***Implementação de Medidas de Segurança***

1. **Princípio do Menor Privilégio**: Os usuários devem ter apenas as permissões necessárias para realizar suas funções.
2. **Autenticação Multifatorial (MFA)**: Todos os acessos a sistemas críticos devem ser protegidos por autenticação multifatorial.
3. **Gerenciamento de Senhas**: Senhas devem ter requisitos mínimos de complexidade e expiração regular.
4. **Acesso Baseado em Funções (RBAC)**: As permissões devem ser atribuídas com base nas funções dos usuários na organização.
5. **Revisões Regulares de Acesso**: Realizar revisões periódicas das permissões de acesso para garantir que sejam adequadas.
6. **Acesso Remoto Seguro**: O acesso remoto a sistemas deve ser feito por meio de VPNs seguras e criptografadas.
7. **Desativação de Contas Inativas**: Contas de usuários inativas por mais de 30 dias devem ser desativadas automaticamente.
8. **Controle de Acesso Físico**: As áreas que contêm sistemas críticos devem ter controle de acesso físico rigoroso.
9. **Auditoria de Acesso**: Registros de acesso devem ser mantidos e revisados regularmente para detectar atividades suspeitas.
10. **Segregação de Funções**: As funções críticas devem ser segregadas para evitar conflitos de interesse e fraudes.
11. **Treinamento em Segurança**: Todos os usuários devem receber treinamento regular sobre as políticas de segurança e controle de acesso.
12. **Acesso a Dados Sensíveis**: O acesso a dados sensíveis deve ser restrito e monitorado, com justificativa necessária para acesso.
13. **Controles de Acesso Temporários**: Acesso temporário deve ser concedido apenas em circunstâncias específicas e revogado imediatamente após o uso.
14. **Gerenciamento de Incidentes de Segurança**: Deve haver um procedimento claro para revogar acessos em caso de incidentes de segurança.
15. **Monitoramento de Atividades de Acesso**: Atividades suspeitas devem ser monitoradas e analisadas em tempo real.
16. **Restrição de Dispositivos**: O acesso a sistemas críticos deve ser restrito a dispositivos autorizados.
17. **Política de Uso Aceitável**: Deve existir uma política clara sobre o uso aceitável dos recursos de TI, incluindo limites de acesso.
18. **Consentimento para Acesso**: Usuários devem fornecer consentimento explícito para acessar dados pessoais ou sensíveis.
19. **Acesso Condicional**: O acesso a recursos deve ser baseado em condições específicas, como localização geográfica ou estado do dispositivo.
20. **Política de Revogação de Acesso**: A revogação de acesso deve ser automática ao desligamento de um funcionário ou ao término de um projeto.