CATEGORIA/REGISTRO:	VERSÃO:
MPO.076	7
CLASSIFICAÇÃO:	FASE:
OSTENSIVO	PRODUÇÃO
PROCESSOS:	DATA VIGÊNCIA:
N/A	31/05/2022
ÁREA RESPONSÁVEL:	DIRETORIA RESPONSÁVEL:
INFRAESTRUTURA	ТІ

IGOR FERREIRA





VERSÃO: 7

Sumário

1. INTRODUÇÃO	
2. REQUISITOS DO SISTEMA OPERACIONAL	
3. CRITÉRIOS MÍNIMOS DE SEGURANÇA	
4. CONFIGURANDO A ESTAÇÃO DE TRABALHO	
4.1 Criptografia de disco.	
4.2 Usuários	9
4.3 Não exibir o último nome de usuário	
4.4. Diretiva de senha	
4.5. Diretiva de bloqueio de conta	
4.6. Logon seguro.	
4.7. Serviço de log e auditoria	
4.8. Diretivas de log	
4.9. Proteção de tela	
4.10. Servico ntp	
4.11. Antivírus.	
4.12. Firewall	
4.13. Atualizações do Windows	
4.14. Software autêntico	
4.15. Acesso remoto	23



1. INTRODUÇÃO

Este manual visa orientar o usuário a executar as configurações de Segurança Lógica nas estações de trabalho do sistema operacional Windows seguindo os requisitos mínimos de segurança exigidos no DOC-03.01.

2. REQUISITOS DO SISTEMA OPERACIONAL

As configurações abaixo descritas neste manual somente funcionam nas seguintes versões do sistema operacional Windows.

- Windows 8 Profissional ou Enterprise 32bit ou 64bit
- Windows 8.1 Profissional ou Enterprise 32bit ou 64bit
- Windows 10 Profissional ou Enterprise 32bit ou 64bit
- Windows 11 Profissional ou Enterprise 32bit ou 64bit

OBS: Este manual foi baseado na versão do Windows 10 Profissional e serve também para as versões citadas acima, qualquer outra versão do Windows não e compatível com este manual.

3. CRITÉRIOS MÍNIMOS DE SEGURANÇA

3.1 A manutenção preventiva/corretiva das estações de trabalho deve ser realizada apenas por agentes autorizados (pelo fabricante, por assistência técnica autorizada ou por pessoa designada pela AC), dentro do período de manutenção recomendado. Os eventos de manutenção devem ser documentados.

3.2 A partição dos discos rígidos das estações devem ser criptografadas.

3.3 As estações de trabalho da AR, incluindo equipamentos portáteis, devem estar protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos.

3.4 O Agente de Registro não deve possuir perfil de administrador ou senha de root dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções.

3.5 As estações de trabalho da AR deverão conter apenas aplicações e serviços que sejam suficientes e necessários para as atividades corporativas.

4. CONFIGURANDO A ESTAÇÃO DE TRABALHO

As estações de trabalho de uso do Agente de Registro e da AR devem seguir as seguintes configurações de segurança:

4.1 Criptografia de disco

Configurar política para habilitar criptografia de disco Bitlocker

Clique no Menu iniciar > Busque por Executar > digite "gpedit.msc"





OSTENSIVO

ATEGORIAREGISTRC

MPO.076

PRODUÇÃO

VERSÃO

7

e	Digite o nome de um pr recurso da Internet e o V	rograma, pasta, docu Windows o abrirá par	ra você.	
Abrin	anedit mcc			
ADIII	gpeakanse		· ·	

Acesse o caminho: Configuração do Computador > Modelos Administrativos > Criptografia de Unidade de Disco BitLocker > Unidades do Sistema Operacional.



Obs.: Mantenha as configurações de acordo com a imagem.



MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO

7

Acesse o Painel de Controle > Sistema e Segurança > Criptografia de Unidade de Disco BitLocker.

🏘 Criptografia de Unidade de Disco	BitLocker	_		×	
← → 🕤 🏘 > Painel de C	Controle > Sistema e Segurança > Criptografia de Unidade de Disco BitLocker 🗸 🖏			P	
Início do Painel de Controle	Criptografia de Unidade de Disco BitLocker Proteja arquivos e pastas contra acesso não autorizado preservando as unidades com o BitLocker.			•	
	Unidade do sistema operacional				
	C: BitLocker desligado	6)		
	Cigar BitLocker				
	Unidades de dados fixas				
	Unidades de Dados Removíveis - BitLocker To Go Insira uma unidade flash USB removível para usar o BitLocker To Go.				
Consulte também Administração do TPM Gerenciamento de Disco					
Política de privacidade					

Clique em "Ligar BitLocker" > inserir um PIN > Defina uma senha PIN forte.

Representation de Unidade de Disco BitLocker (C:)

×

Escolher como desbloquear a unidade na inicialização

Algumas configurações são gerenciadas pelo administrador do sistema.

Para que seus dados tenham mais segurança, é possível definir que o BitLocker solicite uma senha ou uma unidade flash USB sempre que você iniciar o PC.

ightarrow Inserir uma unidade flash USB

Inserir uma senha

Cancelar



CATEGORIA REGISTRO MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO:

7

Clique em "Imprimir a chave de Recuperação" > Armazene em um local confiável que não seja na própria máquina local, para caso de necessidade de recuperação se esquecer ou bloquear o PIN. > Depois clique em Avançar.

		×	
~	🎭 Criptografia de Unidade de Disco BitLocker (C:)		
	Como deseja fazer o backup da chave de recuperação?		
	🚺 A chave de recuperação foi impressa.	-	
	Uma chave de recuperação pode ser usada para acessar seus arquivos e pastas se você estiver com problemas para desbloquear o seu PC. Convém ter mais de uma e manter cada uma em um local seguro que não seja o seu PC.)	
	ightarrow Salvar em uma unidade flash USB		
	\rightarrow Salvar em um arquivo		
	→ Imprimir a chave de recuperação		
	Como posso encontrar minha chave de recuperação mais tarde?		
	Avançar Cancela	r	

Selecione a opção "Criptografar a unidade inteira (mais lento, mas melhor para Pcs e unidades já em uso)" > Depois clique em Avançar.

Х

~	🎭 Criptografia de Unidade de Disco BitLocker (C:)
	Escolher que parte da unidade deve ser criptografada
	Se estiver configurando o BitLocker em uma nova unidade ou um novo PC, você só precisará criptografar a parte da unidade que está sendo usada. O BitLocker criptografa os novos dados automaticamente à medida que você os adiciona.
	Se estiver habilitando o BitLocker em um PC ou em uma unidade que já esteja em uso, considere criptografar a unidade inteira. Criptografar a unidade inteira garante a proteção de todos os dados excluídos por você, mas ainda pode conter informações que podem ser recuperadas.
	🔿 Criptografar apenas espaço em disco usado (mais rápido e melhor para novos PCs e unidades)
	Oriptografar a unidade inteira (mais lento, mas melhor para PCs e unidades já em uso)

Avançar Cancelar



CLASSIFICAÇÃO: OSTENSIVO

MPO.076

PRODUÇÃO

VERSÃO

7

Selecione a opção "Novo modo de criptografia" > Depois clique em Avançar.

Representation de Unidade de Disco BitLocker (C:)

Escolha o modo de criptografia a ser usado

O Windows 10 (Versão 1511) apresenta um novo modo de criptografia de disco (XTS-AES). Esse modo dá suporte adicional a integridade, mas não é compatível com versões anteriores do Windows.

Se você for usar uma versão anterior do Windows em uma unidade removível, escolha Modo compatível.

Caso se trate de uma unidade fixa, ou se você usar essa unidade somente em dispositivos com o Windows 10 (Versão 1511) ou posterior, escolha o novo modo de criptografia.

Novo modo de criptografia (indicado para unidades fixas neste dispositivo)

Modo compatível (indicado para unidades que podem ser movidas deste dispositivo)

Avançar	Cancelar
---------	----------

Continuar

Cancelar

Mantenha a opção "Executar verificação do sistema BitLocker"> Depois cliente em Continua.

		\sim
←	🎭 Criptografia de Unidade de Disco BitLocker (C:)	
	Você está pronto para criptografar essa unidade?	
	A criptografia pode levar algum tempo dependendo do tamanho da unidade.	
	Você pode continuar trabalhando enquanto a unidade está sendo criptografada, mas o PC pode ter um desempenho mais lento.	
	🖂 Executar verificação do sistema BitLocker	
	A verificação do sistema garante que o BitLocker pode ler as chaves de recuperação e de criptografia corretamente antes de criptografar a unidade.	
	O BitLocker reiniciará o computador antes de iniciar a criptografia.	
	Observação: essa verificação pode demorar um pouco, mas é recomendada para garantir que o método de desbloqueio selecionado funcione sem a chave de recuperação.	

Obs.: Após clicar em continuar, será necessário reiniciar o computador para verificar se a chave PIN e de recuperação estão corretas antes de iniciar a criptografia automaticamente.



VERSÃO: 7

Enter the reco	ery key for this drive		
Use the number key Recovery key ID (to	s or function keys F1-F10 (use F10 for dentify your key): F7085B32-	0).	
BitLocker needs you unexpectedly chang	recovery key to unlock your drive be ed.	cause Secure Boot policy has	
Here's how to find y - Try your Microsoft - For more informati	bur key: account at: aka.ms/myrecoverykey on go to: aka.ms/recoverykeyfaq		
Press Enter to co	ontinue		
Press Esc for mo	re recovery options		

Reference Criptografia de Unidade de Disco BitLocker					
	Criptografando				
	Unidade C: 1.8% Concluída				
		Fechar			
Gerenc	<u>Gerenciar o BitLocker</u>				



VERSÃO

7

4.2 Usuários

Todas as estações devem possuir acesso através de senha, e dois usuários, um padrão usado por um agente de registro e outro com perfil de administrador para o suporte.

Crie um usuário para o agente de registro e defina uma senha:

Clique Menu iniciar > Executar > digitar "compmgmt.msc".

Acesse o Gerenciamento do computador > Usuários e Grupos Locais > Usuários > Criar um novo usuário.

🚂 Gerenciamento do computado	r			
Arquivo Ação <mark>E</mark> xibir Ajuda				
🗢 🏟 🙇 📅 🧟 🗟 [
Gerenciamento do computado	Nome Administrador Convidado DefaultAcco Novo Usuário Nome de usuário: Nome completo: Descrição:	Nome completo agr	Descrição Conta interna para a ac Conta interna para ace <u>Uma conta de usuário</u> ? X	dministraçâ sso como α αerenciada erenciada
 Serviços e aplicativos 	Senha: Confirmar senha: O usuário dev O usuário não A senha nunc	e alterar a senha no próxir pode alterar a senha a expira	no logon	
	Ajuda	aoa	Criar Fechar	



MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO

7

Crie um usuário Administrador e defina uma senha:

🛃 Gerenciamento do computador				
Arquivo Ação Exibir Ajuda				
🗢 🔿 🙋 📅 🤷 🔂 👔				
Gerenciamento do computado Gerenciamento do sistema Gerenciamentas do sistema Gerenciador de Tarefas Gerenciador de Eventos Grupos Solución Grupos Solución Grupos Solución Gerenciador de Disposit Solución Compositorio	Nome Administrador Convidado DefaultAcco Novo Usuário Nome de usuário: Nome completo: Descrição:	Nome completo Administrador	Descrição Conta interna para a ac Conta interna para ace Uma conta de usuário ? X	dministraçã sso como c αerenciada erenciada
 Serviços e aplicativos 	Senha: Confirmar senha:	•••••		
	O usuário deve O usuário não p O usuário não p O A senha nunca Conta desativa	e alterar a senha no próximo pode alterar a senha a expira da	logon	
	Ajuda		<u>Criar</u> Fechar	

Obs.: Marcar a opção "A senha nunca expira".

Para adicionar o usuário Administrador no grupo de Administradores do sistema:

Acesse o Gerenciamento do computador > Usuários e Grupos Locais > Grupos > Administradores > Adicionar.



CATEGORIA REGISTRO MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO: 7

🕌 Gerenciamento do computador	
Arquivo Ação Exibir Ajuda	
🔶 🤿 🖄 📊 🔁 🛸 🛙	2 🖬
▲ Gerenciamento do computado ✓ ⅔ Ferramentas do sistema	Nome Descrição Administradores Os administradores têm acesso c
 Agendador de Tarefas Visualizador de Eventos Pastas compartilhadas Usuários e Grupos Loca Grupos O Desempenho Gerenciador de Disposit Repositório Gerenciamento de disco Serviços e aplicativos 	Propriedades de Administradores ? X Geral Administradores ? X Descrição: Os administradores têm acesso completo e irrestrito ao computador/domínio Membros: Administrador Infra SOLUTINET-Admins. do domínio Adicionar Remover As alterações na associação de grupo de um usuário só terão efeito depois que o usuário fizer logon. OK Cancelar Aplicar Ajuda



MPO.076 CLASSIFICAÇÃO: OSTENSIVO

CATEGORIAREGISTRO

PRODUÇÃO

VERSÃO

7

4.3 Não exibir o último nome de usuário

Habilite a opção de não exibir o último nome do usuário a ter realizado logon.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Configuração do Windows > Configurações de segurança > Políticas locais > Opções de segurança.

Obs.: Mantenha as configurações de acordo com a imagem.



MPO.076 CLASSIFICAÇÃO: OSTENSIVO VERSÃO

7

4.4. Diretiva de senha

As senhas devem ser fortes.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas de conta > Políticas de senha.



Obs.: Mantenha as configurações de acordo com a imagem.



VERSÃO

7

4.5. Diretiva de bloqueio de conta

Caso o usuário erre a senha por mais de 3 vezes, a conta do mesmo permanecerá bloqueada por 30 minutos, após esse período o usuário poderá tentar fazer o logon novamente.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas de conta > Políticas de bloqueio da conta.

Editor de Política de Grupo Local

Arquivo Ação Exibir Ajuda		
🔶 📄 🔝 🔂		
🗐 Política Computador Local	Política	Configuração de segura
Configuração do Computador	📓 Duração do bloqueio de conta	30 minutos
Configurações de Software	Limite de bloqueio de conta	3 tentativas de logon inv
Configurações do Windows Política de Resolução de Nome	📓 Zerar contador de bloqueios de conta após	30 minutos
Scripts (Inicialização/Encerramento)		
✓ La Configurações de segurança		
🗸 🔀 Políticas de conta		
强 Políticas de senha		
> 📑 Política de bloqueio de conta		
> 强 Políticas locais		
> 📔 Windows Defender Firewall com Seguran		
🦰 Políticas do Gerenciador de Listas de Rede		
> Políticas de chave pública		
> Políticas de restrição de software		
> Políticas de Controle de Aplicativo		
🔉 😓 Políticas de segurança IP em Computado		
🔉 🧮 Configuração Avançada de Política de Au		
🔉 🎝 QoS baseada em política		
> And Modelos Administrativos		
🗸 💰 Configuração do Usuário		
> Configurações de Software		
> Configurações do Windows		
> 📋 Modelos Administrativos		

Obs.: Mantenha as configurações de acordo com a imagem.

4.6. Logon seguro

Desative a opção para ser exigido que o usuário pressione CTRL+ALT+DEL para fazer logon.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança.



CATEGORIA REGISTRO MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO: 7

Editor de Política de Grupo Local		
Arquivo Ação Exibir Ajuda		
• 🔿 🚈 🔜 💥 🖼 🔒 😰 🖬		
Política Computador Local	Política	Configuração de segura
擾 Configuração do Computador	Logon interativo: comportamento de remoção de cartão int	Nenhuma ação
> Configurações de Software	Logon interativo: exibir informações do usuário guando a se	Não definido
Configurações do Windows	Logon interativo: exigir autenticação de controlador de do	Desabilitada
> Política de Resolução de Nome	Logon interativo: exigir o Windows Hello para Empresas ou	Desabilitada
Scripts (Inicialização/Encerramento)	Logon interativo: limite de blogueio de conta de computador	Não definido
 Configurações de segurança 	Logon interativo: limite de inatividade de computador	Não definido
> Politicas de conta	Logon interativo: não exibir o nome de usuário na entrada	Não definido
Política de auditoria	Logon interativo: não exibir quem entrou pela última vez	Habilitada
Atribuição de direitos de usuário	Logon interativo: não exigir Ctrl+Alt+Del	Desabilitada
🕞 Opcões de seguranca	Logon interativo: número de logons anteriores para armaze	10 logons
> Windows Defender Firewall com Seguran	📓 Logon interativo: pedir que o usuário altere a senha antes q	5 Dias
🧧 Políticas do Gerenciador de Listas de Rede	📓 Logon interativo: texto de mensagem para usuários tentand	
> 📔 Políticas de chave pública	B Logon interativo: título da mensagem para usuários tentand	
> Políticas de restrição de software	B Membro do domínio: assinar digitalmente dados do canal s	Habilitada
> 🧮 Políticas de Controle de Aplicativo	📓 Membro do domínio: criptografar digitalmente dados do ca	Habilitada
🔉 🜏 Políticas de segurança IP em Computado	📓 Membro do domínio: criptografar ou assinar digitalmente o	Habilitada
> 📔 Configuração Avançada de Política de Au	Membro do domínio: desativar alterações de senha de cont	Desabilitada
🔉 🔐 QoS baseada em política	📓 Membro do domínio: duração máxima de senha de conta d	30 Dias
> Modelos Administrativos	Membro do domínio: requer uma chave de sessão de alta se	Habilitada
🔏 Configuração do Usuário	📓 Objetos do sistema: exigir distinção entre maiúsculas e min	Habilitada
Configurações de Software	📓 Objetos do sistema: restringir permissões padrão de objetos	Habilitada
Configurações do Windows	📓 Segurança de rede: Configurar tipos de criptografia permitid	Não definido
Modelos Administrativos	📲 Segurança de rede: forçar logoff quando o horário de logon	Habilitada
	📲 Segurança de rede: não armazenar o valor de hash do LAN	Habilitada
	📓 Segurança de rede: nível de autenticação LAN Manager	Não definido
	📓 Segurança de Rede: permitir fallback de sessão NULA do Lo	Não definido
	📓 Segurança de Rede: permitir que o LocalSystem use a identi	Não definido
	Segurança de rede: permitir que solicitações de autenticaçã	Não definido
	Segurança de rede: requisitos de assinatura de cliente LDAP	Negociar assinatura
	📓 Segurança de Rede: Restringir NTLM: Adicionar exceções de	Não definido
	Segurança de rede: Restringir NTI M: Adicionar exceções de	Não definido

Obs.: Mantenha as configurações de acordo com a imagem.



VERSÃO

7

4.7. Serviço de Log e Auditoria

Acesse o Painel de Controle > Sistema de segurança > Ferramentas Administrativas > Serviços.

	nel de Controle → Sistema e Segurança → Ferrar	mentas Administrativas		
	Nome	Data de modificação	Тіро	Tamanho
📌 Acesso rápido		07/12/2010 05 00		2.175
📃 Área de Trabalho 🖈	Agendador de Tarefas	07/12/2019 06:09	Atalho	2 KB
Downloads 🔹	🔛 Configuração do Sistema	07/12/2019 06:09	Atalho	2 KB
	🚼 Desfragmentar e Otimizar Unidades	07/12/2019 06:09	Atalho	2 KB
🚆 Documentos 🛛 🖈	📷 Diagnóstico de Memória do Windows	07/12/2019 06:09	Atalho	2 KB
📰 Imagens 🛛 🖈	形 Editor do Registro	07/12/2019 06:09	Atalho	2 KB
👌 Músicas	📷 Fontes de Dados ODBC (64 bits)	07/12/2019 06:09	Atalho	2 KB
📕 Vídeos	🞥 Gerenciamento do computador	07/12/2019 06:09	Atalho	2 KB
	👰 Informações do sistema	07/12/2019 06:09	Atalho	2 KB
ineDrive 🍊 🗠	👧 Iniciador iSCSI	07/12/2019 06:09	Atalho	2 KB
💻 Este Computador	🔚 Limpeza de Disco	07/12/2019 06:09	Atalho	2 KB
	🔊 Monitor de Desempenho	07/12/2019 06:09	Atalho	2 KB
💣 Rede	🛞 Monitor de Recursos	07/12/2019 06:09	Atalho	2 KB
	🚌 ODBC Data Sources (32-bit)	07/12/2019 06:10	Atalho	2 KB
	둼 Política de Segurança Local	07/12/2019 06:10	Atalho	2 KB
	訡 Serviços de Componentes	07/12/2019 06:09	Atalho	2 KB
	🗟 Serviços	07/12/2019 06:09	Atalho	2 KB
	📷 Unidade de Recuperação	07/12/2019 06:09	Atalho	2 KB
	🏭 Visualizador de Eventos	07/12/2019 06:09	Atalho	2 KB
	滑 Windows Defender Firewall com Seguran	07/12/2019 06:08	Atalho	2 KB

Verifique se o serviço de log de eventos do Windows não foi parado ou desabilitado.

🔍 Serviços							-	×
Arquivo Ação Exibir Ajuda								
🔶 🧼 🔲 🖾 🙆 🚺 🕨 I								
Serviços (local) Serviços (local)								
Log de Eventos do W	indows	Nome	Descrição	Status	Tipo de Inicialização	Fazer Logon como		^
1		🖾 Ligar/Desligar	Gerencia a	Em Exe	Automático	Sistema local	_	
Parar o serviço		😪 Log de Eventos do Windows	Esse serviç	Em Exe	Automático	Serviço local		
Keiniciar o serviço	l.	Logitech Video Camera Service		Em Exe	Automático	Sistema local		
		🖏 Logon de rede	Mantém u	Em Exe	Automático	Sistema local		
Descrição:		🖏 Logon secundário	Ativa a ini		Manual	Sistema local		
/ Esse serviço gerencia e de eventos. Oferece su	eventos e logs uporte ao log de	🎑 Logs e alertas de desempenho	Os Logs e		Manual	Serviço local		
eventos, à consulta de	eventos, a	🎑 Mapeador da Descoberta de Topologia da C	Cria um		Manual	Serviço local		
assinaturas de eventos	s, ao	🎑 Mapeador de Ponto de Extremidade RPC	Resolve id	Em Exe	Automático	Serviço de rede		
arquivamento de logs	de eventos e	🌼 Mecanismo de Filtragem Básica	O Mecani	Em Exe	Automático	Serviço local		
eventos. Ele pode exib	ir eventos em	🍓 MessagingService_182eee	Serviço de		Manual (Início do Ga	Sistema local		
XML e em formato de	texto não	🏟 Microsoft App-V Client	Manages		Desativado	Sistema local		
criptografado. Interror	mper esse	Microsoft Edge Elevation Service (Microsoft	Keeps Mic		Manual	Sistema local		
serviço pode compron	neter a dade do	🍓 Microsoft Edge Update Service (edgeupdate)	Mantém o		Automático (Atraso	Sistema local		
sistema.	uaue uo	Microsoft Edge Update Service (edgeupdate	Mantém o		Manual	Sistema local		
		🍓 Microsoft Passport	Fornece o		Manual (Início do Ga	Sistema local		
		Microsoft Update Health Service	Maintains		Desativado	Sistema local		
		🍓 Modo inserido	O serviço		Manual (Início do Ga	Sistema local		
		Módulos de Criação de Chaves IKE e AuthIP	O serviço I	Em Exe	Automático (Início d	Sistema local		
		🍓 Mozilla Maintenance Service	O serviço		Manual	Sistema local		
		CCS Inventory Service	Service sta	Em Exe	Automático	Sistema local		
		OpenSSH Authentication Agent	Agent to		Desativado	Sistema local		
		🎡 Otimização de Entrega	Executa ta	Em Exe	Automático (Início c	Serviço de rede		×
Estendido Padrão /								



CATEGORIA/REGISTRO: MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configurações do Computador > Configurações do Windows > Configurações de segurança > Políticas locais > Políticas de auditoria.



Obs.: Mantenha as configurações de acordo com a imagem.

4.8. Diretivas de log

Habilitar as diretivas:

Tamanho Máximo de log (KB) e Fazer backup de log automaticamente quando completo.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Modelos Administrativos > Componentes do Windows > Serviço do Log de Eventos > Segurança.



Obs.: Mantenha as configurações de acordo com a imagem.

4.9. Proteção de tela

Habilitar bloqueio de tela com tempo de 2 minutos e proteger com senha.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Usuário > Modelos Administrativos > Painel de Controle > Personalização.



CATEGORIA REGISTRO: MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO: 7

				A 11 7 1
📱 Editor de Política de Grupo Local				
Arquivo Ação Exibir Ajuda				
🗢 🔿 🔁 🔜 🗟 🖬 🛛 🍞				
🗊 Política Computador Local	Personalização			
 E Configuração do Computador Configuraçães de Software 	Selecione um item para exibir sua	Configuração	Estado	Comentário
Configurações do Windows	descrição.	Impedir a alteração do esquema de cores	Não-configura	Não
Modelos Administrativos		Impedir a alteração de tema	Não-configura	Não
🔹 🕵 Configuração do Usuário		Impedir a alteração de estilo visual para janelas e botões	Não-configura	Não
> Configurações de Software		Habilitar a proteção de tela	Não-configura	Não
> 🧰 Configurações do Windows		Proibir seleção do tamanho da fonte do estilo visual	Não-configura	Não
 Modelos Administrativos 		Impedir a alteração de cor e aparência	Não-configura	Não
> 🚞 Área de Trabalho		Impedir a alteração de plano de fundo da área de trabalho	Não-configura	Não
> 📋 Componentes do Windows		Impedir a alteração de ícones da área de trabalho	Não-configura	Não
Menu Iniciar e Barra de Tarefas		Impedir a alteração de ponteiros do mouse	Não-configura	Não
🔻 🚞 Painel de Controle		Impedir a alteração de proteção de tela	Não-configura	Não
🚞 Adicionar ou Remover Programas		El Impedir a alteração de sons	Não-configura	Não
Impressoras		Proteger com senha a proteção de tela	Habilitado	Não
> Opções Regionais e de Idioma		Tempo limite de Proteção de Tela	Habilitado	Não
Personalização		Forçar proteção de tela específica	Habilitado	Não
Programas		E Carregar um tema específico	Nao-contigura	Não
🔛 Video		Forçar um arquivo de estilo visual específico ou forçar o esti	Não-configura	Não
Pastas Compartilhadas			2	
> Nede				
> Sistema				
-gal iouas as configurações				

Obs.: Mantenha as configurações de acordo com a imagem.



MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO

7

Determinando o tempo limite de Proteção de Tela

					-
Tempo limite de Proteção de Tela					×
📷 Tempo limite de Proteção de Tela	-	Configuração Anterior	Próxima Confi	guração	
○ Não Configurado Comentário:					~
 Habilitado 					
O Desabilitado					~
Aceito em:	Windows 2000 Service Pa	ick 1 ou posterior			^
Opções:	Ajuda:				
Tempo de espera em segundos para at Proteção de Tela Segundos: 120	var a Especif tela seji Quando definid 86.400 : proteci	ica o período de tempo ocioso a iniciada. o definida esta configuração, e o desde um mínimo de 1 segu segundos ou 24 horas. Se ele fi io de tela não será iniciada.	antes que a prot esse tempo ocios Indo até um máx or definido como	teção de o pode se imo de o zero, a	r
	Esta co	nfiguração não terá efeito nas	seguintes circun	stâncias:	
	- a co	onfiguração estiver desabilitad	a ou não estiver (definida.	
	- o te	empo de espera estiver definid	o como zero.		
	- a co desabil	onfiguração "Permitir Proteção itada.	o de Tela" estiver		
	- ner tela" ne ou Víde especifi	n a configuração "Nome do e em a caixa de diálogo Proteção eo do Painel de Controle do co icarem um programa de prote	cecutável da prot de Tela de Perso mputador cliento ção de tela válido	eção de inalização e o existente	, e ,
	L	ОК	Cancelar	Aplica	ar

4.10. Serviço NTP

Configure o relógio para sincronizar horário com o servidor da AC ntp1.acsoluti.com.br ou ntp2.acsoluti.com.br.

Acesse o caminho: Painel de Controle > Relógio e Região > Definir a hora e a data > Horário da Internet > Alterar configurações.

soluti	MANUAL DE CONFIGURAÇÃO DAS ESTAÇÕES DE TRABALHO WINDOWS	CATEGORIA/REGISTRO: MPO.076 CLASSIFICAÇÃO: OSTENSIVO	VERSÃO: 7 FASE: PRODUÇÃO
🗃 🔰 Data e Hora			1 A
Data e Hora Relógios Adicionais Horário na Internet O computador está configurado para sincronizar a 'ntp1.acsoluti.com.br'.	utomaticamente com		
Este computador está definido para sincronizar aul em um agendamento.	tomaticamente com base	de Horario na Internet de horário na Internet m.br Atualiza	r agora
8	Este computador esta definido p em um agendamento.	ara sincronizar automaticamente	com base
OK	Cancelar Aplicar	OK Car	ncelar

4.11. Antivírus

Deve possuir um antivírus de qualidade em cada estação. Caso não tenha adquirido algum antivírus, poderá utilizar o Windows Defender.

Obs.: O antivírus deve ser ativado e se manter sempre atualizado com a vacina mais atual.





MPO.076 CLASSIFICAÇÃO: OSTENSIVO

CATEGORIAREGISTRO

PRODUÇÃO

VERSÃO

7

4.12. Firewall

Verifique se o Firewall do Windows está habilitado.

Acesse o Painel de Controle > Sistemas e segurança > Firewall do Windows > Ativar e Desativar o Firewall do Windows.

2	Personalizar Configurações 🐡 🗕 🗖
€ ⊕ •	🕆 🚔 « Firewall do Windows » Personalizar Configurações v 🖒 Pesquisar Painel de Controle
	Personalizar as configurações para cada tipo de rede
	Vocé pode modificar as configurações do firewall para cada tipo de rede usada.
	Configurações de redes privadas
	Ativar o Firewall do Windows
	Bloquear todas as conexões de entrada, inclusive as que estejam na lista de aplicativos permitidos
	 Avisar-me quando o Firewall do Windows bloquear um aplicativo novo
	O Desativar o Firewall do Windows (não recomendado)
	Configurações de redes públicas
	Ativar o Firewall do Windows
	Bloquear todas as conexões de entrada, inclusive as que estejam na lista de aplicativos permitidos
	 Avisar-me quando o Firewall do Windows bloquear um aplicativo novo
	Desativar o Firewall do Windows (não recomendado)
	OK Cancelar

4.13. Atualizações do Windows

Certifique-se que o Windows esteja sempre atualizado!

4.14. Software autêntico

A licença do Windows instalado deve ser genuína, não deve ser utilizado nenhum software pirata.

Acesse o Painel de Controle > Sistema e segurança > Sistema > Alterar chave do produto (Product Key) ou atualizar a edição do Windows.



CATEGORIA/REGISTRO: MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO

7



4.15. Acesso remoto

O acesso remoto às estações de trabalho deve ser feito somente para suporte técnico se necessário, definindo uma senha e limitando o acesso a usuários que não a possuem.

Exemplo Anydesk:





CATEGORIA/REGISTRO MPO.076 CLASSIFICAÇÃO: OSTENSIVO

PRODUÇÃO

VERSÃO: 7

Exemplo Teamviewer:

Geral	Opções de acesso a este computa	dor
Segurança	Senha pessoal (para acesso não superv	risionado)
Controle Remoto	Senha	•••••
Reunião	Confirmar senha	
Computadores & contatos	💡 📃 Conceder acesso fácil	Configurar
Audioconferência	Senha aleatória (para acesso espontân	eo)
Vídeo	Grau de segurança da senha	Desabilitado (sem senha aleatória) 🗸 🗸
Convite personalizado	Regras de conexão a este computador	
Avançado	Iniciar sessão no Windows Não	permitido 🗸 🗸
	Lista de bloqueio e permissões	Configurar



VERSÃO: 7

HISTÓRICO DE REVISÕES

VERSÃO	DATA	DESCRIÇÃO DA REVISÃO	RESPONSÁVEL	ÁREA/DPTO
1	19/05/2015	- Versão inicial;	Jessé	Suporte
2	20/09/2016	- Alteração nas informações;	Marcos Marques Pícolo Júnior	Suporte AR's
3	14/08/2019	- Alteração de conteúdo no documento;	Marcos Marques Pícolo Júnior	Suporte AR's
4	14/08/2019	- Alteração de Layout;	Marcos Marques Pícolo Júnior	Suporte AR's
5	11/03/2021	- Atualização total de conteúdo do DOC;	Wincius Leal	Infraestrutura
6	26/05/2022	- Alteração de conteúdo no documento;	Igor Ferreira de Jesus Pereira	Infraestrutura
7	31/05/2022	- Adição de configuração BitLocker;	Igor Ferreira de Jesus Pereira	Infraestrutura

REVISOR(ES): IGOR FERREIRA DE JESUS PEREIRA	DATA: 31/05/2022	
APROVADOR(ES):	DATA:	
MARCOS MARQUES PICOLO JUNIOR	31/05/2022	