# Propósito

A Norma de Gestão de Acesso **NOR-SGSI-003** complementa a Política de Segurança da Informação, definindo as diretrizes para a gestão de acessos aos sistemas e aplicações utilizadas internamente pela **Demarco** para a realização de suas atividades e processamento de informações.

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação.

# Glossário

* **Ativo de Informação**: Os dados, informações, aplicações, sistemas, equipamentos de rede, hardware, software e firmware utilizados pela **Demarco**.
* **Autenticação:**  O processo pelo qual um sistema ou serviço verifica a identidade de um usuário ou entidade para determinar se eles têm permissão para acessar determinados recursos, dados ou funcionalidades.
* **Credencial de acesso:** Conjunto de informações utilizadas para autenticar uma identidade, ou seja, verificar se uma pessoa é quem ela realmente diz ser. Pode ser um conjunto de dados como um usuário e uma senha, um certificado digital, uma biometria, etc.
* **Gestão de identidade:** Conjunto de processos e atividades que visam gerenciar o ciclo de vida da identidade de um colaborador ou terceiro durante a sua relação contratual com a **Demarco**. Através dos dados utilizados para a construção da identidade, pode-se compreender se as contas e permissões de acesso concedidas são adequadas.
* **Múltiplo fator de autenticação (MFA):** Combinação de diferentes fatores de autenticação.
* **Nível privilegiado/administrativo:** Conjunto de permissões que possa ser considerado de nível restrito, como: criar, alterar ou deletar arquivos, serviços, usuários, aplicações e sistemas, etc.
* **Permissões de acesso:** Possibilidade de executar ações dentro de uma aplicação ou sistema, como: criação, leitura, edição, compartilhamento, deleção, etc.
* **Sistemas e aplicações:** Ativo de tecnologia da informação, serviço ou outro componente utilizado para o processamento e manuseio de informações.
* **Usuário:** Colaborador ou terceiro que possua relação contratual com a **Demarco** e que possui acesso aos sistemas e suas aplicações.

# Diretrizes

## Controle de acesso - Gestão das contas de usuários

A gestão das contas de usuário é fundamental para garantir a segurança das informações contidas nos sistemas e aplicações da **Demarco**. Através de um conjunto de processos e atividades, deve ser assegurado que os colaboradores e terceiros somente recebam acesso a contas de usuários nos sistemas e aplicações limitadas ao mínimo necessário para a execução de suas atividades. Outro fator importante, é que este acesso seja mantido somente pelo período necessário. Os seguintes critérios devem ser observados na gestão das contas de usuários:

1. Deve ser estabelecido e mantido um processo para controlar a criação, alteração, desativação ou remoção de contas de usuários para os sistemas utilizados pela **Demarco**.
2. Para prosseguir com a criação, alteração, desativação ou remoção de contas de usuário, deve ser realizado um registro formal. As solicitações devem ser devidamente armazenadas e protegidas.
3. A criação, alteração, desativação ou remoção de contas dos usuários deve ser aprovada pelo responsável pelo sistema ou aplicação para a qual foi realizada a solicitação. Para cenários de criação de conta de usuário de nível de acesso privilegiado/administrativo, a aprovação deve ser realizada por no mínimo duas pessoas com o mesmo perfil.
4. Sempre que aplicável, convém que o recurso de múltiplo fator de autenticação (MFA) seja utilizado para reforçar o nível de segurança na autenticação a sistemas e aplicações, principalmente em contas que possuam nível de acesso privilegiado/administrativo.
5. A criação de contas de usuário para os colaboradores da **Demarco** deve seguir a nomenclatura: “**Nome.últimosobrenome@demarco.com.br**”. Caso os colaboradores possuam nomes idênticos, ou a combinação de nome + sobrenome possa constranger o colaborador, poderá ser criada uma conta de usuário utilizando o padrão “[Nome.penúltimosobrenome@demarco.com.br"](mailto:Nome.penúltimosobrenome@demarco.com.br)" ou “Nomesocial.últimosobrenome@demarco.com.br”:
6. Para a criação de contas de usuário para terceiros nos sistemas e aplicações da **Demarco**, como no caso de federação, será aproveitada nomenclatura da empresa terceira. Para os sistemas e aplicações de uso do cliente, esta regra não se aplica.
7. Os colaboradores que têm conta de usuário com privilégios de acesso devem utilizá-lo somente quando necessário para realizar tarefas que demandem esse nível de autorização.
8. Após a alteração do cargo ou função de um colaborador ou terceiro, deve ser realizada a remoção de contas de usuário que não forem mais necessárias para a sua nova função.
9. Após o término da relação contratual com colaborador ou terceiro, deve ser realizada a desativação tempestiva de contas de usuário para todos os sistemas e aplicações ao qual ele possuía acesso.
10. As solicitações de desativação ou remoção de conta de usuário podem ser realizadas através de ferramenta específica disponibilizada para este fim ou através de chamada telefônica em situações de urgência.
11. A desativação ou remoção de conta de usuário pode ser programada com antecedência através do registro da solicitação com a área responsável.
12. Durante período de férias, todos as contas de usuário do colaborador devem ser desativadas por tempo correspondente ao seu período de afastamento em todos os sistemas e aplicações ao qual este possui acesso.
13. A cada 6 (seis) meses, deve ser realizada a revisão de contas de acesso para os sistemas e aplicações utilizadas pela **Demarco**. Esta revisão tem como objetivo remover contas de usuários que já foram desligados ou que já não são mais necessárias. Os resultados da revisão de acesso devem ser devidamente armazenados e protegidos.
14. Deve ser mantida lista contendo os sistemas e aplicações que necessitam de conta de usuário para sua utilização.
15. Convém que seja utilizado recurso para centralizar a autenticação dos usuários de sistemas e aplicações.

## Gestão de Identidade

Para assegurar que ocorra uma gestão efetiva das contas de usuários, é necessário estabelecermos e gerir a identidade dos colaboradores e terceiros da **Demarco**. A construção da identidade deve considerar no mínimo os seguintes itens:

* Nome completo;
* Cargo;
* Função;
* Setor;
* Tipo de contratação;
* Matrícula;
* Telefone;
* Data de início;

1. A identidade do colaborador ou terceiro deve ser ajustada sempre que houver a alteração em algum dos dados listados acima.
2. A identidade do colaborador ou terceiro deve ser utilizada como referência para gerenciar o ciclo de vida das identidades e assegurar que os colaboradores somente possuem acesso a recursos do qual realmente necessitam.
3. Convém que exista um repositório centralizado para a gestão das identidades e que existam identidades únicas.
4. Convém que as contas de usuários existentes sejam associadas as suas respectivas identidades.

## Credenciais de acesso

A proteção das credenciais de acesso utilizadas para acessar nossos sistemas são de grande importância na manutenção da confidencialidade, integridade e disponibilidade das informações tratadas pela **Demarco**. Normalmente, estas credenciais são compostas por um conjunto de dados, como um usuário e uma senha, podendo existir outros meios para reforçar esta autenticação. Os colaboradores e terceiros devem sempre observar:

1. Não é permitido realizar o compartilhamento de suas credenciais de acesso, a menos que exista aprovação e necessidade para tal ação.
2. As credenciais de acesso devem ser armazenadas em local seguro, de preferência em cofre de senhas seguro, com recurso de criptografia e MFA.
3. Credenciais de acesso não devem ser anotadas em documentos digitais, como word, pdf, excel.
4. Credenciais de acesso não devem ser anotadas em post it’s, cadernos, agendas ou outros meios semelhantes.
5. Convém que senhas criadas atendam no mínimo aos seguintes requisitos:

|  |  |  |  |
| --- | --- | --- | --- |
| **Requisito** | **Credencial Comum** | **Credencial Privilegiada** | **Credencial de Serviço** |
| Tamanho mínimo | 8 caracteres | 14 caracteres | 12 caracteres |
| Complexidade | 1 letra minúscula  1 letra maiúscula  1 número  1 caractere especial | 4 letras minúscula  4 letras maiúscula  4 números  2 caracteres especiais | 4 letras minúscula  3 letras maiúscula  3 números  2 caracteres especiais |
| MFA | Obrigatório | Obrigatório | Não |

Sempre que for necessário criar ou alterar credenciais de acesso, os seguintes requisitos devem ser observados:

1. Quando for necessário criar senha temporária, esta deve ser randômica e possuir nível de complexidade adequado. Não é permitido o uso de padrões conhecidos e repetidos de senhas para a criação temporária.
2. Em situações que for necessário realizar a alteração massiva de senhas, estas devem ser randômicas e disponibilizadas diretamente ao usuário.
3. Quando for necessário realizar a disponibilização de credencial de acesso a um colaborador ou terceiro, deve ser realizado através de meio seguro e criptografado.

## Gestão das Permissões de Acesso

A gestão das permissões de acesso é um conjunto de processos que nos permite assegurar a confidencialidade, integridade e disponibilidade das informações em nossos sistemas. Através das permissões de acesso, um usuário ou grupo de usuários em um sistema ou aplicação pode realizar diferentes ações. É fundamental que as contas de usuários possuam os níveis e permissões de acesso adequados, portanto, os seguintes requisitos devem ser observados:

1. As permissões de acessos precisam ser condizentes e adequadas às funções e informações necessárias para a execução do trabalho de cada colaborador ou terceiro.
2. Ao ocorrer a alteração na função de um colaborador ou terceiro, este deve ter suas permissões de acesso revogadas e receber novas permissões de acesso.
3. Permissões de acesso podem ser temporariamente concedidas para a execução de alguma função, desde que seja formalmente solicitada, registrada e aprovada pelo responsável pelo sistema.
4. A cada 6 (seis) meses, devem ser realizadas revisões das permissões de acesso para as contas de usuários existentes nos sistemas e aplicações utilizados pela **Demarco**. Esta revisão tem como objetivo remover permissões de acesso desnecessárias para a execução das atividades dos colaboradores ou terceiros. Os resultados da revisão das permissões de acesso devem ser devidamente armazenados e protegidos.
5. A segregação de funções deve ser observada durante a atribuição das permissões de acesso as contas de usuários, para evitar situações conflitantes que possam causar ou possibilitar a ocorrência de incidentes.

# Papéis e Responsabilidades

## RECURSOS HUMANOS

1. Registrar solicitação formal para a criação de conta de usuário para novo colaborador;
2. Fornecer à área de Infraestrutura as informações necessárias para a manutenção das identidades;
3. Registrar solicitação formal para a desativação temporária de acessos de colaboradores em período de férias
4. Registrar solicitação formal para a alteração de função dos colaboradores;
5. Apoiar os responsáveis por sistemas na revisão de contas de usuários;
6. Comunicar tempestivamente o término de relação contratual com colaborador;
7. Registrar solicitação formal para a remoção das contas de usuário de colaborador desligado.

**5.2 . GESTORES DOS CONTRATOS**

1. Registrar solicitação formal para a criação de conta de usuário para prestadores de serviços da Demarco contratados em modalidade PJ;
2. Fornecer à área de Infraestrutura as informações necessárias para a manutenção das identidades;
3. Apoiar os responsáveis por sistemas na revisão de contas de usuários;
4. Comunicar tempestivamente o término de relação contratual com prestadores de serviços da Demarco contratados em modalidade PJ;
5. Registrar solicitação formal para a remoção das contas de usuário dos prestadores de serviços da Demarco contratados em modalidade PJ.

## RESPONSÁVEIS PELOS SISTEMAS

1. Criar, alterar, desativar e remover contas de acesso, conforme necessário;
2. Assegurar que sistemas criados ou contratados pela **Demarco** possuam, no mínimo, um recurso de autenticação que permita aplicar os requisitos de complexidade de senhas e gerenciar as permissões de acesso dos usuários;
3. Conceder ou remover direitos de acessos das contas de usuários em sistemas sob sua responsabilidade;
4. Aprovar solicitações formais de criação de contas de usuários ou a concessão de direitos de acesso;
5. Revisar periodicamente as contas de usuários e direitos de acesso nos sistemas sob sua responsabilidade;
6. Documentar e disponibilizar à gerência de consultorias os resultados de revisões de contas de usuários e direitos de acesso nos sistemas sob sua responsabilidade.

**5.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE**

1. Assegurar que ocorram revisões periódicas de contas e direitos de acesso.
2. Orientar os colaboradores a respeito do uso de sistemas para o gerenciamento de senhas

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Assegurar que seja realizado o gerenciamento de identidades.
2. Criar, alterar, desativar e remover contas de acesso, conforme necessário;
3. Assegurar que as aplicações utilizadas pela **Demarco** possuam, no mínimo, um recurso de autenticação que permita aplicar os requisitos de complexidade de senhas e gerenciar as permissões de acesso dos usuários;
4. Conceder ou remover direitos de acessos das contas de usuários em aplicações sob sua responsabilidade;
5. Aprovar solicitações formais de criação de contas de usuários ou a concessão de direitos de acesso;
6. Revisar periodicamente as contas de usuários e direitos de acesso nas aplicações sob sua responsabilidade;
7. Criar e manter lista de sistemas e aplicações utilizadas na **Demarco** que requerem autenticação.
8. Documentar e disponibilizar à gerência de consultorias os resultados de revisões de contas de usuários e direitos de acesso nas aplicações sob sua responsabilidade;
9. Sanar dúvidas encaminhadas pelos colaboradores e terceiros sobre acessos.

## ÁREA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

1. Apoiar os responsáveis pelos sistemas na realização da revisão de contas de usuários e direitos de acesso;
2. Armazenar e apresentar ao **CSIP** os resultados das revisões de contas de usuários e direitos de acesso;

## COLABORADORES

1. Seguir os requisitos estabelecidos para o cuidado com as credenciais de acesso;
2. Encaminhar dúvidas sobre acessos para a equipe de Infraestrutura;
3. Comunicar aos responsáveis pelos sistemas quando possuírem conta de acesso ou direito de acesso que seja desnecessário para suas funções.

# Gestão de versões

A revisão, aprovação e alteração desta política segue os requisitos estabelecidos na Política de Segurança da Informação.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 13/07/2023 | CSIP | Criação da norma |
| 0.2 | 18/09/2023 | CSIP | Revisão e ajustes |
| 0.3 | 18/07/2024 | CSIP | Revisão e ajustes |