tecnologias PAM sem VPN. Isso pode implicar na implementação de uma estação de trabalho de acesso privilegiado (*Privileged Access Workstation* – PAW), que são recursos dedicados usados para proteger todos os acessos administrativos. O princípio do menor privilégio também deve ser aplicado para garantir que a gama de atividades e acesso à infraestrutura para qualquer PAW seja limitada.

- **monitorar todas as atividades privilegiadas.** É imperativo a implementação de uma Gestão de Sessão Privilegiada (PSM) de forma que seja possível supervisionar as sessões em andamento a fim de detectar quaisquer anomalias em tempo real, como a passagem de comandos maliciosos e investigar com eficiência as sessões privilegiadas ativas em tempo hábil.

- **implementar acesso dinâmico e baseado em contexto.** Esse é um princípio fundamental de confiança zero e envolve o fornecimento de acesso *just-in-time* (JIT) no contexto adequado. Isso é feito avaliando-se várias informações, como dados de vulnerabilidades/ameaças, inclusive em tempo real, para um ativo de destino, geolocalização, dados temporais, dados do usuário, dentre outros, a fim de determinar quais privilégios devem ser provisionados e por quanto tempo. Esse recurso permite, inclusive, que se restrinjam privilégios automaticamente a fim de evitar riscos potenciais quando se verifica a existência de uma ameaça ou a possibilidade de comprometimento potencial para o usuário, ativo ou sistema.

3) após a delegação do acesso privilegiado, implementar as seguintes medidas:

- **implementar o registro abrangente de atividades de usuários privilegiados como parte da solução PAM.** As trilhas de auditoria devem capturar instantaneamente todos os eventos relativos a operações de contas privilegiadas, tentativas de *login* de usuários, configurações de fluxo de trabalho e conclusão de tarefas e devem incluir carimbos de data/hora e endereços IP. Integrar a plataforma de auditoria de acesso privilegiado com o serviço interno de registro de eventos pode ajudar a correlacionar dados de *endpoint* e acesso privilegiado. Isso dá às equipes de TI um painel consolidado para mapear o acesso privilegiado com as operações gerais do sistema, aumentando a visibilidade e a consciência situacional no monitoramento de usuários privilegiados. Os *logs* combinados fornecem mais contexto, o que pode ajudar na tomada de decisões ao responder a incidentes de segurança na rede; e



- **implementar análises de ameaça/usuário privilegiado.** Deve-se estabelecer linhas de base para atividade comportamental de usuário privilegiado e para o acesso privilegiado de forma a ser possível automatizar a monitoração e emissão de alertas sobre quaisquer desvios da linha de base que atendam a um limite de risco definido. Deve-se incorporar também outros dados de risco a fim de permitir uma visão mais tridimensional dos riscos de privilégios.

O Departamento de Segurança da Informação e Cibernética (DSIC) recomenda aos usuários que:

- incluam em suas políticas a implementação do **princípio do mínimo privilégio;**
- configurem corretamente seus aplicativos com critérios de segurança, inclusive o MFA, que protejam a privacidade, a integridade e a disponibilidade; e
- promovam, divulguem e incentivem o uso do múltiplo fator de autenticação (MFA); e
- ao identificar um incidente cibernético em sua organização informe imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) de sua instituição.

O DSIC relembra que a primeira parte desta OSIC está disponível em:

https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/osic/osic-08-23

Por fim, o DSIC orienta aos integrantes da administração pública federal observar o previsto no na Instrução Normativa do GSI nº 03, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal disponível em:

https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/copy_of_IN03_consolidada.pdf

O DSIC solicita que propostas de temas, sugestões ou outras contribuições sejam encaminhadas ao e-mail educa.si@presidencia.gov.br para fomentar futuras emissões de OSICs.

TLP:CLEAR