1.Security Standards

Na indústria de tecnologia, dependemos de padrões para estabelecer processos formais e reduzir riscos nos ambientes organizacionais. Algumas empresas criam seus próprios padrões de segurança, enquanto outras adotam normas estabelecidas por organizações como a **ISO** (International Organization for Standardization) e o **NIST** (National Institute of Standards and Technology).

Um dos principais aspectos padronizados é a criação de **senhas seguras**. Cada organização define suas próprias regras de complexidade, como comprimento mínimo, uso de caracteres especiais e frequência de troca de senhas. Além disso, padrões podem determinar que dispositivos como **switches, roteadores e firewalls** devem autenticar usuários via um **banco de dados centralizado**, como o **Active Directory** via **LDAP**, em vez de permitir contas locais.

Os padrões também regulam a **gestão de senhas**, definindo como as redefinições devem ser feitas para garantir segurança. Algumas diretrizes incluem requisitos para o **armazenamento seguro de credenciais**, o uso de **gerenciadores de senhas confiáveis** e restrições sobre **reutilização de senhas antigas**.

Além da autenticação, é necessário definir **padrões de controle de acesso**. Esses padrões determinam quem pode acessar determinados dados e sob quais condições. Algumas organizações proíbem o uso de **controle de acesso discricionário (DAC)**, exigindo **controle obrigatório (MAC)**, onde permissões são estritamente definidas por administradores. Outras exigem processos de **aprovação gerencial** ou treinamentos específicos antes de conceder acesso a determinados sistemas.

A **revogação de acessos** também segue padrões rígidos. Contas podem ser desativadas devido a falhas de segurança, expiração de contratos ou desligamento de funcionários. Para evitar acessos indevidos, políticas bem definidas garantem a remoção rápida de permissões quando necessário.

Além da segurança digital, **a proteção física** também é padronizada. Organizações podem exigir **crachás para identificação**, **bloqueios eletrônicos de portas** e até **biometria** para acesso a áreas restritas. Algumas empresas impõem regras específicas para funcionários, contratados e visitantes, garantindo níveis distintos de acesso. Também podem implementar **monitoramento contínuo**, com **detecção de movimento** em determinadas áreas para reforçar a segurança.

Outro aspecto crítico da segurança organizacional é a **criptografia**. Diretrizes estabelecem **quais algoritmos** devem ser utilizados para proteger dados, exigindo, por exemplo, que senhas sejam armazenadas como **hashes criptográficos com salt**. Além disso, os padrões definem diferentes requisitos para **dados em repouso (armazenados), em trânsito (transmitidos pela rede) e em uso (processados**

ativamente). Cada estado pode exigir um tipo de **criptografia específica** para garantir a proteção das informações.

Esses padrões garantem que todas as informações armazenadas e transmitidas sejam protegidas de forma consistente, reduzindo vulnerabilidades e mantendo a confidencialidade e integridade dos dados da organização.