Swift Solutions

1. Política de Princípio do Menor Privilégio (Least Privilege):

Os usuários devem ser concedidos apenas os privilégios de acesso necessários para realizar suas funções específicas.

Acesso adicional deve ser concedido apenas quando estritamente necessário e justificado.

2. Política de Autenticação Forte:

Todos os usuários devem autenticar-se utilizando métodos de autenticação robustos, como senhas seguras, autenticação multifatorial (MFA) ou autenticação biométrica.

A autenticação deve ser exigida para todos os acessos, especialmente aos sistemas e dados sensíveis.

3. Política de Segregação de Funções (Segregation of Duties - SoD):

As funções e responsabilidades dos usuários devem ser claramente definidas e separadas para evitar conflitos de interesse e fraudes.

Usuários com funções distintas devem ser impedidos de acessar recursos críticos de forma inapropriada.

4. Política de Controle de Acesso Baseado em Função (Role-Based Access Control - RBAC):

O acesso dos usuários deve ser atribuído com base nas suas funções e responsabilidades dentro da organização.

O acesso deve ser revisto regularmente para garantir que esteja alinhado com as funções atuais dos usuários.

5. Política de Revisão Periódica de Acesso:

Os privilégios de acesso dos usuários devem ser revisados periodicamente para garantir que permaneçam apropriados e justificados.

As revisões devem ser documentadas e arquivadas para fins de auditoria e conformidade.

6. Política de Controle de Acesso Físico:

O acesso físico às instalações, áreas restritas e equipamentos sensíveis deve ser restrito a pessoal autorizado.

Mecanismos de controle de acesso, como cartões de identificação, câmeras de segurança e biometria, devem ser implementados e mantidos.

7. Política de Criptografia de Dados:

Todos os dados sensíveis devem ser criptografados durante o armazenamento e a transmissão para protegê-los contra acesso não autorizado.

Mecanismos de criptografia devem ser selecionados com base nas melhores práticas e nos requisitos de segurança da informação.

8. Política de Auditoria de Acesso:

Deve ser conduzida auditoria regular das atividades de acesso para detectar e responder a comportamentos suspeitos ou não autorizados.

Registros de auditoria devem ser revisados periodicamente para identificar tendências, anomalias e violações de segurança.

9. Política de Monitoramento de Acesso:

Deve ser implementado um sistema de monitoramento contínuo para acompanhar as atividades de acesso aos sistemas e recursos críticos.

Alertas devem ser configurados para notificar os administradores sobre eventos de acesso incomuns ou suspeitos.

10. Política de Gestão de Incidentes de Segurança:

Deve ser estabelecido um procedimento claro para lidar com incidentes de segurança relacionados ao acesso não autorizado ou violações de dados.

As respostas a incidentes devem ser documentadas e analisadas para identificar áreas de melhoria e prevenção de futuros incidentes.