Política de Gestão de Identidade e Controle de Acessos

Grupo Edson Queiroz

#### ÍNDICE

[1. APRESENTAÇÃO 3](#_Toc138402808)

[1.1. Objetivo 3](#_Toc138402809)

[1.2. Abrangência 3](#_Toc138402810)

[1.3. Vigência 3](#_Toc138402811)

[1.4. Área técnica responsável pela política 3](#_Toc138402812)

[1.5. Aprovação 3](#_Toc138402813)

[2. CONCEITOS E DEFINIÇÕES 4](#_Toc138402814)

[3. DOCUMENTOS DE REFERÊNCIA 5](#_Toc138402815)

[4. DIRETRIZES 5](#_Toc138402816)

[4.1. Gerais 5](#_Toc138402817)

[4.2. Áreas seguras 6](#_Toc138402818)

[4.3. Senha de acesso 7](#_Toc138402819)

[4.4. Autorização de acesso (privilégios de acesso) 8](#_Toc138402820)

[4.5. Armazenamento 8](#_Toc138402821)

[5. DIVULGAÇÃO E DISSEMINAÇÃO 9](#_Toc138402822)

[6. CONSEQUÊNCIAS 9](#_Toc138402823)

[7. RESPONSABILIDADES 9](#_Toc138402824)

[8. EXCEÇÕES 11](#_Toc138402825)

# 

# APRESENTAÇÃO

## Objetivo

Esta política tem por objetivo estabelecer as diretrizes para gestão de identidade e controle de acesso aos ativos e sistemas de informação do Grupo Edson Queiroz (GEQ).

## Abrangência

Esta política é aplicável a todas as empresas do GEQ.

## Vigência

Esta política terá prazo indeterminado e entrará em vigor a partir da data de sua publicação, com revisão periódica a cada 12 meses ou quando for necessária.

## Área técnica responsável pela política

O conteúdo dessa política é de responsabilidade da área de Operações de Infraestrutura do Departamento de Tecnologia da Informação (TI).

## Aprovação

|  |  |  |
| --- | --- | --- |
| Carlos Rotella | Presidente Executivo |  |
| Roberto Costa | Diretor Executivo Jurídico, de RI e *Compliance* |  |
| Aleksandro Oliveira | *Chief Financial Officer* (CFO) |  |
| Elber dos Reis | Diretor de TI |  |

# CONCEITOS E DEFINIÇÕES

* **Ameaça:** causa potencial de um incidente que pode vir a prejudicar o GEQ.
* **Áreas seguras:** ambientes destinados ao processamento das informações críticas ou sensíveis do GEQ, os quais são protegidos contra ameaças à segurança, tais como infiltrações, vazamento de água proveniente de outra área etc.
* **Ativo de informação:** patrimônio intangível do GEQ, constituído por informações de qualquer natureza (estratégica, técnica, administrativa, financeira, mercadológica, de recursos humanos e/ou legal), incluindo àquelas criadas ou adquiridas por meio de parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico, eletrônico ou digitalizado.
* **Colaborador:** empregados, estagiários, temporários e terceiros vinculados às empresas do GEQ.
* **Comitê Gestor de Segurança da Informação (CGSI):** grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do GEQ, que tem por finalidade tratar questões ligadas à Segurança da Informação.
* **Controle:** medida de segurança para o tratamento de um risco específico.
* **Incidente de Segurança da Informação:** um evento ou conjunto de eventos indesejados de Segurança da Informação que tem possibilidade de gerar impactos adversos ao GEQ.
* **Integridade:** propriedade dos ativos da informação de serem precisos, consistentes, confiáveis e completos.
* **Matriz de segregação de função**: documento de indicação de quais funções cada colaborador deve ter de acordo com o cargo ocupado.
* **Múltiplo Fator de Autenticação (MFA):** uso de dois ou mais fatores para as tarefas de autenticação de credenciais. Ex.: senha + pin; senha + digital.
* **Privilégios administrativos:** característica de uma conta/credencialquepermite aos profissionais de TI gerenciar aplicativos, softwares e hardwares de um serviço.
* **Segurança da informação:** preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do GEQ.
* **Usuários:** empregados do GEQ ou terceiros, independente do regime jurídico ao qual estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar e/ou manipular qualquer ativo de informação do GEQ.

# DOCUMENTOS DE REFERÊNCIA

Esta política possui inter-relacionamento e/ou faz referência aos seguintes documentos:

* Código de Conduta;
* Lei nº 1.379/18 (Lei Geral de Proteção de Dados);
* Política de Consequências;
* Política de Acesso a Ambientes de Data Center;
* Política de Segurança da Informação.

# DIRETRIZES

## Gerais

* + 1. Todos os usuários autorizados devem possuir contas de acesso que os permitam o uso de recursos tecnológicos, ativos e sistemas de informação, observando-se o disposto nesta política.
    2. As contas de acesso citadas no item 4.1.1 são exclusivamente para que os usuários realizem suas atividades laborais, em consonância com o Código de Conduta e a Política de Consequências do GEQ.
    3. Toda conta de acesso é pessoal do usuário a qual foi delegada, sendo intransferível e o usuário integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso, considerando o disposto nos itens 4.1.4 e 4.3.1.
    4. Os usuários devem adotar as seguintes medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo, mas não se limitado a:

1. Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo GEQ;
2. Não compartilhar a conta de acesso e senha com outro usuário ou colaborador;
3. Não utilizar senhas consideradas fracas ou com atributos pessoais – data de nascimento, por exemplo;
4. Comunicar a área de Segurança da Informação, por meio de chamado, caso haja suspeita da utilização de suas credenciais de acesso de forma irregular para acessos a sistemas/ativos do GEQ.
   * 1. Os usuários que têm acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito, observando-se o disposto no item 4.1.6.
     2. A credencial privilegiada, citada no item 4.1.5, deve ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso.
     3. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos e sistemas de informação ou a recursos tecnológicos deve ser considerada um incidente de segurança da informação.
     4. Os incidentes de segurança da informação devem ser avaliados pela equipe de Segurança de Informação e reportados ao Comitê Gestor de Segurança da Informação (CGSI) e os responsáveis estão sujeitos às sanções disciplinares, inclusive rescisão do contrato de trabalho por justa causa.
     5. As contas de acesso devem ser desabilitadas quando do desligamento; afastamento temporário (a exemplo de licença-maternidade e afastamento por doença) e gozo de férias de empregados do GEQ. Exceções a esta regra devem ser formalmente autorizadas pelas Diretoria Executiva de Recursos Humanos e pela Diretoria Executiva Jurídica, de RI e *Compliance*.
     6. As contas de acesso de empregados do GEQ podem ser reabilitadas, a pedido do RH, no caso de retorno ao trabalho, como reintegração e/ou decisão judicial.
     7. As contas de acesso de terceiros devem ser desabilitadas por força do encerramento do contrato ou substituição do profissional terceirizado.
     8. Todos os usuários devem seguir os princípios e normas que regem o tratamento dos dados pessoais a que eventualmente tenham acesso, especialmente a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei Federal nº 13.709/2018), zelando pela proteção de direitos fundamentais de liberdade e de privacidade de cada titular de dados pessoais.

## Áreas seguras

* + 1. Os ambientes de processamento das informações críticas ou sensíveis do GEQ devem ser mantidos em áreas seguras, cujo perímetro seja fisicamente isolado contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.
    2. As áreas seguras de datacenter devem ser protegidas por controle de acesso biométrico, sendo necessário o registro do nome do usuário, motivo do acesso, data e hora de entrada e saída.
    3. As demais áreas consideradas seguras (racks de ativos de comunicação, áreas de armazenamento de dados etc.) devem ter acesso restrito aos profissionais da área de tecnologia autorizados para o acesso.

## Senha de acesso

* + 1. As senhas associadas às contas de acesso a ativos e sistemas de informação ou recursos tecnológicos do GEQ são de uso pessoal e intransferível, devendo o usuário zelar por sua guarda e sigilo, seguindo o disposto no item 4.1.4.
    2. O GEQ adota os seguintes padrões para geração de senhas de acessos aos seus ativos/serviços de informação:
       1. Fornecimento de senhas de acesso inicial aos usuários e adoção de mecanismos para a troca imediata de senha após o primeiro acesso;
       2. Senhas com validade de 90 (noventa) dias. Passado esse prazo os sistemas solicitam, automaticamente, a troca da senha;
       3. Senhas associadas a contas de privilégio não administrativo compostas com um mínimo de 8 (oito) caracteres, **quando do uso de tecnologias com MFA**, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
       4. Senhas de acesso, **sem o uso de MFA**, compostas por 14 (quatorze) caracteres, usando a mesma regra de combinação acima;
       5. Senhas de acesso associadas a contas com privilégios administrativos com o uso obrigatório de MFA e compostas por, no mínimo, 14 (quatorze) caracteres, além da combinação de caracteres citados acima;
       6. Após 5 (cinco) tentativas de acesso com senhas inválidas, bloqueio da conta, assim permanecendo por 30 (trinta) minutos;
       7. Histórico das últimas 10 (dez) senhas utilizadas, pelos sistemas de informação, não permitindo sua reutilização;
       8. Prazo mínimo de 7 (sete) dias entre trocas de senhas. Sendo de fato necessária a troca da senha em prazo inferior, o usuário deve acionar a Tecnologia da Informação.

## Autorização de acesso (privilégios de acesso)

* + 1. As permissões de acesso aos ativos, sistemas de informação e recursos tecnológicos do GEQ devem ser concedidas de acordo com os perfis que definem o nível de privilégio dos usuários, diferenciando os tipos a seguir:
       1. **Conta privilegiada:** permite acesso administrativo a um ou mais recursos de TI.
       2. **Administrador de domínio:** permite acesso privilegiado em todas as estações de trabalho e servidores em um domínio *Windows*.
       3. **Conta *root*:** possibilita acesso administrativo em *hosts*/servidores Linux/Unix/Mac OS, possibilitando acesso irrestrito a todos os comandos, arquivos, diretórios e outros recursos.
       4. **Administrador local:** não são contas pessoais e fornece acesso administrativo ao *host* local. Utilizada para realizar manutenção ou para configurar novas estações de trabalho.
       5. **Conta de emergência:** fornece aos usuários não privilegiados o acesso de administrador para sistemas em caso de emergência.
       6. **Conta de serviço:** é uma conta local ou de domínio privilegiadas que é utilizada por um aplicativo ou serviço para interagir com o sistema operacional.
       7. **Conta de aplicativo:** essa conta é usada por aplicativos para acessar bancos de dados e/ou fornecer acesso a outros aplicativos.
    2. As permissões de acesso aos ativos, sistemas de informação e recursos tecnológicos do GEQ, de acordo com os perfis mencionados no item 4.4.1, devem ser concedidas e/ou revogadas com base na avaliação da área de Segurança da Informação e mediante autorização do responsável pelo recurso gerenciado.
    3. É expressamente proibida a utilização de credenciais de acesso utilizadas em contas de serviços para acesso individual de usuários.

## Armazenamento

* + 1. A seu critério exclusivo, o GEQ pode ativar uma cota (espaço) para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) para cada usuário, com a finalidade exclusiva de armazenar arquivos de trabalho.
    2. É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais / propriedade intelectual ou que não sejam de interesse do GEQ, seja na infraestrutura computacional local ou em serviços de armazenamento remoto (nuvem).
    3. Os usuários de recursos tecnológicos do GEQ, cujos acessos são concedidos como ferramentas de trabalho, não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou por meio de serviços de armazenamento remoto (nuvem).

# DIVULGAÇÃO E DISSEMINAÇÃO

A divulgação interna e disseminação da presente política é fundamental para sua efetividade. Dessa forma, cabe à área técnica responsável desenvolver periodicamente planos de comunicação e treinamento para sua disseminação, seja para a totalidade dos colaboradores ou para grupos específicos, conforme a necessidade e/ou confidencialidade do tema.

# CONSEQUÊNCIAS

A violação dessa política sujeitará o infrator às medidas previstas no Código de Conduta e na Política de Consequências.

O conhecimento de qualquer infração ou indício de infração das regras contidas nesta política deve ser relatada no Canal de Conduta, disponível 24 horas por dia, 7 dias por semana, pelo número 0800-602-1836, pela internet ([www.contatoseguro.com.br/grupoedsonqueiroz](http://www.contatoseguro.com.br/grupoedsonqueiroz)) ou pelo aplicativo de celular da Contato Seguro.

Todos os relatos são direcionados ao Comitê de Conduta e tratados de forma confidencial. Não é admitida, sob qualquer circunstância, retaliação ou represália ao colaborador ou outra pessoa que utilizar apropriadamente o Canal de Conduta.

# RESPONSABILIDADES

* + 1. Operações de Infraestrutura de TI:

1. Receber e analisar solicitações para a criação de contas de acesso ou fornecimento de privilégios para colaboradores internos e terceiros.
2. Garantir que seja realizada a concessão e revogação do acesso aos usuários empregados e terceiros.
3. Apoiar a revisão periódica da validade de credenciais de acesso a ativos e sistemas de informação dos usuários de empregados e de terceiros, fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.
4. Comunicar ao Comitê Gestor de Segurança da Informação eventuais tentativas de desvio de conduta dos termos dessa política.
5. Estabelecer e manter um inventário de contas de serviço.
6. Fornecer senhas de acesso inicial ao usuário e criar mecanismos para a troca imediata de senha após o primeiro acesso.
   * 1. Gestores dos usuários:
7. Solicitar a concessão de acesso para novos empregados sob sua gestão ou demais empregados que necessitem de novos acessos conforme mudanças em suas atividades laborais.
8. Solicitar a concessão de acesso a terceiros contratados justificando a necessidade de acesso a ativos e sistemas de informação.
9. Informar a equipe de segurança da informação quando do encerramento do contrato com terceiros contratados que tenham acesso a ativos/sistemas de informação do GEQ.
10. Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação concedidas ou solicitadas.
11. Realizar o bloqueio sistêmico, via ferramenta de gestão de acesso, do empregado desligado, quando da comunicação do seu desligamento.
    * 1. Departamento de Recursos Humanos:
12. Reportar imediatamente quando houver desligamento e afastamento de colaboradores do GEQ à área de Segurança da Informação para que as contas de acesso possam ser desabilitadas.
13. Apoiar a gestão de identidades comunicando, enviando relatórios periódicos dos eventos de admissão de colaboradores para área de Segurança da Informação com 24h de antecedência.
14. Apoiar a revisão periódica da validade de credenciais de acesso a ativos e sistemas de informação, fornecendo informações sobre o dos colaboradores (status de contratação, setor, superior imediato etc.).
15. Comunicar a área de Segurança da Informação com 24h de antecedência sobre as movimentações dos funcionários entre áreas para evitar a multiplicidade de acessos e funcionalidades.
16. Manter uma matriz de segregação de função de forma a apoiar a gestão de acesso a ativos/sistemas de informação.
    * 1. Área de Segurança da Informação
         1. Auditar as concessões de acesso a empregados e a terceiros.
         2. Auditar o acesso a áreas seguras.
         3. Autorizar e auditar a concessão de acessos privilegiados a ativos/sistemas de informação,
         4. Analisar incidentes de segurança referentes à gestão de identidades e acessos.

# EXCEÇÕES

Caberá à Gerência de Segurança da Informação levar qualquer situação excepcional e/ou não contemplada nesta política ao CFO e ao Diretor de Tecnologia da Informação, para que seja tomada a decisão emergencial sobre a medida a ser adotada e, se for o caso, providenciada inclusão de nova regra neste documento.

\* \* \*