Política de privilégios de acesso do usuário

Norma #	Vigência	Versão
06	01/01/2021	1.0

Contato	E-mail	Telefone
Lemuel Victor Dias	victor.dias@medicamental.com.br	(16) 3505-4900

Índice:

1 Visão geral

O potencial de risco de executar tarefas iniciadas pelo usuário usando os mesmos níveis de acesso dos componentes do sistema é incrivelmente alto, particularmente em uma época em que o ransomware pode atravessar redes, criptografando arquivos sob demanda de pagamento. Os níveis de privilégio podem atenuar os danos potenciais causados por ameaças externas, agentes mal-intencionados internos e erros simples do operador.

As organizações empregam o princípio do privilégio mínimo para tarefas específicas e acessos autorizados para usuários e processos. O princípio do menor privilégio é aplicado com o objetivo de privilégios autorizados não superiores ao necessário para cumprir as missões organizacionais ou funções de negócios exigidas.

As organizações consideram a criação de processos, funções e contas de sistema adicionais conforme necessário para obter privilégios mínimos. As organizações também aplicam privilégios mínimos ao desenvolvimento, implementação e operação de sistemas organizacionais. As funções de segurança incluem o estabelecimento de contas do sistema, configuração de eventos a serem registrados, configuração de parâmetros de detecção de intrusão e configuração de autorizações de acesso (ou seja, permissões, privilégios).

Contas privilegiadas, incluindo contas de superusuário, são normalmente destinadas aos administradores de sistemas para vários tipos de sistemas comerciais disponíveis. Restringir contas privilegiadas a funcionários ou funções específicas impede que os usuários diariamente tenham acesso a informações ou funções privilegiadas. As organizações podem diferenciar na aplicação deste requisito entre privilégios permitidos para contas locais e contas de domínio, desde que as organizações mantenham a capacidade de controlar as configurações do sistema para parâmetros de segurança chave e conforme necessário para mitigar suficientemente o risco.

A empresa deve aplicar o princípio do menor privilégio a todos os usuários e processos em todos os sistemas. Isso significa atribuir o mínimo de permissões necessárias para que o usuário ou processo cumpra sua função comercial. Deve-se também:

• restringir o acesso do usuário apenas às máquinas e às informações necessárias para cumprir as responsabilidades do trabalho; e

• limitar quais definições de configuração dos sistemas os usuários podem alterar, permitindo apenas que indivíduos com necessidades comerciais as alterem.

Exemplo

O administrador de TI de uma organização aplica o mínimo de privilégios necessários para que os usuários ou processos concluam suas tarefas diárias. Isso significa atribuir a todos uma função de usuário básica. Isso evita que um usuário modifique as configurações do sistema. Significa também atribuir acesso privilegiado apenas aos usuários e processos que precisam dele, como a equipe de TI.

Fundamentalmente, esta política fornece diretrizes para aplicação do "princípio do menor privilégio", um conceito definido pelo cientista da computação Jerome Saltzer como "Cada programa e cada usuário do sistema deve operar usando o mínimo de privilégio necessário para completar o trabalho/tarefa".

2 Objetivos

Esta política fornece diretrizes para a concessão de privilégios de usuário em sistemas de propriedade da empresa.

Ela também estabelece orientações, regras, critérios e requisitos para a aplicação do princípio do privilégio mínimo aos acessos dos usuários aos sistemas, que permita apenas acessos autorizados que sejam necessários para realização das tarefas organizacionais atribuídas.

3 Aplicabilidade

Esta norma se aplica:

- À todas as unidades, áreas, setores e departamentos da empresa.

- À todos os analistas de segurança da informação e administradores de sistemas responsáveis pela manutenção de sistemas, softwares, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela empresa.

- A todos os dirigentes, funcionários em tempo integral, funcionários em meio período, funcionários em tempo parcial, trabalhadores contratados,

consultores, estagiários, trabalhadores temporários, prestadores de serviços, agentes, parceiros, fornecedores e usuários autorizados que acessam as dependências da empresa.

- À todos os sistemas, aplicativos, dispositivos e equipamentos de TI gerenciados pela empresa que armazenam, processam ou transmitem dados e informações, incluindo redes de computadores, hardwares, softwares e aplicativos, dispositivos móveis e sistemas de telecomunicações.

4 Norma

No interesse da mitigação de risco, o uso de contas de superusuário em sistemas de propriedade da empresa deve ser limitado às circunstâncias que exigem o uso dessas contas de privilégios mais elevados.

O uso de acesso não privilegiado reduz a probabilidade e mitiga o dano potencial de comandos digitados incorretamente, potencialmente danificando os sistemas. Da mesma forma, o uso desnecessário de contas de superusuário pode aumentar o efeito de malware ou vírus em execução com níveis de privilégio mais altos.

Deve ser empregado o princípio do privilégio mínimo para deveres e sistemas específicos. O princípio do privilégio mínimo também deverá ser aplicado aos processos dos sistemas, garantindo que os processos tenham acesso aos sistemas e operem em níveis de privilégio não superiores ao necessário para cumprir as missões organizacionais ou funções de negócios.

Deve ser considerado a criação de processos, funções e contas adicionais conforme necessário, para obter o privilégio mínimo.

Deve ser aplicado o princípio do privilégio mínimo ao desenvolvimento, implementação e operação de sistemas organizacionais.

Os usuários não devem usar contas de administrador ou root (ou tipos de contas de alto nível semelhantes) para tarefas que não requerem acesso privilegiado.

Para tarefas que requerem acesso privilegiado, contas individualizadas devem ser usadas para fins de registro. O uso de acesso privilegiado ou contas de administrador ou root só é aceitável em circunstâncias nas quais os privilégios não podem ser delegados a contas não root.

O acesso total aos sistemas para contas privilegiadas não deve ser permitido ou praticado. Deve ser fornecido apenas os privilégios necessários para que o usuário execute suas funções e tarefas do dia a dia.

Sempre que possível, utilizar “SUDO” ou “Run As...” para escalar privilégios temporariamente, em vez de criar uma conta para realizar uma tarefa.

O compartilhamento de contas deve ser proibido.

Não deve ser permitida a criação de contas duplicadas com privilégios pessoais.

Sempre que finalizar uma tarefa o usuário deverá fazer logout do sistema. O usuário não deve deixar sem segurança um dispositivo conectado a um sistema através de uma conta de superusuário.

As senhas para contas privilegiadas devem ser consistentes com a política de senha da empresa.

Deve ser mantido um inventário atualizado das contas privilegiadas.

As contas de usuários que se desligam da empresa devem ser desativadas/canceladas tempestivamente.

Nos aplicativos do Windows que requerem acesso de administrador o acesso deve ser feito utilizando-se o Controle de conta de usuário (UAC).

Nos dispositivos que não reconhecem o nível de privilégio (normalmente, dispositivos que usam sistemas operacionais incorporados, como impressoras) o login deve ser feito apenas o tempo necessário para executar uma tarefa administrativa.

5 Procedimentos e controles

5.1 Acesso às funções de segurança

5.1.1 Descrição

A empresa deve autorizar explicitamente o acesso as:

- funções de segurança implantadas em hardware, software e firmware; e
- informações relevantes para a segurança.

5.1.2 Detalhamento

As funções de segurança incluem o estabelecimento de contas do sistema; configuração de autorizações de acesso (ou seja, permissões, privilégios); definição de configurações para eventos a serem auditados e estabelecimento de parâmetros de detecção de intrusão.

As informações relevantes para a segurança incluem regras de filtragem para roteadores ou firewalls, parâmetros de configuração para serviços de segurança, informações de gerenciamento de chaves criptográficas e listas de controle de acesso.

Pessoal explicitamente autorizado inclui administradores de segurança, administradores de sistema, programadores de sistema, pessoal de TI da empresa e outros usuários privilegiados.

5.2 Acesso não privilegiado para funções não relacionadas à segurança

5.2.1 Descrição

Os usuários de contas (ou funções) dos sistemas com acesso à funções de segurança ou informações relevantes para a segurança deverão usar contas ou funções não privilegiadas ao acessar funções dos sistemas não relacionadas à segurança.

5.2.2 Detalhamento

A inclusão de funções deverá contemplar situações em que a empresa implemente políticas de controle de acesso, como controle de acesso baseado em funções e onde uma mudança de função forneça o mesmo grau de garantia na mudança de autorizações de acesso para o usuário e todos os processos agindo em nome do usuário como seria fornecido por uma mudança entre uma conta privilegiada e uma não privilegiada.

5.3 Acesso à comandos privilegiados da rede de computadores

5.3.1 Descrição

Os acessos à comandos privilegiados da rede deverão ser autorizados apenas para necessidades operacionais especificas e justificáveis.

5.3.2 Detalhamento

O acesso à rede é qualquer acesso através de uma conexão de rede em vez de um acesso local.

5.4 Segregação de domínios de processamento

5.4.1 Descrição

Os domínios de processamento deverão ser segregados para permitir uma alocação mais refinada de privilégios de acesso do usuário.

5.4.2 Detalhamento

Fornecer domínios de processamento segregados para alocação mais refinada de privilégios do usuário inclui:

- o uso de técnicas de virtualização para permitir privilégios de acesso adicionais em uma máquina virtual, enquanto restringe privilégios de acesso a outras máquinas virtuais ou à uma máquina física subjacente;

- implementar domínios físicos segregados e empregar mecanismos de segregação de domínio de hardware e software.

5.5 Contas privilegiadas

5.5.1 Descrição

As contas com acesso privilegiado aos sistemas deverão estar restritas ao pessoal do departamento de TI da empresa.

5.5.2 Detalhamento

Contas privilegiadas, incluindo contas de superusuário, são normalmente descritas como contas de administradores dos sistemas disponíveis.

A empresa deverá restringir contas privilegiadas a funcionários ou funções específicas do departamento de TI para impedir que os usuários comuns acessem informações privilegiadas ou funções privilegiadas.

Na aplicação da restrição a empresa poderá diferenciar entre privilégios permitidos para contas locais e contas de domínio, desde que mantenha a capacidade de controlar as configurações do sistema para parâmetros-chave e conforme necessário para mitigar suficientemente os riscos.

As contas de domínio são aquelas armazenadas em um local central na rede como no controlador de domínio do Active Directory (para a maioria dos casos de uma rede Windows).

As contas locais são aquelas armazenadas individualmente em cada computador, seja um laptop, desktop ou servidor.

5.6 Acesso privilegiado por usuários não organizacionais

5.6.1 Descrição

A acesso privilegiado aos sistemas por usuários não organizacionais deverá ser proibido.

5.6.2 Detalhamento

Um usuário organizacional é um funcionário ou indivíduo considerado pela empresa como tendo o status equivalente ao de um funcionário.

Os usuários organizacionais incluem indivíduos contratados pela empresa ou indivíduos contratados por outras organizações que fornecem produtos e/ou serviços para a empresa. Um usuário não organizacional é um usuário que não é um funcionário ou indivíduo considerado pela empresa como tendo o status equivalente ao de um funcionário.

5.7 Revisão dos privilégios de acesso dos usuários

5.7.1 Descrição

A empresa deverá:

- Revisar anualmente os privilégios atribuídos às funções ou classes de usuários definidos pela empresa para validar a necessidade de tais privilégios; e

- Atribuir novamente ou remover privilégios, se necessário, para refletir corretamente a missão organizacional e as necessidades de negócios.

5.7.2 Detalhamento

A necessidade de certos privilégios de acesso aos sistemas atribuídos aos usuários pode mudar com o tempo para refletir mudanças na missão organizacional e funções de negócios, ambientes de operação, tecnologias ou ameaças.

Uma revisão periódica dos privilégios de acesso aos sistemas atribuídos aos usuários deverá ser feita pela empresa para determinar se a razão para atribuir tais privilégios permanece válida. Se a necessidade não puder ser revalidada, a empresa deverá tomar as ações corretivas apropriadas.

5.8 Níveis de privilégio para execução de códigos

5.8.1 Descrição

Deverá ser evitado que os sistemas, softwares, programas e aplicativos sejam executados em níveis de privilégio mais altos do que aqueles atribuídos aos usuários que operam o sistema, software ou aplicativo.

5.8.2 Detalhamento

Em certas situações, os sistemas, softwares, programas ou aplicativos precisam ser executados com privilégios elevados para realizar as funções necessárias.

No entanto, dependendo da funcionalidade e configuração, se os privilégios necessários para a execução estiverem em um nível mais alto do que os privilégios atribuídos a usuários organizacionais que operam tais aplicativos ou programas, esses usuários poderão receber indiretamente privilégios maiores do que os atribuídos.

5.9 Logs de auditoria do uso de funções privilegiadas

5.9.1 Descrição

A execução de funções privilegiadas nos sistemas deverá ser registrada e analisada mensalmente através de logs de auditoria devidamente configurados, gerados e armazenados de forma segura.

5.9.2 Detalhamento

A detecção do uso indevido de funções privilegiadas, intencionalmente ou não por usuários autorizados ou por entidades externas não autorizadas que possam comprometer contas dos sistemas, deve ser uma preocupação constante da empresa, pois isso pode ter impactos adversos significativos em seus negócios.

Por isso, a empresa deve registrar e analisar através de logs de auditoria o uso de funções privilegiadas como uma maneira de detectar a sua utilização indevida e mitigar o risco de ameaças internas e ameaças persistentes avançadas.

5.10 Não execução de funções privilegiadas por usuários não privilegiados

5.10.1 Descrição

Não deve ser permitido que usuários não privilegiados executem funções privilegiadas nos sistemas.

5.10.2 Detalhamento

As funções privilegiadas incluem desabilitar, burlar ou alterar os controles de segurança ou privacidade implementados, criar, configurar ou estabelecer contas nos sistemas, executar verificações de integridade nos sistemas e administrar atividades de gerenciamento de chaves criptográficas.

Os usuários não privilegiados são indivíduos que não possuem as autorizações apropriadas.

As funções privilegiadas que requerem proteção contra usuários não privilegiados incluem contornar a detecção de intrusão e mecanismos de prevenção ou mecanismos de proteção de código malicioso.

Assim sendo, não deve ser permitido que usuários não privilegiados executem funções privilegiadas nos sistemas.

6 Responsabilidade

É responsabilidade do departamento de TI e de cada gestor de departamento, área, setor ou unidade da empresa garantir a aplicação desta norma.

7 Verificação da Conformidade

A equipe de TI, o departamento de RH e os gestores de cada departamento, área, setor ou unidade da empresa verificarão a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a, walk-thrus periódicos, logs de auditoria de sistemas e banco de dados, auditorias de TI e feedbacks para o responsável pela política.

Qualquer mudança nesta política deve ser aprovada pelo departamento de TI.

8 Exceções

Não há exceções a esta política. Qualquer exceção à esta norma deverá ser previamente aprovada pela equipe de TI.

9 Violação

Qualquer violação desta norma pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho. A empresa reserva-se o direito de notificar as

autoridades responsáveis pela aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade. A empresa não considera que a conduta que viole esta norma esteja dentro do curso e âmbito das atividades de um funcionário, parceiro ou prestador de serviço, ou como consequência direta da execução de suas funções. Consequentemente, na medida do permitido por lei, a empresa reserva-se o direito de não defender ou pagar quaisquer danos concedidos aos funcionários, parceiros ou prestadores de serviços que resultem da violação desta norma.

10 Aprovação e responsabilidade

Responsável	Cargo/Função	Data
LEMUEL VICTOR DIAS	ADVOGADO	18/10/2021
Aprovado por	**Cargo/Função**	**Data**
EDGAR ROBERTO THEODORO	DIRETOR	19/10/2021

11 Histórico de revisões

Versão	Descrição	Última Revisão	Próxima Revisão	Revisor/ Aprovador
1.0	Versão inicial	01/03/2021	01/03/2022	