Poder Judiciário

Conselho Nacional de Justiça

ANEXO VI – Manual de Referência – Gestão de Identidade e de Controle de Acessos

Manual de Referência

GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS

Material de referência com os principais controles e padrões para o gerenciamento de identidade e controle de acessos baseados em frameworks de segurança

Sumário

1. Visão geral

1.1 Este Manual estabelece as diretrizes principais para a gestão de identidades e credenciais eletrônicas bem como para o controle de acessos aos sistemas, serviços e equipamentos de tecnologia da informação (TI).

1.2 Orienta, também, quanto à criação de identidades e contas, formas de autenticação, gerenciamento de autorizações, remoção de contas e privilégios e registro das ações executadas para fins auditoria.

1.3 Este Manual é aplicável aos titulares de contas individuais e define as responsabilidades deles quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação.

2. Principais *frameworks* de referência utilizados

3.0.1. Quando se fala sobre "segurança digital", "segurança cibernética" ou até mesmo "segurança da informação", é muito importante identificar os principais modelos e referências utilizados no mercado, analisar e comparar os requisitos, implementar as orientações que se adequam melhor ao cenário em que as instituições se encontram e buscar melhorias que possibilitem alcançar uma visão de futuro.

3.0.2. Por isso, para os principais temas correlatos serão listados a seguir alguns padrões que podem auxiliar essa busca.

2.1. CIS Controls 7.1

2.1.1. O *Center for Internet Security Critical Security Controls for Effective Cyber Defense1* é uma publicação de diretrizes de práticas recomendadas para segurança cibernética.

2.1.2. O projeto foi concebido em 2008 em resposta a perdas de dados por organizações na base industrial de defesa dos EUA. A publicação foi desenvolvida

[1] https://www.cisecurity.org/controls/

inicialmente pelo SANS *Institute*, transferida para o *Council on Cyber Security* (CCS) em 2013 e, em posteriormente, transferida para o *Center for Internet Security* (CIS) em 2015.

2.1.3. A versão 7.1 dos controles CIS foi disponibilizada em abril de 2019 para se adequar aos dados de ameaças cibernéticas mais atuais.

2.2. MITRE ATT&CK

2.2.1 A MITRE ATT&CK é uma base de conhecimento de táticas e técnicas adversárias pautada em observações do mundo real[2]. A base de conhecimento da MITRE é fundamental para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética. A publicação está disponível para uso gratuito por qualquer pessoa ou organização.

2.3. Norma ABNT NBR ISO/IEC 27001:2013

2.3.1. Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização[3].

2.4. NIST SP 800-53

2.4.1. Fornece um catálogo de controles de segurança e privacidade para os sistemas de informações e organizações para proteger operações e ativos organizacionais, indivíduos e outras organizações de um conjunto diversificado de ameaças. É publicado pelo *National Institute of Standards and Technology* (NIST)[4] e busca estabelecer

[2] https://attack.mitre.org.
[3] https://www.abntcatalogo.com.br/norma.aspx?ID=306580.
[4] https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53.

controles flexíveis e personalizáveis, implementados como parte de um processo de toda a organização para gerenciar riscos.

3. Diretrizes gerais

3.1. Os órgãos do Poder Judiciário devem efetuar a gestão de identidade e o controle de acessos de seus usuários, sejam magistrados ou magistradas, servidores ou servidoras, prestadores ou prestadoras de serviços, usuários ou usuárias dos serviços e equipe de TIC.

3.2. Deve ser estabelecido, em normativo próprio, o regramento de cada órgão, considerando as boas práticas de segurança da informação e em observância às seguintes diretrizes:

3.2.1. Definição de padrão de identidade do órgão, que contemple, no mínimo, os critérios para padronização de nome de usuário e de conta de *e-mail*;

3.2.2. Consideração do princípio de privilégio mínimo e de segregação de funções, visando a evitar acessos indevidos e reduzir os riscos de vazamento de informações;

3.2.3. Estabelecimento de processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso, preferencialmente de forma automática;

3.2.4. Utilização de *login* único para acesso a serviços de diretório corporativo e para acesso aos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais;

3.2.5. Adoção de modelo de controle de acesso, preferencialmente utilizando controle de acesso baseado em funções (RBAC) em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários;

3.2.6. Criação de processos de verificação de identidade nas interações entre sistemas, internos ou externos, com vinculação das credenciais aos usuários e às suas autorizações;

3.2.7. Registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período;

3.2.8. Definição de requisitos de tamanho, reutilização, critérios de complexidade e período de expiração de senhas;

3.2.9. Empenho pela adoção de múltiplo fator de autenticação;

3.2.10. Busca pela unificação de plataformas de autenticação, autorização e autenticação (AAA);

3.2.11. Estabelecimento de regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet;

3.2.12. Gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado;

3.2.13. Rastreabilidade de acessos e ações executadas por administradores de TI;

3.2.14. Utilização de mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de acesso;

3.2.15. Segregação de redes conforme o grupo dos serviços, sistemas ou usuários;

3.2.16. Controle do acesso físico aos ativos de tecnologia da informação e comunicação (TIC);

3.2.17. Implementação de controles de acesso proporcionais à classificação da informação;

3.2.18. Monitoração dos acessos e tentativas de acesso para identificação de ataques.

4. Tipos de contas

4.1. Contas de usuário: estão exclusivamente associadas a uma pessoa específica. Essas contas podem existir em um repositório central ao qual os sistemas podem federar para consumir as informações de identidade e autenticação ou podem ser criadas localmente em um sistema ou dispositivo em que a federação não é prática ou possível.

O uso da conta criada centralmente com autenticação federada é sempre o método preferido.

4.2. Contas compartilhadas: as contas compartilhadas são criadas para oferecer suporte a vários usuários que utilizam a mesma identidade. Por exemplo, elas podem ser criadas quando há necessidade de compartilhar um conjunto de recursos ou porque uma implementação deficiente do produto exige isso. O uso de contas compartilhadas não é recomendado, pois são insuficientes para fins de responsabilização e auditoria.

4.3. Contas de serviço: uma conta de serviço é usada quando é necessário que sistemas ou serviços se autentiquem em outros sistemas ou serviços sem qualquer associação a uma pessoa. Essas contas devem ser criadas com moderação e a documentação da finalidade para elas deve ser mantida. Seu uso deve ser revisado periodicamente. Além disso, os requisitos de senha para contas de serviço não devem ser menos rigorosos do que contas de usuário. Finalmente, as contas de serviço não podem ser usadas por pessoas para autenticação, exceto no teste inicial. Contas de serviço com privilégios elevados devem ser monitoradas com atenção.

4.4. Contas privilegiadas: certas contas podem ter privilégios adicionais relacionados ao gerenciamento de um dispositivo ou sistema. Geralmente, isso é considerado um tipo de conta, mas é descrito com mais precisão como uma conta com autorizações privilegiadas. O privilégio administrativo pode ser adicionado a qualquer um dos três tipos anteriores de conta. Ter pelo menos uma conta com privilégios geralmente é inevitável, mas o uso de privilégios deve ser limitado e o uso direto de contas compartilhadas com privilégios deve ser fortemente desencorajado ou vedado.

4.5. Serviços de Diretório Coorporativos: as informações sobre contas e identidades criadas centralmente são armazenadas no diretório central gerenciado pela área de TI. As implementações mais comuns do serviço de diretório são *Active Directory* (AD) e *Lightweight Directory Access Protocol* (LDAP). Os sistemas de informação do Poder Judiciário devem utilizar serviços de diretório corporativo, utilização das credenciais de *login* único com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais.

5. Autenticação

5.1. A autenticação é o processo pelo qual um sistema ou serviço confirma que uma pessoa ou dispositivo realmente é quem afirma ser e por meio do qual o acesso ao recurso solicitado é autorizado. É necessário a autenticação antes do uso de qualquer conta.

5.2. Devem ser empregados protocolos de autenticação seguros para a proteção das informações pessoais e do órgão e evitar o uso indevido.

5.3. A autenticação geralmente é dividida em três tipos:

5.3.1. Algo que você sabe: as formas mais comuns são senha, *pin* ou padrão;

5.3.2. Algo que você tem: as formas mais comuns são *token* de *hardware*, certificado ou um autenticador de *software* como o *Google Authenticator*, *Duo* ou outros;

5.3.3 Algo que você é: essa categoria costuma ser chamada de autenticação biométrica e a forma mais comum são os leitores de impressão digital.

5.3.4. A autenticação *multifator* (MFA) envolve a combinação de mais de um tipo de autenticação e geralmente fornece garantia mais forte da identidade da pessoa. A combinação de apenas dois dos tipos é chamada de autenticação de dois fatores (2FA).

5.3.5. É dispensada a autenticação quando se tratar de informação pública, conforme previsão legal e definição em política de classificação de informações.

6. Autorização

6.1. Autorizações são a permissão implícita ou explícita para usar um recurso associado a uma conta. Depois que o uso de uma conta é autenticado, um sistema ou recurso pode determinar se a pessoa ou *software* que solicita acesso está autorizado a usá-lo. O gerenciamento e a manutenção das autorizações são de responsabilidade compartilhada da área de tecnologia da informação e dos gestores de sistemas.

6.2. Todas as unidades envolvidas na concessão de autorizações são incentivadas a desenvolver procedimentos que atendam aos requisitos articulados a seguir na política de autorização.

6.3. **Princípios de autorização**

6.3.1 Menor privilégio

6.3.1.1. Uma autorização deve fornecer apenas os privilégios necessários para a função a ser executada e nada mais. Observar esse princípio ajuda a garantir que os fluxos de trabalho adequados sejam seguidos e o acesso às funções que podem expor os dados seja contido tanto quanto possível.

6.3.2 Separação de funções

6.3.2.1. Quando uma autorização é concedida a uma conta, ela deve ser aprovada preferencialmente por um ou vários indivíduos. Múltiplos aprovadores garantem que o princípio do menor privilégio seja seguido tanto do ponto de vista técnico quanto do processo, diminui a oportunidade de conflito de interesses ou fraude e reduz o risco de erro. Conforme aplicada a autorização, exige-se que as funções de aprovador administrativo e de aprovador técnico não sejam exercidas pela mesma pessoa ou, quando for o caso, que o custodiante de dados não desempenhe nenhuma dessas funções.

6.3.3 Custodiantes de dados

6.3.3. Em geral, essas autorizações são concedidas por custodiantes de dados, que são responsáveis pela manutenção dos dados. Normalmente, são administradores de sistemas, administradores de banco de dados ou administradores de aplicativos. Esses indivíduos são responsáveis por executar a solicitação de definição, modificação, remoção de conta aprovada, depois de validar se as aprovações apropriadas foram concedidas.

6.3.4. Desprovisionamento

6.3.4.1. Os sistemas e aplicativos devem ser projetados e implantados de forma que facilite a remoção das autorizações e contas de uma pessoa nos momentos apropriados.

7. Responsabilidades dos usuários

7.1. Cada pessoa com credencial de acesso é responsável por selecionar senhas fortes, mantê-las seguras e relatar à unidade de TI qualquer uso não autorizado de contas. Os usuários devem:

7.1.1. Criar senhas que estejam em conformidade com os critérios de senhas seguras estabelecidos pelo órgão;

7.1.2. Não compartilhar senhas relacionadas a algum sistema corporativo com qualquer outra pessoa;

7.1.3. Não reutilizar senhas relacionadas a qualquer sistema corporativo em contas pessoais;

7.1.4. Alterar imediatamente as senhas e notificar o gestor do sistema apropriado e/ou área de segurança da informação se houver motivos para acreditar que uma senha foi divulgada, acessada ou utilizada indevidamente por uma pessoa não autorizada;

7.1.4. Utilizar os privilégios associados a uma conta apenas para a finalidade para a qual foram autorizados e nada mais;

7.1.5. Valer-se de contas e autorizações privilegiadas apenas quando tal privilégio for necessário para completar uma função;

7.1.6. Fazer *logoff* ou utilizar bloqueio de tela que exija autenticação ao deixar um dispositivo sem supervisão.

8. Checklist

8.1. Após definida a estratégia de segurança cibernética da organização espera-se que sejam estipuladas metas de atendimento e implantação desses recursos, com acompanhamento pela alta administração.

8.2. No caso de adequação de dependências descentralizadas ou distribuídas geograficamente pelo país, o ideal é definir o tempo de adequação que cada uma terá que atender, possibilitando o apoio centralizado da área de segurança.

8.3. Considerando que as tecnologias mudam rapidamente e que as ameaças cibernéticas crescem exponencialmente não haverá momento de "relaxamento" no atendimento desses requisitos mínimos num futuro próximo.

8.4. Recomenda-se que a aplicação dos *checklists* ou das listas de autoverificação implementadas pela organização seja periódica (sugere-se no mínimo periodicidade anual) e que sejam estabelecidos níveis de maturidade nessa avaliação. O objetivo é possibilitar a melhoria contínua de normativos, processos e iniciativas em segurança cibernética da organização.

8.5. O quadro a seguir apresenta sugestão de níveis de maturidades a serem empregados.

Definição	Descrição
1 – Não observado ou inicial	Fator não foi demonstrado claramente.
2 – Maturidade baixa ou em desenvolvimento	Fator demonstrado claramente, mas não integrado.
3 – Maturidade média ou definida	Fator suficientemente demonstrado, integrado, mas não está medido.
4 – Maturidade alta ou gerenciada	Fator constantemente demonstrado, integrado, gerenciado, mas não possui melhoria contínua.
5 – Melhoria contínua ou otimizada	Fator complemente demonstrado, integrado, gerenciado e continuamente melhorado.

No Anexo I serão apresentados controles sugeridos para o presente Manual.

9. Anexo I – Modelo de *checklist*

Checklist de controles para o gerenciamento de identidade e controle de acessos.

Nr.	Item	Referencial	Maturidade				
			1	2	3	4	5
1.	Gestão de identidade e controle acesso						
2.1	Formalizar Política de Gestão de Identidade e Controle de Acesso em conformidade com as diretrizes previstas neste Manual e boas práticas de segurança.	CIS Control 7.1					
2.2	Aplicação dos critérios de padronização de nome de usuário e de conta de *e-mail*.	CIS Control 7.1					
2.3	Realizar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço.	CIS Control 7.1					
2.4	Definir e utilizar um processo para a revogação de direitos de acesso, desabilitando imediatamente as contas no momento do término do vínculo ou da alteração das responsabilidades de um servidor ou prestador de serviços.	CIS Control 7.1					
2.5	Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços remotos.	CIS Control 7.1					
2.6	Adotar modelo de controle de acesso baseado em funções (RBAC).	CIS Control 7.1					
2.7	Registrar em *logs* acessos, operações e período para fins de auditoria.	CIS Control 7.1					
2.8	Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado.	CIS Control 7.1					
2.9	Gerenciar acessos e ações executadas com credenciais privilegiados, não utilizando credenciais genéricas e de uso compartilhado.	CIS Control 7.1					
2.10	Criptografar ou embaralhar (*hash*) com a utilização de *salt* as credenciais de autenticação armazenadas.	CIS Control 7.1					
2.11	Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso.	CIS Control 7.1					
2.14	Configurar o acesso a todas as contas por meio da menor quantidade de pontos de autenticação centralizados possível, incluindo sistemas de rede, segurança e sistemas em nuvem.	CIS Control 7.1					
2.15	Garantir que todas as contas (*usernames*) e senhas sejam transmitidas em rede utilizando canais criptografados.	CIS Control 7.1					
2.16	Manter um inventário de todas as contas organizadas por sistema de autenticação.	CIS Control 7.1					

2.17	Desabilitar contas, em vez de excluí-las, visando à preservação de trilhas de auditoria.	CIS Control 7.1					
2.18	Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário.	CIS Control 7.1					
2.19	Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido.	CIS Control 7.1					
2.20	Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido.	CIS Control 7.1					
2.21	Monitorar tentativas de acesso a contas desativadas, por meio de *logs* de auditoria.	CIS Control 7.1					
2.22	Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários.	CIS Control 7.1					
2.23	Implementar controles de acesso físico aos ativos de TIC.	CIS Control 7.1					