SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 05: POLÍTICA DE CONTROLE DE ACESSO

SUMÁRIO

Fatec Mauá

1. **Objetivo da Aula – Tópico da Ementa**
2. **Sumário** da Política de Controle de Acesso
3. Capítulo: **Introdução**
4. Capítulo: **Política de Controle de Acesso**
5. Capítulo: **Monitoramento da Política**
6. Capítulo: **Conformidade**
7. Capítulo: **Anexos**

1. OBJETIVO E EMENTA

Fatec Mauá

- **Objetivo da Aula**

  Apresentar um exemplo de uma ampla Política de Controle de Acesso aplicada no mercado, para ser usada como template de formato e conteúdo.

- **Tópico da Ementa**

  Conceitos fundamentais do pilar de segurança: confidencialidade, integridade, disponibilidade e autenticidade.

2. SUMÁRIO DA POLÍTICA

Fatec Mauá

CAPÍTULOS DA POLÍTICA

- Introdução
- Política de Controle de Acesso
- Monitoramento da Política
- Conformidade
- Anexos

3. Capítulo: INTRODUÇÃO

Fatec Mauá

➢ Subitens da INTRODUÇÃO

- **Propósito**
- **Escopo da política**
- **Glossário**
- **Requisitos de negócio do controle de acesso**
- **Princípios de controle de acesso**

➢ PROPÓSITO

O objetivo desta política é estabelecer os requisitos de segurança que devem ser seguidos para garantir o gerenciamento adequado do controle de acesso aos ativos de informação da [Empresa] com base em seu valor, classificação e nível de risco para o negócio.

Fatec Mauá

➢ ESCOPO DA POLÍTICA

Esta política é aplicável à [Empresa] e a todas as subsidiárias, unidades de negócios, funcionários, consultores, contratados, funcionários temporários e sazonais, estagiários, terceiros e parceiros afiliados, aqui referidos como Funcionários, que têm acesso aos ativos de informação da [Empresa],
ou seja, sistemas, dados, rede, etc.
A abordagem descrita neste documento está alinhada com a ISO/IEC 27002:2022: Segurança da Informação, Segurança Cibernética e Proteção da Privacidade — Controles de Segurança da Informação.

Fatec Mauá

➢ GLOSSÁRIO

As definições formais da maioria dos termos usados em toda a família de políticas da [Empresa] estão contidas no
Anexo A: "Glossário de Segurança da Informação".

Fatec Mauá

➢ REQUISITOS DE NEGÓCIOS DO CONTROLE DE ACESSO (1/2)

Ao conceder acesso a sistemas e informações, os sistemas de informação da [Empresa] devem cumprir os seguintes princípios de Controle de Acesso Baseado em Função (RBAC):

1. **Função atribuída**: uma entidade pode executar ou exercer permissões em um sistema somente se tiver sido atribuída uma função ou um grupo (ou seja, administrador, operadores, usuários).
2. **Função Autorizada**: Uma função ou grupo ativo de assunto deve ser autorizado. Em conjunto com a Função Atribuída, essa regra garante que os sujeitos possam assumir apenas funções para as quais estão autorizados.

Fatec Mauá

➢ REQUISITOS DE NEGÓCIOS DO CONTROLE DE ACESSO (2/2)

3. **Transação Autorizada**: uma entidade pode usar determinadas permissões para executar uma ação em um sistema ou acessar informações somente se o usuário estiver autorizado a essa permissão específica, de acordo com sua atribuição de função ou grupo na hierarquia de estrutura baseada em função. Esta regra especifica que a Função Atribuída e a Função Autorizada foram exercidas.

Quando houver falta de orientação na Política de Controle de Acesso, os Princípios de Controle de Acesso e as práticas recomendadas devem ser seguidos.

Fatec Mauá

➢ PRINCÍPIOS DE CONTROLE DE ACESSO (1/2)

Além do **Manifesto de Segurança da Informação** da [Empresa] aprovado (**Anexo B**), que define a **Separação de Funções**, os seguintes princípios de segurança devem ser aplicados:

1. **Direito de Saber:** Um funcionário sempre pede permissões e tem uma Necessidade de Saber válida para acessar um sistema, independentemente de seu nível na organização ou outras aprovações.

Fatec Mauá

➢ PRINCÍPIOS DE CONTROLE DE ACESSO (2/2)

2. **Necessidade de Saber:** Um funcionário respeita a privacidade dos sistemas e das informações. Um funcionário é informado apenas do que é considerado necessário para que ele saiba realizar uma tarefa de forma eficaz dentro de um sistema.

3. **Privilégio mínimo:** um funcionário cria um ambiente seguro no sistema para ele e para as informações. Um funcionário em um sistema recebe apenas os privilégios necessários para executar tarefas efetivamente autorizadas.

Fatec Mauá

➢ Subitens da POLÍTICA DE CONTROLE DE ACESSO

- Funções e responsabilidades de controle de acesso
- Gerenciamento de acesso de usuário
- Autenticação de usuários, senhas e credenciais
- Redes e sistemas

Fatec Mauá

➢ FUNÇÕES E RESPONSABILIDADES DE CONTROLE DE ACESSO (1/3)

Responsabilidades da função de provisionamento

1. A equipe de Segurança da Informação deve designar uma "Função de Provisionamento" responsável pelas atividades de controle de acesso de acordo com suas responsabilidades.
2. A " Função de Provisionamento " em conjunto com os proprietários de ativos deve garantir que o uso de acessos privilegiados seja restrito seguindo os princípios de "segregação de funções", "menor privilégio" e "necessidade de saber".
3. Trabalhe com proprietários de ativos para identificar, remover ou desabilitar credenciais de acesso redundantes ou desnecessárias pelo menos uma vez por ano.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

4. Defina e gerencie mecanismos de desafio e/ou resposta para confirmar identidades de usuário antes de alterar credenciais.
5. Mantenha uma lista centralizada de aplicativos, funções e usuários autorizados para acesso.
6. Trabalhe com gerentes de linha para suspender os direitos de acesso aos ativos oportunamente quando necessário.
7. Defina e siga um procedimento formal para verificar e conceder autorizações de registro de usuário.
8. Atualizar ou encerrar as conexões do fornecedor mediante notificação do proprietário do contrato ou da parte responsável pelo serviço.

Fatec Mauá

➢ FUNÇÕES E RESPONSABILIDADES DE CONTROLE DE ACESSO (2/3)

Responsabilidades dos proprietários de ativos

1. Determine regras de controle de acesso, direitos de acesso e restrições apropriadas para funções de usuário específicas para seus ativos em conjunto com a "Função de provisionamento".
2. Revisar e autorizar formalmente, juntamente com a "Função de Provisionamento", solicitações de acesso aos seus ativos de informação, garantindo que a autorização seja dada por alguém que não seja o solicitante.
3. Trabalhe com a Função de Provisionamento para identificar, remover ou desabilitar periodicamente credenciais de acesso redundantes ou desnecessárias.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

4. Determinar controles físicos e lógicos de seus ativos em conjunto com o departamento de Segurança da Informação.
5. Defina controles de acesso aos ativos de informações considerando a criticidade e o impacto nos negócios para manter a consistência entre os direitos de acesso e os requisitos de segurança da informação.
6. Trabalhe em conjunto com a legalidade, a continuidade de negócios e a conformidade para garantir que os controles de acesso em vigor estejam em conformidade com a legislação e os contratos relevantes.
7. A autoridade para conceder, revisar e revogar acessos deve ser exclusivamente do proprietário do ativo ou de uma função designada e autorizada por ele.
8. Certifique-se de que os usuários com contas privilegiadas tenham o conhecimento técnico suficiente para entender as implicações de seu uso.

Fatec Mauá

➢ FUNÇÕES E RESPONSABILIDADES DE CONTROLE DE ACESSO (3/3)

Responsabilidades do usuário

1. Compreenda e siga as declarações descritas nesta política.
2. Os utilizadores devem ter a obrigação de desempenhar o seu papel na protecção do acesso que lhes foi concedido.
3. Certifique-se de que sua conta não seja usada para usar indevidamente ou abusar da organização.
4. Os usuários não devem escalar privilégios ou remover controles de acesso concedidos, a menos que aprovados anteriormente.
5. Relate qualquer desvio dos controles descritos neste documento.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

➢ INSTRUÇÕES DE CONTROLE DE ACESSO

As declarações a seguir devem ser seguidas nos controles de acesso da [Empresa], a fim de proteger a confidencialidade, integridade e disponibilidade de seus ativos de informação

- **Gerenciamento de acesso de usuário**
- **Autenticação de usuários, senhas e credenciais**
- **Redes e sistemas**

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (1/6)

1. CADASTRO DE USUÁRIO

a) Qualquer solicitação de acesso à rede e aos sistemas de computadores da organização deve primeiro ser submetida à "Função de provisionamento" para aprovação.

b) Todas as solicitações devem ser processadas de acordo com um procedimento formal que garanta que verificações de segurança apropriadas sejam realizadas e a autorização correta seja obtida antes da criação da conta de usuário.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

c) A criação da conta de usuário deve seguir os procedimentos formais definidos, e aderir aos princípios de "segregação de funções", "necessidade de saber" e "privilégio mínimo".
d) Cada conta de usuário terá um nome de usuário exclusivo (identificador) que não é compartilhado com nenhum outro usuário e está associado a um indivíduo específico.
e) Senhas fortes iniciais e subsequentes devem ser configuradas em todas as contas e devem seguir as características descritas no
Anexo C: "Política de Senha Forte"

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (2/6)

2. CANCELAMENTO DO REGISTRO DE USUÁRIO

a) Quando um funcionário deixa a organização em circunstâncias normais, seu acesso a sistemas e dados de computador deve ser suspenso no encerramento do expediente no último dia útil do funcionário.

b) É de responsabilidade da equipe de Pessoas solicitar a suspensão dos direitos de acesso por meio da "Função de Provisionamento" (por meio de um processo que registra a solicitação).

c) As contas de usuário devem ser inicialmente suspensas ou desativadas e não excluídas para obter as informações de trabalho do ex-funcionário, se necessário.

d) Os nomes de conta de usuário não devem ser reutilizados, pois isso pode causar confusão no caso de uma investigação posterior.

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (3/6)

3. PROVISIONAMENTO DE ACESSO DE USUÁRIO

a) A cada usuário devem ser atribuídos direitos de acesso e permissões a sistemas e dados de computador que sejam válidos para fins comerciais e seguindo os princípios de "privilégio mínimo" e "necessidade de saber".

b) Os perfis baseados em função devem ser gerados, atribuídos e mantidos, e qualquer exceção de particularidade deve ser documentada.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

c) As funções do grupo devem ser mantidas periodicamente de acordo com os requisitos de negócios e quaisquer alterações devem ser formalmente autorizadas, documentadas e controladas por meio de um processo de gerenciamento de alterações.

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (4/6)

4. REMOÇÃO OU AJUSTE DE DIREITO DE ACESSO

a) As atualizações de direitos de acesso ou permissões devem ser realizadas quando necessário e solicitadas por meio de um processo válido de gerenciamento de alterações. (por exemplo, devido a uma mudança de papel individual).

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

b) Deve-se garantir que os acessos não mais necessários sejam removidos da conta de usuário.

c) Se um usuário estiver assumindo uma nova função além da existente (em vez de em vez de), uma nova função composta deverá ser solicitada por meio de um processo de gerenciamento de alterações.

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (5/6)

5. GESTÃO DE DIREITOS DE ACESSO PRIVILEGIADO

a) Os direitos de acesso privilegiado, como os associados a contas de nível de administrador, devem ser identificados para cada ativo.

b) Os usuários técnicos não devem fazer uso diário de contas de usuário com acesso privilegiado.

c) Uma conta de usuário de nível "admin" separada deve ser criada e usada somente quando privilégios adicionais são necessários e essas contas devem ser específicas para um indivíduo.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

d) O acesso a permissões de nível de administrador só deve ser alocado a indivíduos qualificados cujas funções exijam e que tenham recebido treinamento relevante suficiente (técnico ou não técnico) para entender as implicações de seu uso.

e) O uso de contas de usuário com acesso privilegiado em rotinas automatizadas, como trabalhos em lote ou de interface, deve ser evitado sempre que possível. Quando tal for tecnicamente inviável, as credenciais de autenticação utilizadas devem ser protegidas (por exemplo, com encriptação, sem texto não criptografado, salga de palavra-passe) e alteradas regularmente.

f) Sempre que possível, os direitos de acesso privilegiado devem ter definido um período de expiração em função do ciclo de vida dos projetos e/ou tarefas que exijam esses privilégios.

Fatec Mauá

➢ GERENCIAMENTO DE ACESSO DE USUÁRIO (6/6)

6. REVISÃO DE DIREITOS DE ACESSO DO USUÁRIO

a) Uma revisão de contas de usuário com acesso privilegiado será realizada periodicamente pelo Chief Information Security Officer (CISO) ou uma pessoa delegada para garantir que essa política esteja sendo cumprida.

b) Periodicamente, os proprietários de ativos e sistemas em conjunto com a Função de Provisionamento devem analisar quem tem acesso às suas áreas de responsabilidade e o nível de acesso em vigor. Essas revisões devem ser realizadas para identificar:

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

i. Pessoas que não devem ter acesso (por exemplo, abandonando)
ii. Contas de usuário com mais acesso do que o exigido por suas funções.
iii. Contas de usuário com alocações de função incorretas
iv. Contas de usuário que não fornecem identificação adequada, por exemplo, contas genéricas ou compartilhadas
v. Quaisquer outros problemas que não estejam em conformidade com esta política.

Fatec Mauá

➢ AUTENTICAÇÃO DE USUÁRIO, SENHAS E CREDENCIAIS (1/3)

1. AUTENTICAÇÃO DE USUÁRIO

a) Os tipos de autenticação devem ser implementados com base em diferentes critérios, tais como:

i. O valor dos bens protegidos
ii. O grau de ameaça que se acredita existir
iii. O custo do(s) método(s) de autenticação adicional
iv. A facilidade de uso e praticidade do(s) método(s) proposto(s)
v. Quaisquer outros controlos relevantes em vigor

b) O uso de métodos de autenticação multifator deve ser baseado na criticidade do ativo de informação considerando os fatores acima e deve ser implementado e mantido com segurança.

c) O uso do Single Sign-On (SSO) deve ser habilitado para todos os sistemas internos que o suportem, a menos que os requisitos de segurança sejam considerados tais que um login adicional seja necessário.

Fatec Mauá

➢ AUTENTICAÇÃO DE USUÁRIO, SENHAS E CREDENCIAIS (2/3)

2. AUTENTICAÇÃO DE USUÁRIO PARA CONEXÕES EXTERNAS

a) Quando qualquer dispositivo externo deseja ser conectado à rede da organização (incluindo acesso remoto à rede via VPN), a aprovação específica deve ser obtida da Função de Provisionamento antes de se conectar.

b) Quando tecnicamente viável, o Single-Sign-On com autenticação de 2 fatores também deve ser usado para essas conexões externas.

Fatec Mauá

➢ AUTENTICAÇÃO DE USUÁRIO, SENHAS E CREDENCIAIS (3/3)

3. SENHAS E CREDENCIAIS

a) As credenciais de usuário não podem ser utilizadas por ninguém além das pessoas para as quais foram emitidas.

b) Uma senha temporária deve ser criada na configuração da conta e comunicada ao usuário por meios seguros. O usuário deve ser solicitado a alterar a senha no primeiro uso da conta.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

c) As credenciais de todos os sistemas são consideradas informações confidenciais e nunca devem ser anotadas ou transmitidas sem criptografia. Isso inclui senhas, autenticadores ou qualquer outra chave privada ou credencial secreta.

d) A identidade de um usuário deve ser verificada por meio de mecanismos adequados de contestação e/ou resposta antes de qualquer alteração nas credenciais de um usuário.

e) Senhas, chaves SSH e outros autenticadores criptográficos devem ser alterados caso o autenticador seja perdido ou considerado comprometido.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

f) Quando tecnicamente viável, todos os sistemas e senhas de aplicativos devem aderir ao

Anexo C: "Política de Senha Forte".

g) As senhas de contas de serviço e de sistema não devem ser divulgadas a indivíduos. Quando tecnicamente inviável, o conhecimento de tais senhas deve ser limitado a funcionários autorizados pelo proprietário do ativo e deve estar em conformidade com os padrões estabelecidos para contas de serviço no **Anexo C**: "Política de Senha Forte"relativos à complexidade, frequência, alteração e características de reutilização.

h) Onde não for tecnicamente viável aplicar o **Anexo C**: "Política de Senha Forte", senhas e autenticadores devem ser definidos para seguir um conjunto mínimo razoável de requisitos de complexidade, práticas rotacionais, inatividade e bloqueio de acordo com a documentação específica do sistema, nível de risco, práticas recomendadas ou classificação do sistema de TI.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

i) As senhas não devem ser "codificadas" ou armazenadas em formato de "texto sem formatação" em aplicativos de software.
j) As senhas padrão do fornecedor devem ser modificadas após a instalação de sistemas ou software.
k) Sempre que tecnicamente possível, as palavras-passe temporárias devem ser definidas com um valor único e expirar no prazo de 72 horas, solicitando a alteração imediata da palavra-passe na primeira utilização.

Fatec Mauá

➢ REDES E SISTEMAS (1/2)

1. CONTROLE DE ACESSO A REDE E SISTEMAS

a) O acesso à rede deve ser restrito a indivíduos, dispositivos e sistemas autorizados.

b) Os sistemas e/ou dispositivos não devem ser conectados à rede da [Empresa] sem a autorização prévia do proprietário do ativo da [Empresa] correspondente.

4. Capítulo: POLÍTICA DE CONTROLE DE ACESSO

Fatec Mauá

c) A Função de Provisionamento deve ser responsável por manter o controle de acesso à rede e impedir que dispositivos não autorizados acessem a rede.

d) A postura padrão deve ser negar todo o acesso à rede, a menos que seja especificamente autorizado ou permitido.

Fatec Mauá

➢ REDES E SISTEMAS (2/2)

2. CONTROLE DE ACESSO A REDE E SISTEMAS

a) Todas as permissões e métodos de acesso devem ser controlados pela Função de Provisionamento seguindo os princípios de "segregação de funções", "privilégio mínimo" e "necessidade de saber".

b) Parceiros ou fornecedores terceirizados devem entrar em contato com a Função de Provisionamento para solicitar permissão para se conectar à rede e um log de atividade deve ser mantido.

c) As agências parceiras ou fornecedores terceirizados não devem receber detalhes sobre como acessar a rede da organização sem a permissão da Função de Provisionamento.

d) Quaisquer alterações nas conexões do fornecedor (por exemplo, na rescisão de um contrato) devem ser imediatamente enviadas à Função de Provisionamento para que o acesso possa ser atualizado ou interrompido.

5. Capítulo: MONITORAMENTO DA POLÍTICA

Fatec Mauá

A área de **Governança, Riscos e Conformidade de Segurança da Informação** revisará essa política **pelo menos uma vez por ano**, quando a postura de segurança da organização mudar ou quando mudanças relevantes nos requisitos da política forem consideradas necessárias.

Quaisquer alterações ao conteúdo deste documento devem ser analisadas e autorizadas pelo Diretor de Segurança da Informação.

6. Capítulo: CONFORMIDADE

Fatec Mauá

Todos os funcionários estão sujeitos a seguir os requisitos descritos aqui, a menos que uma exceção seja identificada e exigida pelos mesmos órgãos reguladores aos quais a [Empresa] está sujeita. Qualquer exceção ou desvio à Política de Segurança da Informação e às diretivas de suporte deve ser baseado em requisitos legislativos ou de negócios exclusivos.

Um pedido de exceção pode ser enviado ao Diretor de Segurança da Informação para consideração. As solicitações de exceção de política devem ser devidamente documentadas, o risco relacionado avaliado e submetido ao Lead, ao Risco de Segurança da Informação ou ao seu delegado antes que a renúncia ou exceção possa ser implementada.

6. Capítulo: CONFORMIDADE

Fatec Mauá

Todas as exceções ou desvios aprovados devem ser registrados e gerenciados no registro de risco e revisados anualmente.

À [Empresa] reserva-se o direito de tomar medidas disciplinares em relação ao pessoal, que podem incluir a demissão, por qualquer desvio do conteúdo da Política de Segurança da Informação ou quaisquer outras políticas destacadas na Política de Segurança da Informação.

Dependendo da gravidade da violação da política, isso pode levar a um processo de acordo com a lei local.

Fatec Mauá

➢ LISTA DE ANEXOS

1. Anexo A: "Glossário de Segurança da Informação"

2. Anexo B: "Manifesto de Segurança da Informação"

3. Anexo C: "Política de Senha Forte"

SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 05: POLÍTICA DE CONTROLE DE ACESSO