SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

Guia CIS-Hardening

Windows Server 2022

2024

GOVERNO DO ESTADO DE RONDÔNIA

Cel. Marcos José Rocha dos Santos

Governador

Sérgio Gonçalves da Silva

Vice-Governador

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Cel. Delner Freire

Superintendente

Gabriel Carrijo Bento Teixeira

Diretor Técnico

COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva

Coordenador de Segurança da Informação

ELABORAÇÃO

André Luís Cabral da Silva

Analista de Segurança da Informação

REVISÃO

Daltro Barbosa Filho

Gerente de Prevenção e Respostas a Incidentes

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	20/09/2023	André Luís Cabral da Silva	Criação do documento
2.0	20/06/2024	André Luís Cabral da Silva	Atualizações de itens e finalização
3.0	27/06/2024	Daltro Barbosa Filho	Revisão e atualização

LISTA DE ABREVIATURAS

SETIC	Superintendência Estadual de Tecnologia da Informação e Comunicação
CAF	Coordenadoria de Administração e Finanças
CAGD	Coordenadoria de Análise e Gestão de Dados
COGE	Coordenadoria de Gestão Estratégica
CODE	Coordenadoria de Desenvolvimento
COINFRA	Coordenadoria de Infraestrutura e Serviços
COSEGI	Coordenadoria de Segurança da Informação
CI	Controle Interno
LGPD	Lei Geral de Proteção de Dados Pessoais
CIS	Center for Internet Security
GPREVI	Gerência de Prevenção e Respostas a Incidentes
GPO	Group Policy Object

SUMÁRIO

1 INTRODUÇÃO

Este manual *CIS Hardening* foi criado usando um processo de revisão de consenso composto por um comunidade global de especialistas no assunto. O processo combina o mundo real e experiência com informações baseadas em proteger seus ambientes.

Todas as informações foram geradas através da Solução Tenable IO. A Tenable foi certificada pelo CIS para realizar uma ampla variedade de auditorias de plataformas e aplicativos com base nos benchmarks de consenso de melhores práticas desenvolvidos pelo CIS.

Os participantes do consenso fornecem uma perspectiva de um conjunto diversificado de experiências, incluindo consultoria, desenvolvimento de software, auditoria e conformidade, pesquisa de segurança, operações, governo e jurídico.

Cada manual CIS passa por duas fases de revisão. A primeira fase ocorre durante o desenvolvimento inicial do manual. Durante esta fase, especialistas no assunto se reúnem para discutir, criar e testar versões preliminares das auditorias, levantando informações sobre a arquitetura do produto.

Esta discussão ocorre até que se chegue a um consenso sobre as recomendações. A segunda fase começa após a publicação da auditoria. Durante esta fase, todos os feedbacks fornecidos pelas equipes envolvidas são revisados pela equipe de segurança da informação para a incorporação do processo de *hardening*.

O Fluxo foi totalmente baseado na “*Orientação impulsionada pelo consenso da comunidade*”, desenvolvido pela Center for Internet Security, Inc. (CIS®)

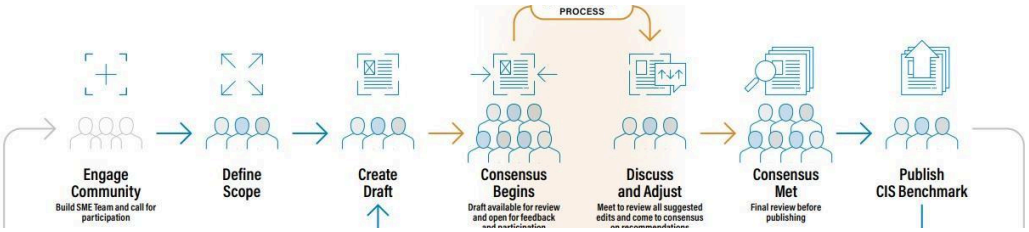


Figura 1: Orientação impulsionada pelo consenso da comunidade.

Este manual tem por objetivo descrever, através dos feedbacks e benchmarks gerados, todos os itens que estão em conformidade com o consenso CIS, dando um embasamento técnico de como replicar isso em ambientes semelhantes ao ambiente alvo auditado.

2 ALVO DE AUDITORIA

O Ambiente alvo da auditoria foram os Produtos ***Windows Server 2022*** que já se encontram em produção, e também um ambiente “Template”, no qual é usado para realizar clonagem para novos ambientes que porventura entrem na infraestrutura.

No levantamento do produto em questão, a *GPREVI* (*Gerência de Prevenção e Respostas a Incidentes da SETIC*) leva em consideração principalmente:

- Rastreabilidade - Configuração de eventos de sistema, principalmente de segurança e aplicações;
- Redução de Ataque de Superfície (ASR) - Utilizado os principais (Criação de processos filhos Adobe, Roubo de Credenciais, Assinatura de Eventos, etc);
- Melhorias de Protocolos Internos - RPC, NTLM, Kerberos;
- Desativação de Protocolos/Criptografias Legados - SMBv1 e RC4_HMAC_MD5;
- Segurança de Acesso de Contas - Reset, Inatividade e etc;
- Permissões de Serviços.

3 ITENS APLICADOS

1.1.2 Certifique-se de que a "*Idade máxima da senha*" esteja definida como '365 dias ou menos, mas não 0'.

Valor Atual: 42 dias.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age*

1.1.5 Certifique-se de que "A senha deve atender aos requisitos de complexidade" esteja definida como 'Ativada'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements*

1.1.7 Certifique-se de que 'Armazenar senhas usando criptografia reversível' esteja definido como 'Desativado'

Valor Atual: Desabilitado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption*

1.2.1 Certifique-se de que a 'Duração do bloqueio da conta' esteja definida como '15 minutos ou mais'

Valor Atual: 30.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration*

1.2.3 Certifique-se de que 'Redefinir contador de bloqueio de conta após' esteja definido como '15 ou mais minuto(s)

Valor Atual: 30.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after*

17.5.3 Certifique-se de que 'Logoff de auditoria' esteja definido para incluir 'Sucesso'

Valor Atual: Sucesso.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\AuditPolicies\Logon/Logoff\Audit Logoff*

17.9.3 Certifique-se de que 'Auditoria de mudança de estado de segurança' esteja definida para incluir 'Sucesso'

Valor Atual: Sucesso.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change*

17.9.4 Certifique-se de que a 'Extensão do Sistema de Segurança de Auditoria' esteja definida para incluir 'Sucesso''

Valor Atual: Sucesso.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension*

18.3.4 Certifique-se de que 'Ativar proteção contra gravação de tratamento de exceções estruturadas (SEHOP)' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)*

18.4.1 Certifique-se de que 'MSS: (AutoAdminLogon) Ativar logon automático (não recomendado)' esteja definido como 'Desativado'
Valor Atual: Desativado.
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)*

18.8.21.5 Certifique-se de que 'Desativar atualização em segundo plano da Política de Grupo' esteja definido como 'Desativado'
Valor Atual: Desativado.
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy*

18.9.108.2.1 Certifique-se de que 'Configurar atualizações automáticas' esteja definido como 'Ativado'
Valor Atual: Ativado.
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates*
18.9.108.2.2 Certifique-se de que 'Configurar atualizações automáticas' esteja definido como 'Ativado'
Valor Atual: Ativado.
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day*

18.9.47.4.2 Certifique-se de que 'Ingressar no Microsoft MAPS' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS\Join Microsoft MAPS*

18.9.47.9.1 Certifique-se de que 'Verificar todos os arquivos e anexos baixados' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\RealTime Protection\Scan all downloaded files and attachments*

18.9.47.9.2 Certifique-se de que 'Desativar proteção em tempo real' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\RealTime Protection\Turn off real-time protection*

18.9.65.3.9.4 Certifique-se de que 'Exigir autenticação de usuário para conexões remotas usando autenticação em nível de rede' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication*

18.9.91.1 Certifique-se de que 'Fazer login e bloquear o último usuário interativo automaticamente após uma reinicialização' esteja definido como 'Desativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Sign-in and lock last interactive user automatically after a restart*

19.1.3.1 Certifique-se de que 'Ativar proteção de tela' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Enable screen saver*

19.1.3.2 Certifique-se de que 'Proteger a proteção de tela com senha' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Password protect the screen saver*

19.1.3.3 Certifique-se de que 'Tempo limite de proteção de tela' esteja definido como 'Ativado: 900 segundos ou menos, mas não 0'

Valor Atual: 15 min.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout*

19.5.1.1 Certifique-se de que 'Desativar notificações do sistema na tela de bloqueio' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen*

19.6.6.1.1 Certifique-se de que 'Desativar Programa de Melhoria da Experiência de Ajuda' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings\Turn off Help Experience Improvement Program*

19.7.28.1 Certifique-se de que 'Desativar Programa de Melhoria da Experiência de Ajuda' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.*

19.7.4.1 Certifique-se de que 'Não preservar informações da zona em anexos de arquivo' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments*

19.7.4.2 Certifique-se de que 'Notificar programas antivírus ao abrir anexos' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments*

19.7.43.1 Certifique-se de que 'Sempre instalar com privilégios elevados' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges*

19.7.47.2.1 Certifique-se de que 'Impedir download de codec' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Windows Media Player\Playback \Prevent Codec Download*

19.7.8.1 Certifique-se de que 'Configurar destaque do Windows na tela de bloqueio' esteja definido como Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Configure Windows spotlight on lock screen*

19.7.8.2 Certifique-se de que 'Não sugerir conteúdo de terceiros no destaque do Windows' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not suggest third-party content in Windows spotlight*

19.7.8.3 Certifique-se de que 'Não usar dados de diagnóstico para experiências personalizadas' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not use diagnostic data for tailored experiences*

19.7.8.4 Certifique-se de que 'Desativar todos os recursos de destaque do Windows' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off all Windows spotlight features*

19.7.8.5 Certifique-se de que 'Desativar coleta Spotlight na área de trabalho' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Spotlight collection on Desktop*

2.2.1 Certifique-se de que 'Access Credential Manager como um chamador confiável' esteja definido como 'Ninguém'

Valor Atual: Ninguém.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller*

2.2.11 Certifique-se de que 'Alterar a hora do sistema' esteja definido como 'Administradores, SERVIÇO LOCAL'

Valor Atual: 'Administrators, LOCAL SERVICE'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time*

2.2.12 Certifique-se de que 'Alterar fuso horário' esteja definido como 'Administradores, SERVIÇO LOCAL'

Valor Atual: 'Administrators, LOCAL SERVICE'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone*

2.2.13 Certifique-se de que 'Criar um arquivo de paginação' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile*

2.2.14 Certifique-se de que 'Criar um objeto token' esteja definido como 'Ninguém'

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object*

2.2.15 Certifique-se de que 'Criar objetos globais' esteja definido como 'Administradores, SERVIÇO LOCAL, SERVIÇO DE REDE, SERVIÇO'

Valor Atual: 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects*

2.2.16 Certifique-se de que 'Criar objetos compartilhados permanentes' esteja definido como 'Ninguém'

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects*

2.2.18 Certifique-se de que 'Criar links simbólicos' esteja definido como 'Administradores, NT VIRTUAL MACHINE\Virtual Machines' (somente MS) - Administradores, NT VIRTUAL MACHINE\Virtual Machines

Valor Atual: 'Administrators’

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links*

2.2.19 Certifique-se de que 'Programas de depuração' esteja definido como 'Administradores'

Valor Atual: 'Administrators’

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs*

2.2.28 Certifique-se de que 'Ativar contas de computador e de usuário sejam confiáveis para delegação' esteja definido como 'Ninguém' (somente MS) - Ninguém

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation*

2.2.29 Certifique-se de que 'Forçar desligamento de um sistema remoto' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system*

2.2.30 Certifique-se de que 'Gerar auditorias de segurança' esteja definido como 'SERVIÇO LOCAL, SERVIÇO DE REDE'

Valor Atual: 'LOCAL SERVICE, NETWORK SERVICE'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits*

2.2.32 Certifique-se de que 'Representar um cliente após autenticação' esteja definido como 'Administradores, SERVIÇO LOCAL, SERVIÇO DE REDE, SERVIÇO' e (quando a função de servidor Web (IIS) com serviço de função de serviços da Web estiver instalada)'IIS_IUSRS' (somente MS) - IIS_IUSRS

Valor Atual: 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment \Impersonate a client after authentication*

2.2.33 Certifique-se de que 'Aumentar prioridade de agendamento' esteja definido como 'Administradores, Gerenciador de janelas\Grupo de gerenciadores de janelas'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority*

2.2.34 Certifique-se de que 'Carregar e descarregar drivers de dispositivo' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers*

2.2.35 Certifique-se de que 'Bloquear páginas na memória' esteja definido como 'Ninguém'

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory*

2.2.38 Certifique-se de que 'Gerenciar log de auditoria e segurança' esteja definido como 'Administradores' (somente MS) - Administradores

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log*

2.2.39 Certifique-se de que 'Modificar um rótulo de objeto' esteja definido como 'Ninguém'

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label*

2.2.4 Certifique-se de que 'Agir como parte do sistema operacional' esteja definido como 'Ninguém'

Valor Atual: Ninguém

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system*

2.2.40 Certifique-se de que 'Modificar valores do ambiente de firmware' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values*

2.2.41 Certifique-se de que 'Processo único de perfil' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks*

2.2.42 Certifique-se de que 'Executar tarefas de manutenção de volume' esteja definido como 'Administradores'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process*

2.2.43 Certifique-se de que 'Desempenho do sistema de perfil' esteja definido como 'Administradores, NT SERVICE\WdiServiceHost'

Valor Atual: 'Administrators'

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance*

2.2.44 Certifique-se de que 'Substituir um token de nível de processo' esteja definido como 'SERVIÇO LOCAL, SERVIÇO DE REDE'
Valor Atual: 'LOCAL SERVICE, NETWORK SERVICE'
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token*

2.2.48 Certifique-se de que 'Substituir um token de nível de processo' esteja definido como 'SERVIÇO LOCAL, SERVIÇO DE REDE'
Valor Atual: 'LOCAL SERVICE, NETWORK SERVICE'
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token*

2.2.6 Certifique-se de que 'Ajustar cotas de memória para um processo' esteja definido como 'Administradores, SERVIÇO LOCAL, REDE SERVIÇO'
Valor Atual: 'Administrators, LOCAL SERVICE, NETWORK SERVICE'
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process*

2.2.9 Certifique-se de que 'Permitir logon por meio de serviços de área de trabalho remota' esteja definido como 'Administradores, usuários de área de trabalho remota' (somente MS) - Administradores, usuários de área de trabalho remota
Valor Atual: 'Administrators, Remote Desktop Users'
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services*

2.3.1.3 Certifique-se de que 'Contas: status da conta de convidado' esteja definido como 'Desativado' (somente MS) - Desativado
Valor Atual: Desativado
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status*

2.3.1.4 Certifique-se de que 'Contas: Limitar o uso de senhas em branco na conta local apenas para logon do console' esteja definido como 'Ativado'
Valor Atual: Ativado
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only*

2.3.10.1 Certifique-se de que 'Acesso à rede: permitir tradução anônima de SID/nome' esteja definido como 'Desativado'
Valor Atual: Desativado
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation*

2.3.10.10 Certifique-se de que 'Acesso à rede: Restringir acesso anônimo a pipes nomeados e compartilhamentos' esteja definido como 'Ativado'
Valor Atual: Ativado
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares*

2.3.10.12 Certifique-se de que 'Acesso à rede: compartilhamentos que podem ser acessados anonimamente' esteja definido como 'Nenhum'
Valor Atual: Nenhum
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously*

2.3.10.13 Certifique-se de que 'Acesso à rede: modelo de compartilhamento e segurança para contas locais' esteja definido como 'Clássico - usuários locais autenticam como eles próprios'
Valor Atual: Clássico
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts*

2.3.10.13 Certifique-se de que 'Acesso à rede: modelo de compartilhamento e segurança para contas locais' esteja definido como 'Clássico - usuários locais autenticam como eles próprios'
Valor Atual: Clássico
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts*

2.3.10.2 Certifique-se de que 'Acesso à rede: não permitir enumeração anônima de contas SAM' esteja definido como 'Ativado' (somente MS) - Ativado
Valor Atual: Ativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts*

2.3.10.5 Certifique-se de que 'Acesso à rede: permitir que as permissões de todos sejam aplicadas a usuários anônimos' esteja definido como 'Desativado'
Valor Atual: Desativado
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users*

2.3.10.7 Configurar 'Acesso à rede: Pipes nomeados que podem ser acessados anonimamente' (somente MS) - Acesso à rede: Pipes nomeados que podem ser acessados anonimamente
Valor Atual: Nenhum
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously*

2.3.10.8 Configurar 'Acesso à rede: caminhos de registro acessíveis remotamente'
Valor Atual: *System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software \Microsoft\Windows NT\CurrentVersion*
Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).
Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths*

2.3.10.9 Configurar 'Acesso à rede: caminhos e subcaminhos de registro acessíveis remotamente'

Valor Atual:

System\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\Eventlog Software\Microsoft \OLAPServerSoftware\Microsoft\WindowsNT\CurrentVersion\PrintSoftware\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndexSystem\CurrentControlSet\Control\Terminal ServerSystem\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\WindowsNT\CurrentVersion\PerflibSystem\CurrentControlSet\Services\SysmonLog

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths*

2.3.11.5 Certifique-se de que 'Segurança de rede: não armazenar valor hash do LAN Manager na próxima alteração de senha' esteja definido como 'Ativado'

Valor Atual: Ativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change*

2.3.11.8 Certifique-se de que 'Segurança de rede: requisitos de assinatura do cliente LDAP' esteja definido como 'Negociar assinatura' ou superior'

Valor Atual: Negociar assinatura. Se o Transport Layer Security/Secure Sockets Layer (TLS/SSL) não tiver sido iniciado, a solicitação LDAP BIND será iniciada com a opção de assinatura de dados LDAP definida além das opções especificadas pelo chamador. Se o TLS/SSL tiver iniciado, a solicitação LDAP BIND será iniciada com as opções especificadas pelo chamador.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements*

2.3.13.1 Certifique-se de que 'Desligar: permitir que o sistema seja desligado sem precisar fazer logon' esteja definido como 'Desativado'

Valor Atual: Desabilitado. (Os operadores terão que fazer logon nos servidores para desligá-los ou reiniciá-los.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on*

2.3.15.1 Certifique-se de que 'Objetos do sistema: exigem insensibilidade a maiúsculas e minúsculas para sub sistemas não Windows' esteja definido como 'Ativado'

Valor Atual: Ativado. (Todos os subsistemas serão forçados a observar a insensibilidade a maiúsculas e minúsculas. Esta configuração pode confundir os usuários que estão familiarizados com qualquer sistema operacional baseado em UNIX que faça distinção entre maiúsculas e minúsculas.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on*

2.3.15.2 Certifique-se de que 'Objetos do sistema: fortalecer permissões padrão de objetos internos do sistema (por exemplo, links simbólicos)' esteja definido como 'Ativado'

Valor Atual: Ativado. (A DACL padrão é mais forte, permitindo que usuários que não sejam administradores leiam objetos compartilhados, mas não permitindo que esses usuários modifiquem objetos compartilhados que não criaram.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)*

2.3.17.5 Certifique-se de que 'Controle de conta de usuário: elevar apenas aplicativos UIAccess instalados em locais seguros' esteja definido como 'Ativado'

Valor Atual: Ativado. (Se um aplicativo estiver em um local seguro no sistema de arquivos, ele será executado somente com integridade do UIAccess.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations*

2.3.17.6 Certifique-se de que 'Controle de conta de usuário: executar todos os administradores no modo de aprovação de administrador' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode*

2.3.17.7 Certifique-se de que 'Controle de conta de usuário: alternar para a área de trabalho segura ao solicitar elevação' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation*

2.3.17.8 Certifique-se de que 'Controle de conta de usuário: virtualizar falhas de gravação de arquivo e registro em locais por usuário' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations*

2.3.2.2 Certifique-se de que 'Auditoria: desligue o sistema imediatamente se não for possível registrar auditorias de segurança' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits*

2.3.2.2 Certifique-se de que 'Dispositivos: Impedir que os usuários instalem drivers de impressora' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers*

2.3.6.1 Certifique-se de que 'Membro do domínio: criptografar ou assinar digitalmente dados de canal seguro (sempre)' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)*

2.3.6.2 Certifique-se de que 'Membro do domínio: criptografar digitalmente os dados do canal seguro (quando possível)' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)*

2.3.6.3 Certifique-se de que 'Membro do domínio: assinar digitalmente dados de canal seguro (quando possível)' esteja definido como 'Ativado'

Valor Atual: Ativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)*

2.3.6.4 Certifique-se de que 'Membro do domínio: Desativar alterações de senha da conta da máquina' esteja definido como 'Desativado'

Valor Atual: Desativado.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes*

2.3.6.5 Certifique-se de que 'Membro do domínio: duração máxima da senha da conta da máquina' esteja definido como '30 dias ou menos, mas não 0'

Valor Atual: 30 Dias.

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age*

2.3.6.6 Certifique-se de que 'Membro do domínio: Exigir chave de sessão forte (Windows 2000 ou posterior)' esteja definido como 'Ativado'

Valor Atual: Ativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key*

2.3.7.1 Certifique-se de que 'Logon interativo: Não requer CTRL+ALT+DEL' esteja definido como 'Desativado'

Valor Atual: Desativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL*

2.3.7.2 Certifique-se de que 'Logon interativo: não exibir o último login' esteja definido como 'Ativado'

Valor Atual: Ativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Don't display last signed-in*

2.3.7.7 Certifique-se de que 'Logon interativo: solicitar ao usuário que altere a senha antes da expiração' esteja definido como 'entre 5 e 14 dias'

Valor Atual: 5 dias

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration*

2.3.8.2 Certifique-se de que 'Cliente de rede Microsoft: assinar digitalmente as comunicações (se o servidor concordar)' esteja definido como 'Ativado'

Valor Atual: Ativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)*

2.3.8.3 Certifique-se de que 'Cliente de rede Microsoft: Enviar senha não criptografada para servidores SMB de terceiros' esteja definido como 'Desativado'

Valor Atual: Desativado

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers*

2.3.9.1 Certifique-se de que 'Servidor de rede Microsoft: Quantidade de tempo ocioso necessário antes de suspender a sessão' esteja definido como '15 ou menos minuto(s)'

Valor Atual: 15 minutos

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session*

2.3.9.4 Certifique-se de que 'Servidor de rede Microsoft: desconectar clientes quando o horário de logon expirar' esteja definido como 'Ativado'

Valor Atual: Habilitado. (As sessões do cliente com o serviço SMB são desconectadas à força quando o horário de logon do cliente expira.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire*

9.1.2 Certifique-se de que 'Firewall do Windows: Domínio: Conexões de entrada' esteja definido como 'Bloquear (padrão)'

Valor Atual: Bloquear (padrão). (O Firewall do Windows com Segurança Avançada bloqueará todas as conexões de entrada que não correspondam a uma regra de firewall de entrada neste perfil.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security \Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections*

9.1.3 Certifique-se de que 'Firewall do Windows: Domínio: Conexões de saída' esteja definido como 'Permitir (padrão)'

Valor Atual: Permitir (padrão). (O Firewall do Windows com Segurança Avançada permitirá todas as conexões de saída neste perfil, a menos que haja uma regra de firewall bloqueando-o explicitamente.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security \Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections*

9.1.3 Certifique-se de que 'Firewall do Windows: Domínio: Conexões de saída' esteja definido como 'Permitir (padrão)'

Valor Atual: Permitir (padrão). (O Firewall do Windows com Segurança Avançada permitirá todas as conexões de saída neste perfil, a menos que haja uma regra de firewall bloqueando-o explicitamente.)

Método de Implementação: Aplicado por meio do *GPO* (Group Policy Object).

Caminho da Diretiva: *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security \Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections*

4 ANEXOS

Auditorias usadas como base:

CIS_Microsoft_Windows_Server_2022_Benchmark_v1.0.0_L1_MS.audit from CIS Microsoft Windows Server 2022 Benchmark

CIS_Microsoft_Windows_Server_2022_Benchmark_v1.0.0_L2_MS.audit from CIS Microsoft Windows Server 2022 Benchmark

Fonte: *https://workbench.cisecurity.org/files/3709*

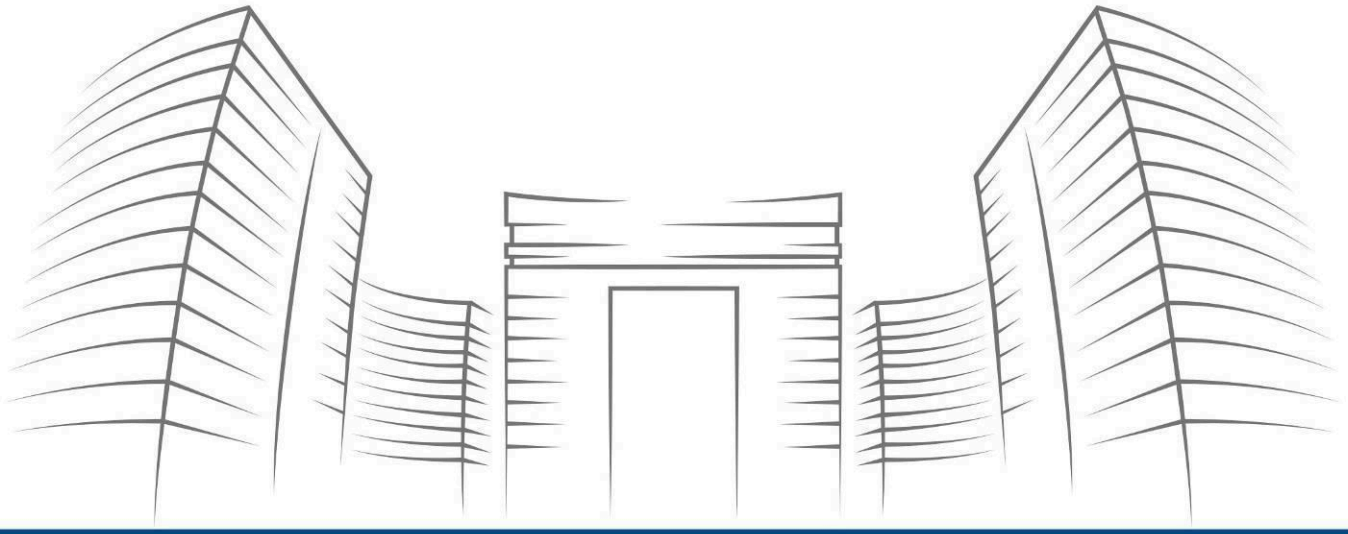
Ambientes Alvos - Windows Server 2022:

pau-de-mastro
jaboticaba
windows-server (template)
pauvelho
brejauva
mircia
bajuruvoca
jacare

SETIC
Superintendência Estadual de
Tecnologia da Informação e Comunicação

Governo do Estado de
RONDÔNIA

Wiki.SETIC
Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC
wiki.setic.ro.gov.br



setic.ro.gov.br
@setic.rondonia
Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470