[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

POLÍTICA DE CONTROLE DE ACESSO

Commented [AES2]: Para saber mais sobre o assunto, leia este artigo:

How to handle access control according to ISO 27001
https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-according-to-iso-27001/

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é definir regras para acesso a diversos sistemas, equipamentos, instalações e informações com base nos requisitos comerciais e de segurança para obtenção de acesso.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os sistemas, equipamentos, instalações e informações do escopo do SGSI.

Os usuários deste documento são todos os funcionários da [nome da organização].

Commented [AES4]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5 e A.8.11
- Política de segurança da informação
- Declaração de aplicabilidade
- [Política de classificação da informação]
- [Declaração de aceitação de documentos do SGSI]
- [Lista de requisitos, legais, regulamentares, contratuais e outros]

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "07_Aplicabilidade_de_controles" do Kit de documentação ISO 27001.

Commented [AES7]: Caso não tenha esta lista, então neste item liste todos os requisitos da legislação e contratuais para o controle de acesso.

3. Controle de acesso

3.1. Introdução

O princípio básico de controle de acesso é que o acesso a todos os sistemas, redes, aos serviços e às informações é proibido a menos que expressamente permitido a usuários e grupos de usuários.

O acesso a todas as áreas físicas não é permitido, exceto às áreas que requerem concessão de privilégios por parte da pessoa autorizada (seção "Gestão de privilégios").

[redacted]

Commented [AES8]: Trecho a ser excluído se a Política de [redacted]

3.2. Perfil de usuário A

Commented [AES9]: Adapte ao sistema de atribuição de [redacted]

O perfil de usuário A possui os seguintes direitos de acesso:

Nome do sistema / rede / serviço	[redacted]

Commented [AES10]: Pode ser especificado de acordo com todo o sistema ou para módulos independentes.

Commented [AES11]: Especifique se esses direitos incluem [redacted]

Os seguintes arquivos têm direitos de acesso de acordo com o Perfil de usuário A:

- [cargo 1]
- [cargo 2]

Commented [AES12]: Liste todos os cargos. Também é

3.3. Perfil de usuário B

Commented [AES13]: Outros perfis de usuário podem ser

O perfil de usuário B possui os seguintes direitos de acesso:

Nome do sistema / rede / serviço	[Direitos de usuário]

Commented [AES14]: Pode ser especificado de acordo com

Commented [AES15]: Especifique se esses direitos incluem

Os seguintes arquivos têm direitos de acesso de acordo com o Perfil de usuário B:

- [cargo 1]
- [cargo 2]

3.4. Gestão de privilégios

Commented [AES16]: Exclua este seção se o controle A.8.2

Os privilégios relacionados aos perfis de usuários mencionados acima (concedendo ou removendo os direitos de acesso são alocados da seguinte forma:

Commented [AES17]: Esta tabela pode ser substituída pela

Nome do sistema / rede / serviço / área física	[Pessoa autorizada para conceder ou remover direitos de acesso]	[Forma de processo de autorização]

Commented [AES18]: Por e-mail, decisão por escrito,

Ao alocar os privilégios, o responsável deve levar em consideração os requisitos dos negócios e de segurança para acesso, conforme definido na avaliação de riscos, bem como a classificação das informações que são acessadas com esses direitos de acesso, de acordo com a Política de classificação da informação.

Responsável pela implementação técnica do controle de acesso	Formas de acesso à rede e aos serviços de rede

3.5. Análise periódica dos direitos de acesso

Os proprietários do sistema e das instalações para os quais são necessários direitos de acesso especiais devem, de acordo com os seguintes intervalos, analisem se os direitos de acesso concedidos estão de acordo com os requisitos dos negócios e de segurança:

Nome do sistema / rede / serviço / área física	Intervalos de análise periódica

Todas as análises devem ser registradas [especifique como os registros são mantidos].

3.6. Alteração de status

Mediante a alteração ou o encerramento das atividades, o [cargo] deve informar imediatamente aos responsáveis que aprovaram os privilégios para o funcionário em questão.

Mediante a alteração das relações contratuais com partes externas que têm direito de acesso aos sistemas, aos serviços e às instalações ou mediante a expiração do contrato, o proprietário do contrato deve informar imediatamente aos responsáveis que aprovaram os privilégios para as partes externas em questão.

Os direitos de acesso para todas as pessoas que mudaram de status de emprego ou relacionamento contractual precisam ser imediatamente removidas por pessoas responsáveis com dedinido na próxima seção.

Commented [AES19]: Exclua este seção se o controle A.5.18 [redacted]

Commented [AES20]: Adapte se necessário.

Commented [AES21]: A frequência deve ser definida com base [redacted]

Commented [AES22]: Um formulário, um relatório formal, [redacted]

Commented [AES23]: Exclua este seção se o controle A.5.18 [redacted]

3.7. Implementação técnica

A implementação técnica da alocação ou remoção dos direitos de acesso é responsabilidade de:

Nome do sistema / rede / serviço / área física	[illegible]

As pessoas listadas nesta tabela podem não conceder ou remover direitos de acesso livremente, mas [illegible]

3.8. Autenticação segura

O [cargo] deve garantir que um procedimento de logon seguro seja implementado para todos os [illegible]

3.9. Gestão de senhas de usuário

Ao alocar e usar senhas de usuário, as seguintes regras devem ser atendidas:

- assinando a Declaração de aceitação de documentos do SGSI, os usuários também aceitam a obrigação de manter as senhas como confidenciais, conforme indicado neste documento
- os usuários só devem usar seus próprios nomes de usuários exclusivos
- [illegible]
- [illegible]
- as senhas temporárias devem ser comunicadas ao usuário de forma segura e a identidade do usuário devem ser verificadas anteriormente
- o sistema de gestão de senhas deve solicitar que o usuário altere a senha temporária na primeira entrada no sistema
- [illegible]
- [illegible]
- se o usuário solicitar uma nova senha, o sistema de gestão de senhas deve determinar a identidade do usuário [especifique como]
- o sistema de gestão de senhas deve impedir a reutilização das últimas [especifique quantas] senhas anteriores
- [illegible]
- [illegible]

Commented [AES24]: Exclua este seção se o controle A.8.5 [illegible]

Commented [AES25]: Exclua este seção se a Política de senhas [illegible]

Commented [AES26]: Adapte essas regras de acordo com os [illegible]

Commented [AES27]: Regras em separado devem ser [illegible]

Commented [AES28]: É possível fornecer mais detalhes aqui.

Commented [AES29]: Isso é apenas uma recomendação; [illegible]

Commented [AES30]: Por exemplo, com o envio de e-mails [illegible]

Commented [AES31]: Por exemplo, três senhas anteriores.

Commented [AES32]: Por exemplo, entrando no sistema [illegible]

- se um usuário inserir uma senha incorreta três vezes consecutivas, o sistema deve bloquear a conta do usuário em questão
- as senhas criadas pelo fabricante do software ou hardware devem ser alteradas durante a instalação inicial
- os arquivos que contêm senhas devem ser armazenados separadamente dos dados do sistema de aplicativo

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	*Responsável pelo armazenamento*	*Controles para proteção do registro*	*Tempo de retenção*
[Registro da atribuição de privilégios (em formato eletrônico – mensagem de e-mail)]	[pasta na intranet]	[cargo responsável pela implementação técnica]	Os registros não podem ser editados, somente o [cargo] tem o direito de armazenar esses registros	Os registros são armazenados por três anos.
[Registros das análises periódicas dos direitos de acesso]	[computador / armário do [cargo]]	[cargo]	Somente o [cargo] tem o direito de acessar esses registros.	Os registros são armazenados por três anos.

Commented [AES33]: Ajuste conforme adequado.

Somente o [cargo] pode conceder aos demais funcionários o acesso a qualquer um dos documentos mencionados acima.

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

O proprietário do documento é o [cargo], que deve verificar e, se necessário, atualizar o documento pelo menos uma vez a cada ano inteiro.

Commented [AES34]: Isso é apenas uma recomendação;

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes relacionados ao acesso não autorizado às informações
- alteração atrasada dos direitos de acesso em caso de alteração ou encerramento das atividades/do contrato
- quantidade de sistemas não incluídos neste documento
- nível de confusão relacionado às responsabilidades de implementação deste documento

[cargo]
[nome]

[assinatura]

Commented [AES35]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.