UNIVERSIDADE RUY BARBOSA - WYDEN

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Gabriella Mizrach Benevides

Relatório de Definição de Política de Segurança

SALVADOR

[2025]

- **Introdução à Segurança em Sistemas Operacionais:**

A segurança da informação é um dos pilares fundamentais na administração de infraestrutura de TI moderna. Com o aumento exponencial de ameaças cibernéticas, como *ransomwares* e ataques de engenharia social, a proteção do Sistema Operacional deixa de ser uma opção e torna-se um requisito obrigatório para garantir a confidencialidade, integridade e disponibilidade dos dados corporativos.

O Windows, sendo um dos sistemas operacionais mais utilizados em ambientes corporativos, exige uma configuração rigorosa de suas políticas. "Secure by design" e "Defense in depth" (Defesa em Profundidade) são conceitos que ilustram a necessidade de aplicar camadas de segurança que vão desde a autenticação do usuário até a criptografia do disco.

Este relatório apresenta a definição e a aplicação prática de uma Política de Segurança baseada em diretrizes de mercado. Serão demonstradas configurações de endurecimento (*hardening*) do sistema Windows 10 Pro, utilizando ferramentas administrativas como o Editor de Política de Grupo, Windows Defender Firewall e controles de acesso, visando mitigar vulnerabilidades e estabelecer um ambiente controlado e seguro.

- **Assunto:** Diretrizes de Segurança da Informação.
- **Objetivo:** Implementar uma postura de defesa, onde múltiplas camadas de segurança protegem os ativos de informação.

1. Política de Senha

- **Tamanho Mínimo (8+):** Senhas curtas são vulneráveis a ataques de força bruta. Cada caractere adicional aumenta o tempo necessário para a quebra de senha.
- **Complexidade (Maiúscula, minúscula, número, símbolo):** Evita ataques baseados em dicionário. A complexidade garante que o "espaço de busca" para um invasor seja o maior possível.
- **Expiração (60 dias):** Limita a janela de oportunidade para um invasor que tenha comprometido uma credencial.
- **Histórico (Não repetir as 5 últimas):** Impede que usuários alternem entre duas ou três senhas fáceis de lembrar, anulando o propósito da expiração.

2. Política de Autenticação

- **Login Nominal:** Fundamental para a rastreabilidade. Em caso de incidente, é preciso saber quem realizou a ação, e não apenas a conta genérica.
- **Autenticação Multifator (2FA):** O 2FA exige um fator adicional (como um app, token, biometria etc), tornando a senha roubada inútil sozinha.
- **Bloqueio (Após 3 tentativas):** Mitigação direta contra ataques de força bruta. O ideal é um bloqueio progressivo (ex: 5 min, depois 30 min, depois bloqueio manual) para evitar ataques de Negação de Serviço no usuário.

3. Controle de Permissões

- **Princípio do Privilégio Mínimo:** Um usuário ou processo deve ter apenas as permissões estritamente necessárias para realizar sua função.
- **Grupos de Usuários:** A gestão de permissões deve ser feita por função. Ex: O grupo "Analista de dados" tem acesso de leitura ao banco de dados X. Quando um novo analista entra, ele é adicionado ao grupo e herda as permissões corretas.

4. Acesso Externo

- **VPN (Rede Privada Virtual):** Cria um túnel criptografado entre o usuário externo e a rede interna. Garante a confidencialidade e integridade dos dados, mesmo em redes públicas (ex: Wi-Fi de cafeteria).

5. Firewall e Proxy

- **Firewall :** O firewall de borda aplicará regras gerais. O firewall de host aplicará regras específicas.
- **Regras:** A política padrão deve ser bloquear tudo. Apenas os serviços e portas explicitamente necessários (ex: porta 443 para HTTPS) devem ser liberados.

- **Proxy :** Atua como um intermediário. Permite filtragem de conteúdo (bloqueio de domínios de malware/phishing), logging detalhado de acessos e cache.

6. Antivírus/Antimalware

- **Detecção :** Utilizar antivírus tradicionais que usam assinaturas (listas de malware conhecido) e soluções modernas que usam análise comportamental para detectar ameaças novas.
- **EDR :** É a evolução do antivírus, não apenas bloqueia, mas registra toda a atividade do sistema, permitindo que analistas de segurança investiguem como uma infecção ocorreu.

7. Controle de Portas

- **Desabilitar Serviços:** Fechar a porta no firewall e desabilitar o serviço se não for necessário.
- **Portas de Risco:** Portas de gerenciamento legado (ex: Telnet 23, FTP 21) são perigosas por trafegarem dados e credenciais em texto claro. Devem ser substituídas por equivalentes seguros (ex: SSH 22, SFTP).

8. Política de Backup

- **RPO e RTO:** Definir o Recovery Point Objective (quanto tempo de dados podemos perder. Ex: 1 hora) e o Recovery Time Objective (em quanto tempo o sistema precisa voltar ao ar. Ex: 4 horas).
- **Testes de Restauração:** Realizar testes trimestrais que validem a integridade dos dados e o procedimento de restauração.
- **Integridade:** Backups devem ser armazenados de forma que não possam ser alterados ou criptografados.

9. Criptografia de Senhas e Dados

- **BitLocker,:** Protege os dados caso o dispositivo físico (notebook, HD) seja roubado. Sem a chave, os dados no disco são ilegíveis.
- **Dados em Trânsito (TLS/SSL):** Garante que a comunicação entre o cliente (navegador) e o servidor (site) não possa ser interceptada.
- **Criptografia de Senhas (Hashing):** Usar algoritmos de hash (ex: bcrypt, Argon2) torna inviável a quebra de senhas mesmo se o banco de dados vazar.

10. Token e 2FA

- **Métodos:**
    1. **TOTP (Apps Autenticadores):** Google/Microsoft Authenticator, Authy.
    2. **U2F:** (YubiKey) O padrão mais seguro, imune a phishing, pois a autenticação é ligada ao domínio do site.

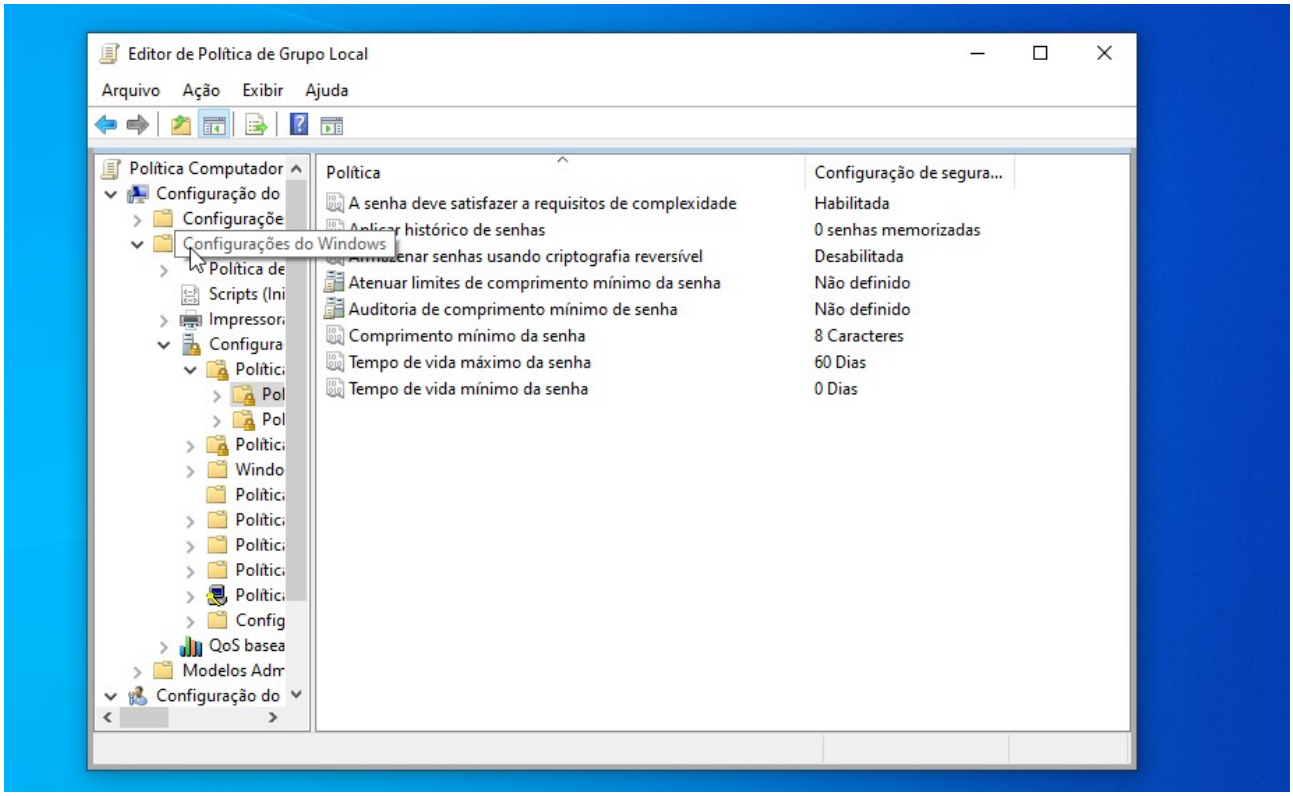
- **Uso Mandatório:** Essencial para contas administrativas, acesso financeiro e qualquer acesso externo (VPN, e-mail).

11. Treinamento de Usuários

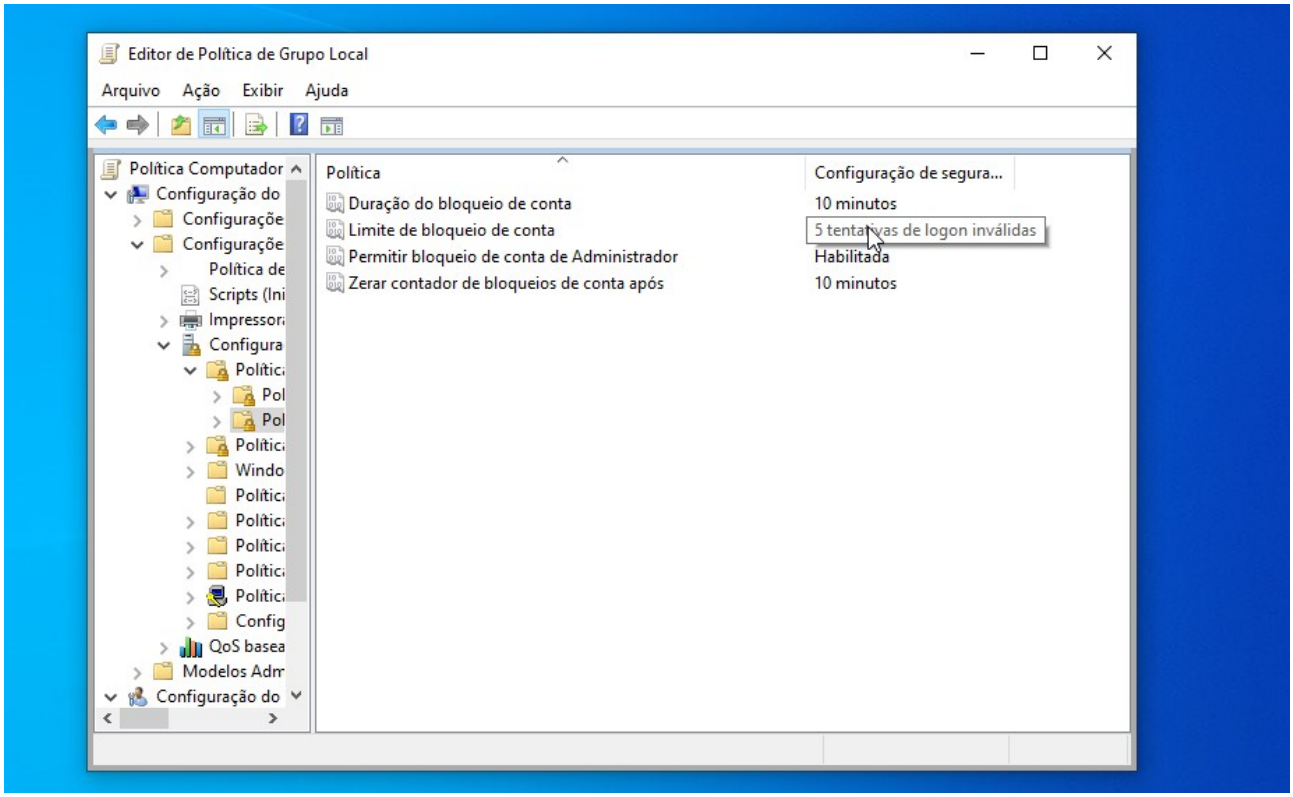
- **Variações de Ataque:** Treinar para identificar não só Phishing (e-mail em massa), mas Spear-Phishing (ataque direcionado), Vishing (phishing por voz) e Smishing (phishing por SMS).
- **Cultura de Segurança:** Criar um ambiente onde o usuário se sinta seguro para reportar um incidente suspeito imediatamente, sem medo de punição.

• PRINTS:

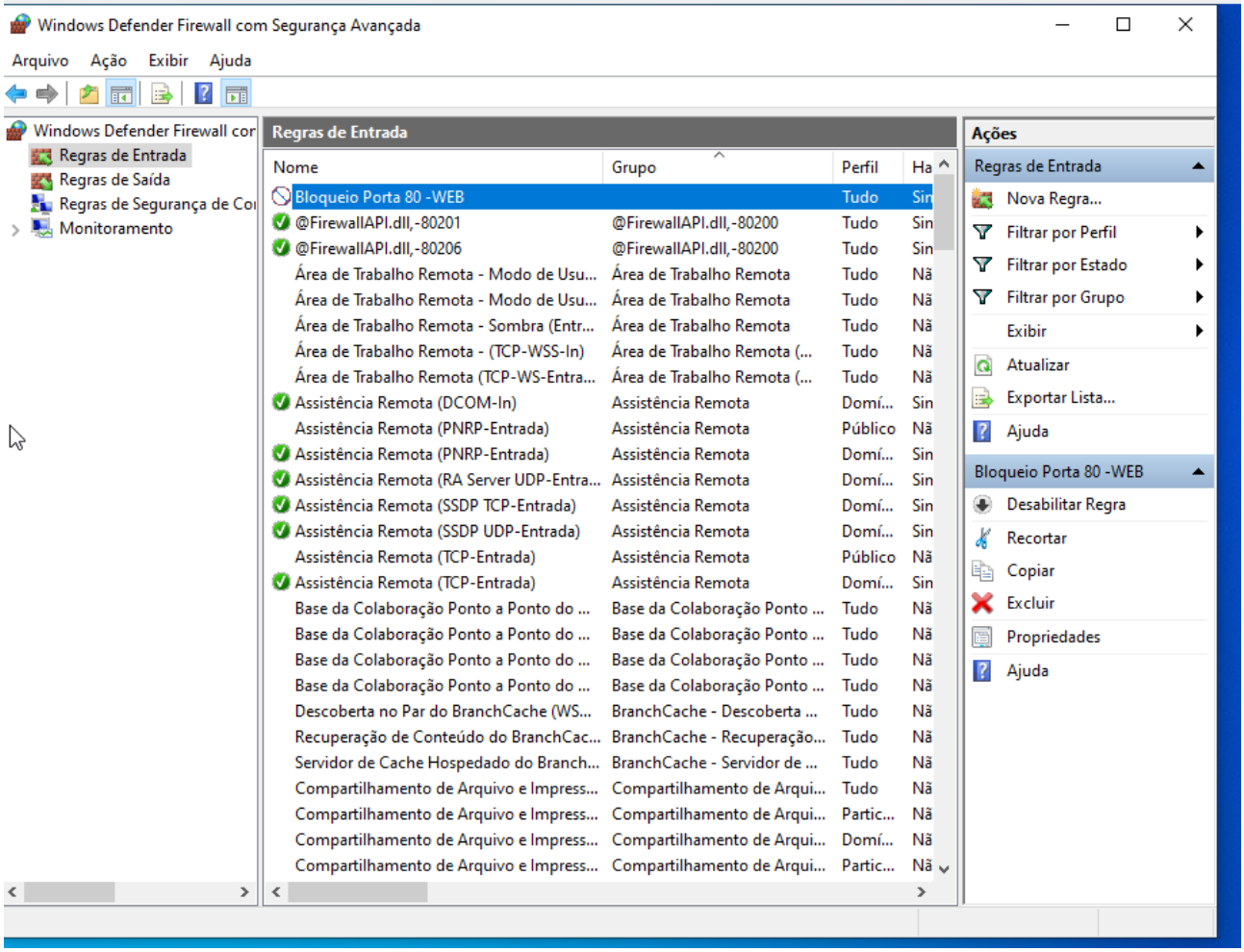
1. Senha:



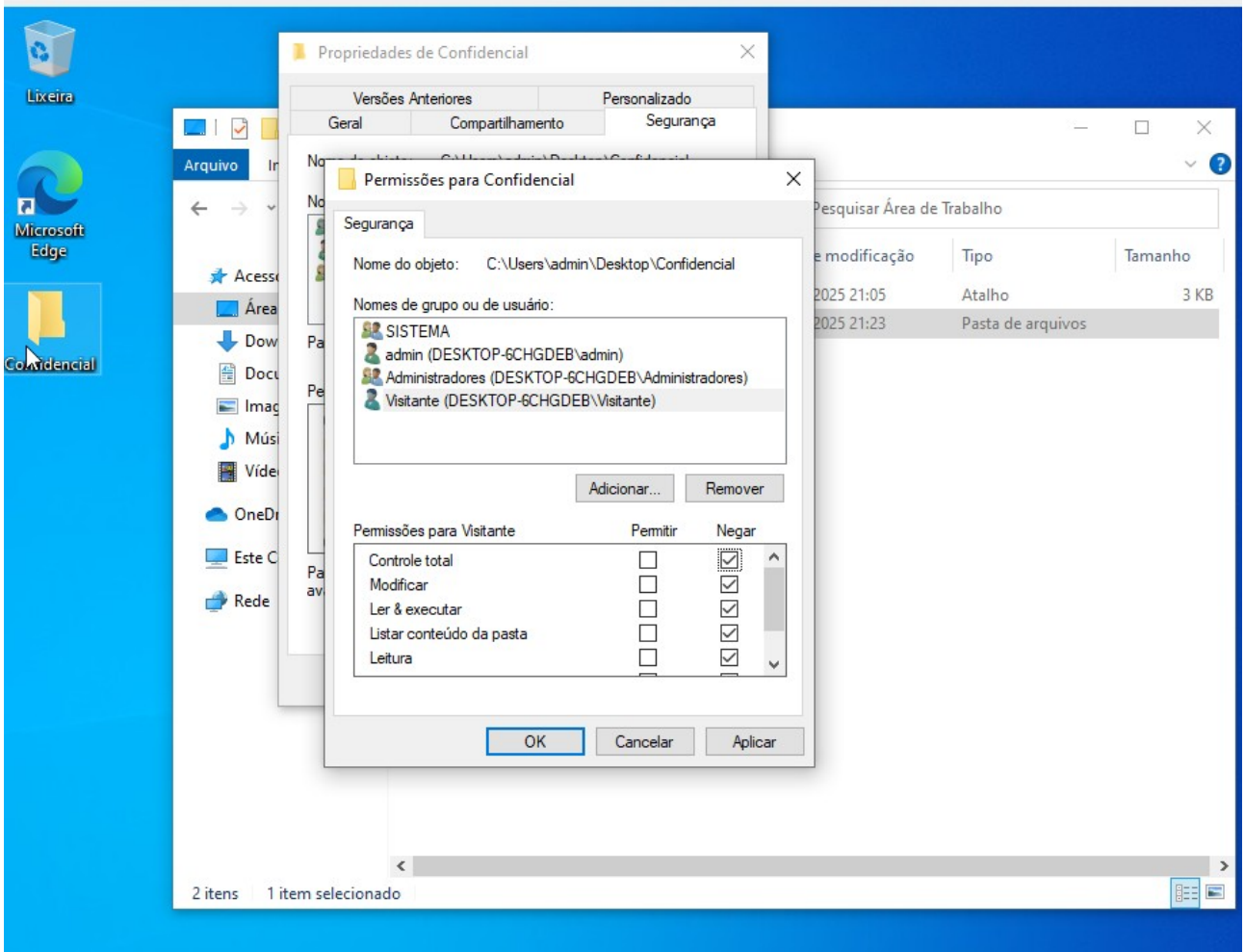
2. Bloqueio:



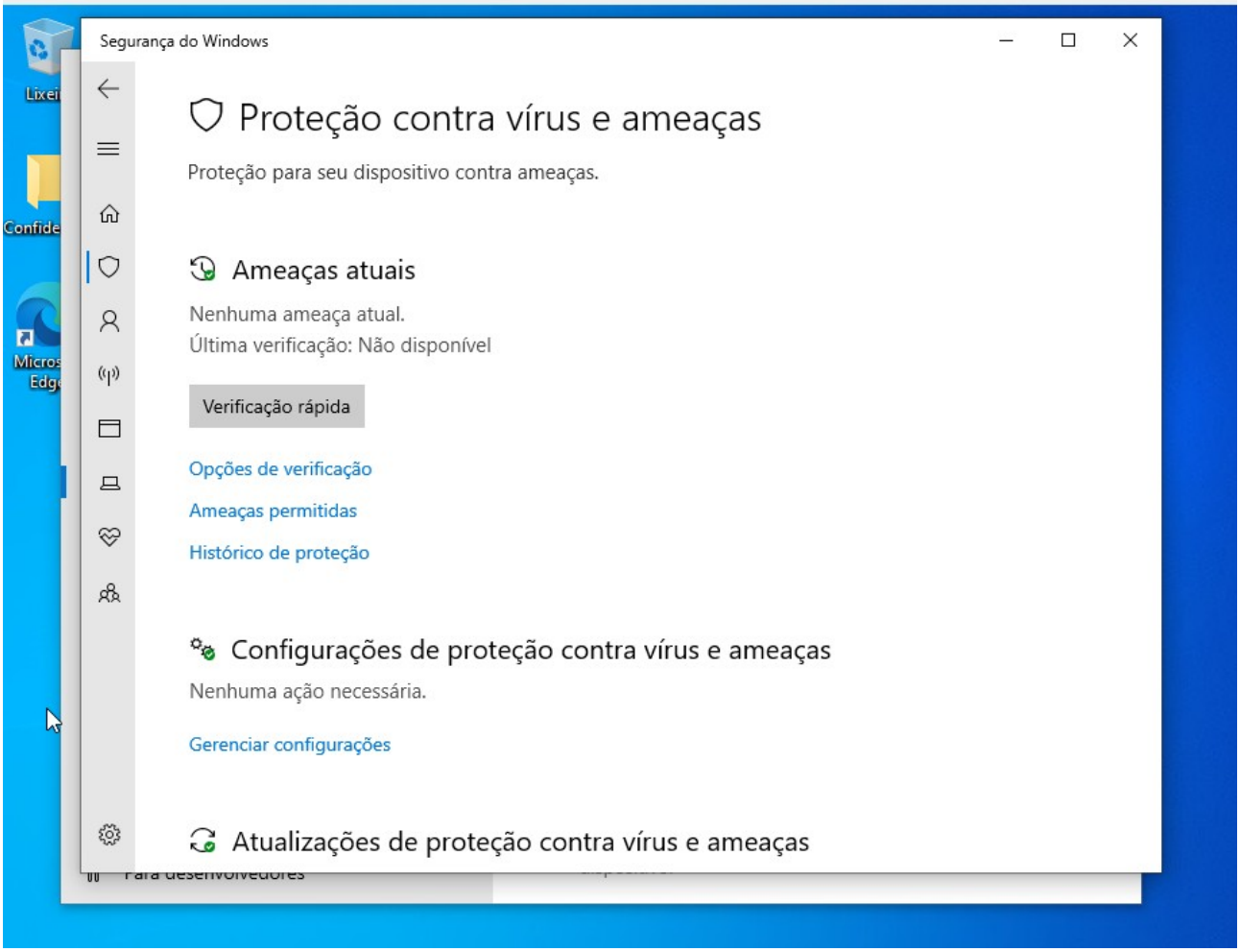
3. Firewall:



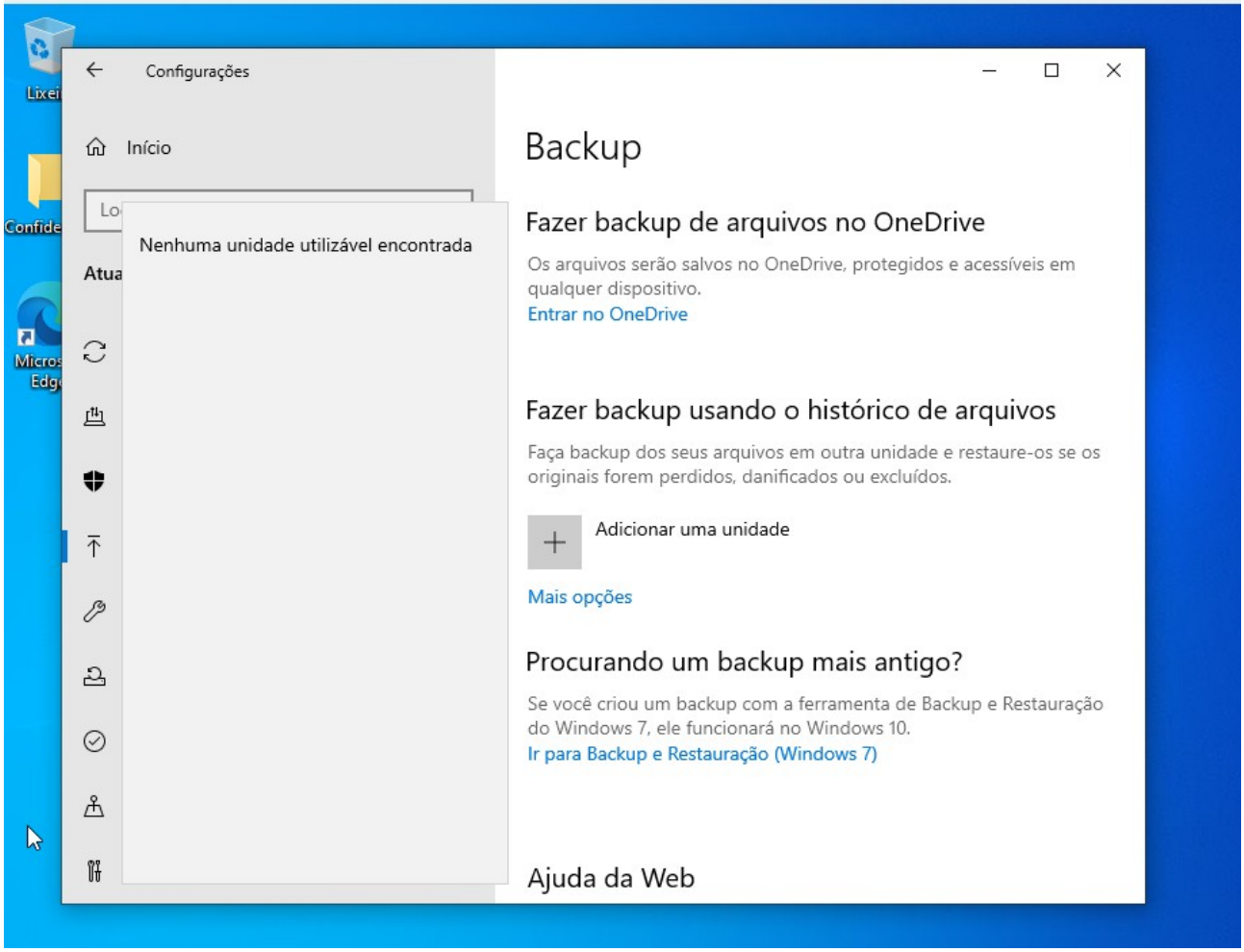
4. ACL:



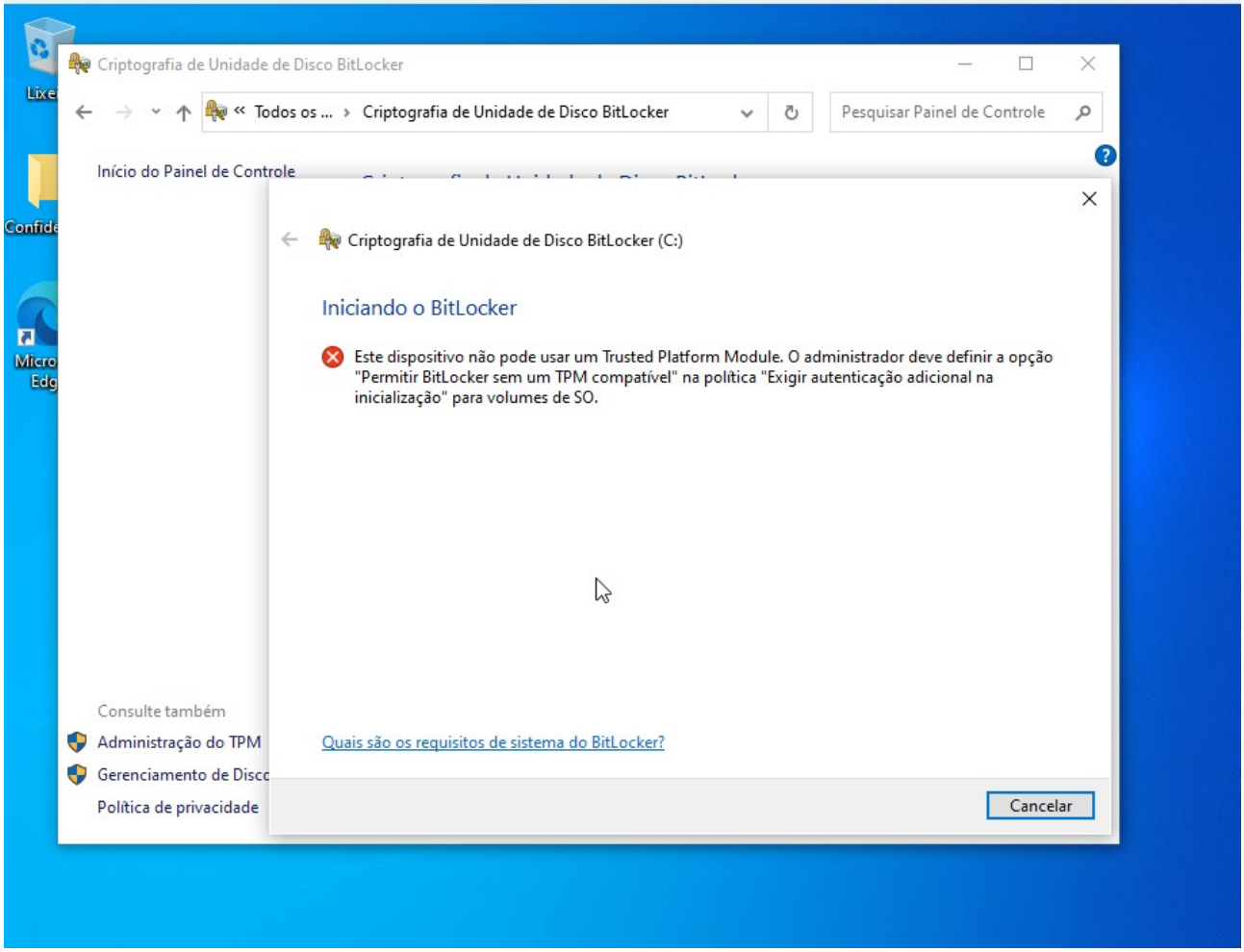
5. Proteção:


Segurança do Windows
Proteção contra vírus e ameaças
Proteção para seu dispositivo contra ameaças.
Ameaças atuais
Nenhuma ameaça atual.
Última verificação: Não disponível
Verificação rápida
Opções de verificação
Ameaças permitidas
Histórico de proteção
Configurações de proteção contra vírus e ameaças
Nenhuma ação necessária.
Gerenciar configurações
Atualizações de proteção contra vírus e ameaças

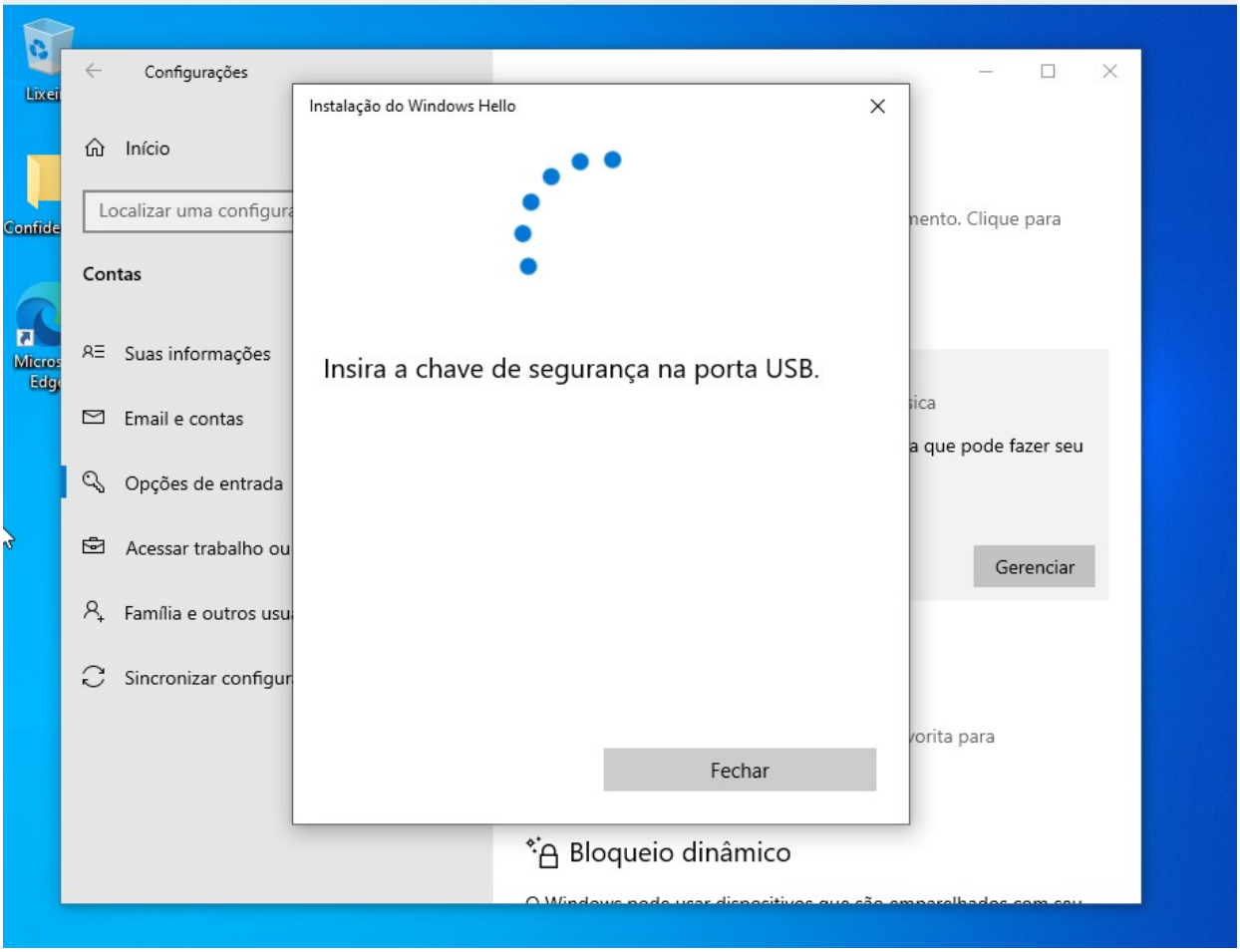
6. Backup:


Configurações
Início
Nenhuma unidade utilizável encontrada
Backup
Fazer backup de arquivos no OneDrive
Os arquivos serão salvos no OneDrive, protegidos e acessíveis em qualquer dispositivo.
Entrar no OneDrive
Fazer backup usando o histórico de arquivos
Faça backup dos seus arquivos em outra unidade e restaure-os se os originais forem perdidos, danificados ou excluídos.
Adicionar uma unidade
Mais opções
Procurando um backup mais antigo?
Se você criou um backup com a ferramenta de Backup e Restauração do Windows 7, ele funcionará no Windows 10.
Ir para Backup e Restauração (Windows 7)
Ajuda da Web

7. BitLocker:


Criptografia de Unidade de Disco BitLocker
Todos os ... › Criptografia de Unidade de Disco BitLocker
Pesquisar Painel de Controle
Início do Painel de Controle
Criptografia de Unidade de Disco BitLocker (C:)
Iniciando o BitLocker
Este dispositivo não pode usar um Trusted Platform Module. O administrador deve definir a opção "Permitir BitLocker sem um TPM compatível" na política "Exigir autenticação adicional na inicialização" para volumes de SO.
Consulte também
Administração do TPM
Política de privacidade
Quais são os requisitos de sistema do BitLocker?
Cancelar

8. 2FA


Configurações
Início
Contas
Suas informações
Email e contas
Opções de entrada
Gerenciar
Bloqueio dinâmico
Instalação do Windows Hello
Insira a chave de segurança na porta USB.
Fechar

- **Conclusão e Análise Crítica do Ambiente Configurado:**

A implementação prática das políticas de segurança no ambiente virtualizado permitiu validar a eficácia das ferramentas nativas do Windows 10 Pro.

Pontos Fortes: O ambiente configurado demonstra robustez na gestão de identidades através das GPOs (*Group Policy Objects*), garantindo que senhas fracas sejam rejeitadas e que ataques de força bruta sejam mitigados pelo bloqueio automático de conta. Além disso, o uso de ACLs (Listas de Controle de Acesso) provou ser eficaz para segregar dados confidenciais, impedindo que usuários não autorizados visualizem ou modifiquem arquivos críticos. A regra de Firewall criada adicionou uma camada extra de proteção de borda, essencial para controlar o tráfego de entrada e saída.

Limitações e Pontos de Melhoria: A execução na maquina virtual apresentou limitações ligadas ao hardware simulado. A ativação completa do BitLocker, por exemplo, foi restringida pela ausência de um chip TPM (*Trusted Platform Module*) físico na máquina virtual, o que em um cenário real exigiria hardware compatível ou configurações adicionais de *startup key*.

Considerações Finais: Com isso, é possível concluir que as configurações aplicadas elevam significativamente o nível de segurança base do sistema operacional. Para um cenário corporativo real, recomenda-se a escalabilidade dessas políticas através de um domínio Active Directory e a implementação de soluções de backup em nuvem para garantir redundância geográfica, superando as limitações do armazenamento local único testado neste trabalho.