 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	3
5.	RESPONSABILIDADES	3
6.	REGRAS BÁSICAS	4
7.	CONTROLE DE REGISTROS.....	34
8.	ANEXOS.....	34
9.	REGISTRO DE ALTERAÇÕES.....	34

1. OBJETIVO

Garantir a proteção dos servidores em redes e a proteção da infraestrutura do **Grupo CPFL Energia**.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas com participação direta do **Grupo CPFL Energia** e sistemas considerados críticos e para SOX.


2.2. Área

Todas as áreas do **Grupo CPFL Energia**.

3. DEFINIÇÕES


- **CONFIDENCIALIDADE:** É a garantia de que a informação é acessada somente por usuários com o devido direito. Está diretamente vinculada a proteção da privacidade dos usuários e suas informações.
- **INTEGRIDADE:** É a garantia de que a informação no momento que é acessada está em sua completeza, totalidade, plenitude, sem qualquer alteração em seu conteúdo, quando foi armazenada.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	1 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **DISPONIBILIDADE:** É a garantia de que a informação está disponível para o usuário (que tem tal direito de acesso) e para o sistema de informação no momento que o usuário necessita consumi-la.
- **SEGURANÇA DA INFORMAÇÃO:** Proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no **Grupo CPFL Energia**.
- **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** Qualquer evento que possa comprometer a Segurança da Informação do **Grupo CPFL Energia**.
- **RISCOS:** Combinação da probabilidade de um evento e suas possíveis consequências.
- **HARDENING:** É uma técnica de blindagem de sistemas que envolve um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas com foco na infraestrutura. Seu objetivo principal é tornar o sistema preparado para enfrentar tentativas de ataque.
- **ACESSO:** É o nível de permissão onde se pode realizar uma operação sobre algum recurso computacional.
- **AUTORIZAÇÃO:** Trata-se do que o usuário autenticado pode fazer.
- **CONTROLE:** Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
- **DISPOSITIVO:** Equipamento e/ou acessório utilizado para acessar, transmitir, compartilhar, visualizar, editar, fazendo-se uso do meio eletrônico para tal.
- **SERVIDOR:** São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**.
- **REDE CORPORATIVA:** São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**.
- **USUÁRIO:** Qualquer pessoa (colaboradores, visitantes, estagiários, empregados, temporários, prestadores de serviços etc.) que possua ou não ligação com o **Grupo CPFL Energia** e que necessite de Credenciais de Acesso para acessar um sistema ou recurso computacional da organização.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	2 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **WINDOWS SERVER:** O Windows Server é uma plataforma para compilar uma infraestrutura de aplicativos, redes e serviços Web conectados, do grupo de trabalho ao data center da Microsoft®.

4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- Política de Segurança da Informação do **Grupo CPFL Energia**;
- Norma de Classificação da Informação do **Grupo CPFL Energia**;
- Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia**;

5. RESPONSABILIDADES


• Diretoria de Tecnologia da Informação

- ✓ Aplicar as regras de instalação e configuração de sistemas conforme descrito neste documento;
- ✓ Propor mecanismos e processos para restringir o acesso e monitorar o cumprimento das regras contidas neste documento;
- ✓ Implementar os controles tecnológicos e processos para manter controle e monitoração de toda a rede do **Grupo CPFL Energia**.

• Departamento de Segurança da Informação

- ✓ Definição de regras de instalação e configuração de sistemas;
- ✓ Auditoria da aplicação das regras de instalação e configuração de sistemas;
- ✓ Prover e manter o sistema de guarda, criação e alteração das credenciais dos usuários;
- ✓ Bloquear ou desabilitar as credenciais após tentativas de troca de senhas sem sucesso, notificando o usuário e o setor responsável pelo Tratamento de Incidentes de Segurança da Informação;
- ✓ Reportar as irregularidades/incidentes detectados;
- ✓ Liberar o acesso de acordo com as normas previstas;
- ✓ Implementar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a Internet, dispositivos móveis ou wireless e outros componentes da rede - a informação gerada por esses sistemas poderá ser utilizada para identificar usuários e respectivos acessos efetuados, bem como o material que foi manipulado;
- ✓ Instalar sistemas de proteção, prevenção e detecção, para garantir a segurança das informações e dos perímetros de acesso.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	3 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6. REGRAS BÁSICAS

O hardening consiste na realização de alguns ajustes finos para o fortalecimento da segurança de um sistema.

Muitos administradores sem experiência em segurança preparam seus servidores com uma instalação básica e depois que suas aplicações estão disponíveis nenhum procedimento é feito para manter a integridade do sistema.


Em um sistema GNU/Linux é possível atingir um alto nível de segurança implementando configurações que permitam o aperfeiçoamento da segurança aplicada ao sistema.

Quando se deseja aplicar a técnica de hardening há três grandezas que devem ser consideradas: segurança, risco e flexibilidade.

O administrador de redes deve analisar muito bem essas grandezas e encontrar um estado de harmonia entre elas, levando o sistema a uma alta produtividade e segurança, pois quanto maior a segurança menor o risco e a flexibilidade. É importante ressaltar que as técnicas aqui apresentadas podem não ser adequadas para todas as situações.

Por isso, antes de implantar efetivamente as técnicas de hardening, é fundamental que haja um estudo completo do cenário e serviços em questão.

Inicialmente recomenda-se sempre instalar versões atuais dos sistemas operacionais, que contenham correções e patches de segurança, pois pode ser problemático utilizar uma versão antiga sem atualizações, deixando os sistemas temporariamente vulneráveis no caso da existência de pacotes com falhas.

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6.1 Aplicação de Patches


• Windows update

Descrição:
Este controle define se o Windows irá receber atualizações de segurança do Windows Update ou WSUS. Para todos os perfis, o estado recomendado para essa configuração está habilitado: 3 - Fazer o download automático e notificar para instalar.
Justificativa:
Estabelecer meios automatizados para implantar e aplicar as atualizações do sistema irá ajudar a garantir o sistema sempre tem as mais recentes atualizações críticas do sistema operacional e service packs instalados.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates

• Método de atualização

Descrição:
Os sistemas deveram receber download de atualizações a partir de servidores WSUS localizados dentro da rede corporativa.
Justificativa:
A partir de servidores WSUS a gerência de aplicação de patches é melhor controlada e diminui o tempo de download a partir da Internet.
Configuração/Correção:
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Specify intranet Microsoft update service location

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	5 de 34


 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6.2 Política de Auditoria

• Auditoria de eventos de login e conta

Descrição:
Auditoria de eventos de logon de conta criará uma entrada no log de eventos de segurança quando um logon local interativo, logon de rede, processo em lote, ou de logon do serviço ocorre. Logons conta falha pode mostrar uma tendência para ataques de senha; eventos de logon bem-sucedidas são importantes para identificar qual usuário estava conectado ao computador em um determinado momento. "Conta Logon" eventos são gerados a partir da utilização de contas de domínio, o que difere de "eventos de logon", que são gerados pelo uso de contas locais. Para todos os perfis, o estado recomendado para essa configuração é Sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account logon events

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	6 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


• Auditoria de gerenciamento de contas

Descrição:
Esta configuração pode ser usada para criar uma entrada no log de eventos de segurança quando as atividades de gerenciamento de contas ocorrerem. Exemplos de atividades de gerenciamento de contas incluem criar ou excluir um usuário ou grupo, desativar ou ativar um usuário, e renomeando um usuário ou grupo. Para todos os perfis, o estado recomendado para essa configuração é sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account management

• Auditoria de gerenciamento de contas

Descrição:
Auditoria de eventos de logon de conta criará uma entrada no log de eventos de segurança quando um logon local interativo, logon de rede, processo em lote, ou de logon do serviço ocorre. Logons conta falha pode mostrar uma tendência para ataques de senha; eventos de logon bem-sucedidas são importantes para identificar qual usuário estava conectado ao computador em um determinado momento. "Conta Logon" eventos são gerados a partir da utilização de contas de domínio, o que difere de "eventos de logon", que são gerados pelo uso de contas locais. Para todos os perfis, o estado recomendado para essa configuração é Sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account logon events

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	7 de 34


 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

• Auditoria de acesso a objeto

Descrição:
Este controle fornece recursos de auditoria no nível do objeto. Esta é mais comumente usada para objetos do sistema de arquivos. Habilitando este controle não tem efeito a menos que um determinado objeto SACL contém uma ACE com sinalizadores de auditoria. Para todos os perfis, o estado recomendado para essa configuração é Sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit object access


• Mudança de política de auditoria

Descrição:
Este controle define se a auditoria para cada evento de alteração de diretiva é ativada. Alterações de direitos de usuário, diretivas de auditoria ou diretivas de confiança irá produzir eventos no log de eventos de segurança se este for ativado. Para todos os perfis, o estado recomendado para essa configuração é Sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit policy change

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


• Auditoria de uso de privilégio

Descrição:
<p>Uso de privilégios Auditoria permite a auditoria para qualquer operação que exige uma concessão de privilégio específico. Se isso for ativada, os eventos serão gerados no log de eventos de segurança quando um usuário ou tentativas de processo para ignorar a verificação completa, os programas de depuração, crie um objeto token, substituir um token no nível de processo, ou gerar auditorias de segurança.</p> <p>Se as credenciais de segurança são usadas para fazer backup ou restaurar arquivos ou diretórios, usando o "backup ou restauração" direito do usuário, e se essa configuração for definida, os eventos de segurança serão gerados.</p> <p>Uso de privilégios é usado por todas as contas de usuário em uma base regular. Se os eventos de sucesso e fracasso são auditados, haverá muitos eventos no log de eventos refletindo tal uso. Para todos os perfis, o estado recomendado para essa configuração é falha.</p>
Justificativa:
<p>Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p> <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit privilege use</p>

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

• Auditoria de eventos de sistema

Descrição:
A auditoria dos eventos de sistema é muito importante. Os eventos do sistema incluem iniciar ou desligar o computador, logs de eventos completos, e outros itens que têm impacto sobre o computador, mas não pode ser diretamente relacionado à segurança. Os eventos do sistema são particularmente úteis quando da revisão de um sistema durante ou após o incidente. Para todos os perfis, o estado recomendado para essa configuração é Sucesso e Falha.
Justificativa:
Recomenda-se que subcategorias de auditoria ser aproveitado em vez de políticas de auditoria legados. Um sistema não é considerado menos seguro se esta política é definida para o sucesso e / ou falha.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit system events

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6.3 Privilégios de usuários


• Acesso ao computador via rede

Descrição:
<p>Este controle define se os outros usuários da rede podem se conectar a este computador. Recomenda-se que esta configuração ser configurado como descrito abaixo:</p> <ul style="list-style-type: none"> ✓ Para o servidor membro da empresa e do perfil do servidor SSLF Membro (s), o valor recomendado é de administradores, usuários autenticados; ✓ Para o domínio da empresa e controlador de domínio SSLF Controlador de perfil (s), o valor recomendado é de administradores, usuários autenticados, CONTROLADORES DE DOMÍNIO DA EMPRESA.
Justificativa:
Configurando o sistema como recomendado assegurará apenas as contas autorizadas podem acessar o computador local a partir da rede.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network

• Ajusta quotas de memória para um processo

Descrição:
<p>Este controle permite ao usuário modificar a quantidade máxima de memória disponível para um processo. Recomenda-se que esta configuração ser configurado como descrito abaixo:</p> <ul style="list-style-type: none"> ✓ Para o servidor membro SSLF e Domínio SSLF Controlador de perfil (s), o valor recomendado é de Administradores, LOCAL SERVICE, NETWORK SERVICE; ✓ Para o servidor membro da empresa e do domínio da empresa perfil Controller (s), o valor recomendado é Administradores;
Justificativa:
Limitar a concessão deste direito vai ajudar a minimizar a chance de um usuário mal-intencionada ou o desempenho do sistema sem querer impactante, que pode resultar em negação de serviço.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	11 de 34

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Configuração/Correção:

Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process

• **Backup de arquivos e diretórios**

Descrição:

Este controle define se um usuário tem permissão para fazer backup de arquivos e diretórios no sistema. Recomenda-se que esta configuração ser configurado como descrito abaixo:

- ✓ Para o servidor membro SSLF e Domínio SSLF perfil Controller (s), o valor recomendado é administradores e operadores de Backup;
- ✓ Para o servidor membro da empresa e do domínio da empresa perfil Controller (s), o valor recomendado é administradores e operadores de Backup;


Justificativa:

Configurando o sistema como recomendado irá reduzir a probabilidade de a divulgação não autorizada de dados históricos sensíveis. Além disso, restringindo a concessão deste direito irá limitar a exposição ao usuário de forma maliciosa ou acidentalmente sobrescrever os dados que é mais recente.

Configuração/Correção:

Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories


 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

• **Negar acesso ao computador a partir da rede**

Descrição:
Este controle define que as contas não estão autorizadas a se conectar ao computador local a partir da rede. Para todos os perfis, o estado recomendado para esta configuração é Guests.
Justificativa:
Configurando o sistema como recomendado assegurará apenas as contas autorizadas podem acessar o computador local a partir da rede.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network

• **Forçar desligamento de computador remotamente**

Descrição:
Este controle define se uma conta de usuário tem permissão para desligar remotamente um computador. Recomenda-se que esta configuração ser configurado como descrito abaixo:
<ul style="list-style-type: none"> ✓ Para o servidor membro SSLF e Domínio SSLF perfil Controller (s), o valor recomendado é de administradores; ✓ Para o servidor membro da empresa e do domínio da empresa perfil Controller (s), o valor recomendado é de administradores;
Justificativa:
Configurando o sistema como recomendado vai limitar o potencial de negação de serviço ataque (DoS).
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


• **Aumentar prioridade de agendamento**

Descrição:
Este controle define se um usuário tem permissão para alterar a classe de prioridade base para um processo. Recomenda-se que esta configuração ser configurado como descrito abaixo: <ul style="list-style-type: none"> ✓ Para o servidor membro SSLF e Domínio SSLF perfil Controller (s), o valor recomendado é de administradores; ✓ Para o servidor membro da empresa e do domínio da empresa perfil Controller (s), o valor recomendado é de administradores;
Justificativa:
Restringir quais usuários podem aumentar a prioridades de agendamento irá reduzir a probabilidade de o desempenho do sistema tornando-se bastante degradado devido a alterações não intencionais ou mal-intencionado a prioridade do processo.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima: <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority</p>

• **Negar acesso ao computador a partir da rede**

Descrição:
Este controle define se uma conta de usuário é ***permitida carregar dinamicamente um novo driver de dispositivo no sistema. Para todos os perfis, o estado recomendado para esta configuração é de administradores.
Justificativa:
Drivers operar em um nível de privilégio muito grande. Restringir o que os diretores podem carregar drivers de dispositivo vai ajudar a reduzir a capacidade de um usuário mal-intencionado para impactar negativamente a confidencialidade, integridade e disponibilidade das informações no sistema.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	14 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers

• **Aumentar prioridade de agendamento**

Descrição:
<p>Este controle define se um usuário tem permissão para alterar as opções de auditoria para arquivos e diretórios e limpar o log de Segurança. Recomenda-se que esta configuração ser configurado como descrito abaixo:</p> <ul style="list-style-type: none"> ✓ Para o servidor membro Enterprise, SSLF servidor membro e SSLF Domain perfil Controller (s), o valor recomendado é de administradores, fnis-br\sva-secaudit; ✓ Para o perfil Domain Controller Enterprise (s), o valor recomendado é de administradores, fnis-br\sva-secaudit;
Justificativa:
<p>Impondo e restringir o acesso a esse controle vai limitar o potencial de um usuário para apagar evidência de atividade não autorizada.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p>
<p>Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log</p>


 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

• **Modificar valores do ambiente de firmware**

Descrição:
<p>Este controle define se um usuário tem permissão para configurar as variáveis de todo o sistema de ambiente que afetam a configuração de hardware. Recomenda-se que esta configuração ser configurado como descrito abaixo:</p> <ul style="list-style-type: none"> ✓ Para o servidor membro Enterprise, SSLF servidor membro e SSLF Domain perfil Controller (s), o valor recomendado é de administradores; ✓ Para o perfil Domain Controller Enterprise (s), o valor recomendado é de administradores;
Justificativa:
<p>Configurando o sistema como recomendado irá limitar o potencial de um hardware corrupção de dados, falha ou negação de serviço causado por usuários não autorizados.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p> <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values</p>

• **Perfil de desempenho do sistema**


Descrição:
<p>Este controle define se um usuário tem permissão de usar ferramentas para visualizar o desempenho dos processos do sistema. Para todos os perfis, o estado recomendado para esta configuração é de administradores.</p>
Justificativa:
<p>A configuração do sistema, como recomendado irá limitar o potencial de utilizadores não autorizados para ganhar informação adicional para executar um ataque sobre o sistema.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p>

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance

• **Restauração de arquivos e diretórios**

Descrição:
<p>Este controle define se um usuário tem permissão para ignorar arquivo, diretório, Registro e outras permissões de objetos persistentes ao restaurar dados de backup. Recomenda-se que esta configuração ser configurado como descrito abaixo:</p> <ul style="list-style-type: none"> ✓ Para o servidor membro SSLF e Domínio SSLF perfil Controller (s), o valor recomendado é de administradores, Operadores de Backup; ✓ Para o servidor membro da empresa e perfil da empresa Domain Controller (s), o valor recomendado é de Administradores, Operadores de Backup;
Justificativa:
<p>Conta que possuem esse direito de usuário pode ter acesso a dados sensíveis, corrompendo e sobrescrever a informação, bem como realizar negação de serviço (DoS) ataques contra o sistema.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p> <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories</p>


 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

• **Desligamento de sistema**

Descrição:
Este controle define se um usuário tem permissão para usar desligar o sistema operacional quando conectado localmente no computador. Para todos os perfis, o estado recomendado para esta configuração é de administradores.
Justificativa:
Configurando o sistema como recomendado irá limitar o potencial para que usuários não autorizados para desligar o sistema.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system

• **Apropriar-se de arquivos e objetos**

Descrição:
Este controle define se um usuário está autorizado a se apropriar de arquivos, pastas, chaves de registro, processos ou threads. Para todos os perfis, o estado recomendado para esta configuração é de administradores.
Justificativa:
Contas com esse direito de usuário pode apropriar-se de qualquer recurso, apesar de uma lista de controle de acesso que poderiam proteger o recurso. Como tal, a confidencialidade, integridade e disponibilidade de todos os dados em um sistema que tem esse direito de forma insegura configurado está em risco.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects


 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6.4 Opções de Segurança

- **Contas:** limitar o uso de senhas em branco para uso somente em logins de console

Descrição:
Windows divide logons de computador em dois tipos principais: logons de console ou locais e logins remotos. Em um logon no console, o usuário faz logon fisicamente o dispositivo com o teclado conectado. Logons remotos são realizadas através da rede usando vários protocolos, como RPC, telnet, FTP e desktop remoto. Quando essa configuração estiver ativada, o computador se recusa logons remotos se o usuário tentar usar uma senha em branco, mesmo que a senha em branco é válida para essa conta. Essa configuração deve ser ativada mesmo que as senhas nunca devem ser deixadas em branco. Para todos os perfis, o estado recomendado para essa configuração estiver ativado.
Justificativa:
Recusa pedido de autenticação remota para conta com senhas em branco ajuda a garantir que somente usuários autorizados possam acessar o sistema.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	19 de 34

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


- **Contas: renomear a conta de administrador**

Descrição:
<p>Este controle recomenda escolher um nome para a conta de administrador incorporada local que é diferente do padrão. Muitas vezes a desativação da conta do administrador não é prático. No entanto, basta saber o nome de uma conta em uma máquina pode ser uma informação valiosa para um atacante. Na tentativa de esconder a conta, as melhores práticas recomendam conta renomear o a algo único para a sua implementação.</p> <p>Se a conta for renomeada, identificador de segurança anônimo (SID) / conversão de nomes também deve ser desativado. Isso impede que um invasor localizar a conta renomeada por seu SID. Para todos os perfis, o estado recomendado para esta configuração é qualquer valor que seja de conhecimento apenas do departamento de Tecnologia.</p>
Justificativa:
Aplicando esta recomendação torná-la mais difícil para usuários não autorizados de adivinhar e ter acesso à conta de administrador e, finalmente, o sistema.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account

- **Contas: renomear a conta guest**

Descrição:
<p>Este controle recomenda a escolha de um nome para a conta suposição incorporado no local que é diferente do padrão. Similar à conta de administrador, a conta <u>Convidado</u> deve ser renomeado, mesmo se ele está desativado. O sistema operacional coloca salvaguardas adicionais na conta do cliente, e é menos de um alvo do que a conta de administrador, mas ainda merece uma atenção significativa mandado de mudar o nome da conta. Para todos os perfis, o estado recomendado para esta configuração é de que seja de conhecimento apenas do departamento de Tecnologia.</p>
Justificativa:
Aplicando esta recomendação torná-la mais difícil para usuários não autorizados de adivinhar e ter acesso à conta de convidado e, finalmente, o sistema.
Configuração/Correção:

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	20 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:


Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account

- **Auditoria: desligar o sistema imediatamente no caso de indisponibilidade dos logs de segurança**

Descrição:
Esta configuração faz o sistema desligar, se for incapaz de registrar um evento de segurança no log de eventos de segurança. Para todos os perfis, o estado recomendado para essa configuração é Desativado.
Justificativa:
O risco de causar danos irreparáveis ao sistema operacional, aplicações ou dados, juntamente com a indisponibilidade dos serviços prestados pelo sistema devido a ser imediatamente desligado normalmente superam em muito o risco de ser incapaz de registrar um evento de segurança.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits

- **Dispositivos: permissão para formatar e ejetar mídias removíveis**

Descrição:
Esta configuração controla o tipo de utilizadores que têm autoridade para remover a mídia NTFS formatado a partir do computador. As opções disponíveis (listados do mais para a menos restritiva) são Administradores, Administradores e Usuários avançados ou Administradores e usuários interativos. Para todos os perfis, o estado recomendado para esta configuração é de administradores.
Justificativa:
Limitar os usuários que podem remover a mídia NTFS a partir do sistema reduz a probabilidade de um usuário mal-intencionado montar o. Remover um disco do computador local para acessá-lo em outro, fora do contexto das restrições de segurança, como DACLS.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o


 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

valor prescrito acima:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media

- **Dispositivos: impedir que usuários instalem drivers de impressoras**

Descrição:
Os usuários geralmente precisam da capacidade de instalar e configurar suas próprias impressoras. No entanto, a instalação do driver carrega código diretamente no espaço privilegiado do kernel do sistema operacional. O usuário mal-intencionado pode optar por instalar um driver de impressão maliciosos para ganhar controle sobre o sistema. Se os usuários devem ter o direito de instalar drivers de impressora, solicite que o driver ser assinado digitalmente antes que possa ser instalado. Cuidado com a sintaxe para esta opção: Enabled significa que os usuários não poderão instalar drivers de impressora e pode impedir a configuração adequada de impressoras; Desativado permite ao usuário gerenciar totalmente suas próprias impressoras. Para todos os perfis, o estado recomendado para essa configuração estiver ativado.
Justificativa:
Impedir que os usuários instalem drivers de impressora reduz a probabilidade de um usuário afetar a estabilidade ea segurança do Windows.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


- Membro de Domínio: duração máxima de senha de contas**

Descrição:
Este controle define quantos dias membro do domínio pode usar a mesma senha antes que ela expire. Para todos os perfis, o estado recomendada para essa configuração é de 30 dia(s).
Justificativa:
Impor prazos de validade razoavelmente curtos aumentará a eficácia dos sistemas de autenticação baseados em senha, reduzindo a oportunidade de um atacante para alavancar uma credencial conhecido.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age

- Logon Interativo: não exibir o último nome de usuário**

Descrição:
Qualquer pessoa que tentar entrar em um computador pode ver o nome do último usuário que fez logon válido para esse sistema. Isso não impede exibir o usuário conectado no momento ao desbloquear uma estação de trabalho. Esta informação pode parecer trivial, mas ajuda um atacante amarrar uma estação de trabalho para um determinado indivíduo, ou pode ajudar um atacante para obter acesso de um dispositivo móvel furtado. Educar os usuários antes de ativar esta configuração em um ambiente de domínio. Alguns usuários podem não saber o seu logon, especialmente quando se diferente do endereço de e-mail ou outras contas. Cuidado com a sintaxe para esta opção: Enabled significa que o usuário deve digitar seu ID de usuário a cada logon; Deficientes significa que o último acesso do usuário aparece na caixa de diálogo de login. Para todos os perfis, o estado recomendada para essa configuração estiver ativada.
Justificativa:
Impondo e restringir este controle vai limitar o potencial de usuários não autorizados a coletar os nomes de conta e obter informações adicionais para realizar um ataque no sistema.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	23 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name


- **Logon Interativo: não exigir uso do CTRL+ALT+DEL**

Descrição:
<p>Este controle define se um usuário deve pressionar CTRL + ALT + DEL antes de fazer logon. O sistema operacional Windows trata o CTRL + ALT + DEL sequência diferente de qualquer outro. Construção do sistema operacional impede qualquer aplicação de interceptar e responder quando essas teclas são pressionadas. Quando você digita CTRL + ALT + DEL, você está garantido que o processo de autenticação operacional sistema irá processar o pedido.</p> <p>Quando o console não exigir CTRL + ALT + DEL para fazer logon, os usuários não verão a caixa de diálogo "Pressione CTRL + ALT + DEL para fazer logon." Pelo contrário, a estação de trabalho simplesmente apresenta o diálogo de logon padrão. Cuidado com a sintaxe para esta opção: Desativado significa que o usuário deve pressionar CTRL + ALT + DEL antes de cada sessão não-smartcard; habilitado apresentará o diálogo de logon sem a necessidade de CTRL + ALT + DEL. Para todos os perfis, o estado recomendado para essa configuração é Desativado.</p>
Justificativa:
<p>Com a exigência CTRL + ALT + DEL levantado, o usuário poderia realmente estar digitando sua senha em um aplicativo de trojan, ao invés do processo de autenticação do sistema operacional. Lembre-se, a aplicação trojan não seria capaz de responder se o usuário pressionou CTRL + ALT + DEL.</p>
Configuração/Correção:
<p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p> <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL</p>

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **Logon Interativo: número de logons prévios em cache (caso do controlador de domínio não estar disponível)**


<p>Descrição:</p> <p>Este controle define se um usuário pode fazer logon em um domínio do Windows usando informações de conta armazenadas em cache. Quando uma estação de trabalho pertence a um domínio, os usuários podem fazer logon a ele usando credenciais de domínio. As credenciais de domínio podem ser armazenadas em cache no Gerenciador de estação de trabalho local de Contas de Segurança (SAM). No próximo logon, se nenhum controlador de domínio esteja disponível, o usuário ainda pode fazer logon localmente por meio da autenticação com as informações armazenadas em cache.</p> <p>Ao fazer logon usando credenciais em cache, algumas propriedades da conta não serão aplicadas, uma vez que o controlador de domínio mantém a responsabilidade pela aplicação da política de conta. O banco de dados SAM local não "possuir" a conta, senhas de contas de modo em cache não expiram, e contas de domínio não podem ser bloqueadas quando o domínio não está disponível.</p> <p>Ao estabelecer a política corporativa para contas em cache, considere o usuário remoto. Eles comumente logon com credenciais em cache a partir de um laptop. Para acessar os recursos corporativos, o usuário estabelece uma conexão Virtual Private Network (VPN) à rede da empresa. Desde logon ocorre antes o domínio está disponível, a VPN ainda não foi estabelecida, o usuário nunca será solicitado a alterar a senha da conta armazenadas em cache.</p> <p>Esta configuração afeta somente estações de trabalho associados a um domínio, e só afeta os logons interativos com contas de domínio. A estação de trabalho não irá armazenar em cache não-interativo informações de logon. Altere esta definição para zero para desabilitar o cache de contas de domínio no banco de dados SAM local. Para todos os perfis, o estado recomendado para essa configuração é 0 logons.</p>
<p>Justificativa:</p> <p>Definir o número de logon em cache para o nível adequado para o perfil do sistema irá remover uma avenida para um atacante para comprometer ainda mais o ambiente, decorrentes credenciais do cache enquanto permite logons do domínio deve tornar-se indisponível.</p>
<p>Configuração/Correção:</p> <p>Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:</p> <p>Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain</p>

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

controller is not available)

- **Logon Interativo: solicitar ao usuário a troca de senha antes da expiração**

Descrição:
Este controle define quantos dias de antecedência um usuário é notificado antes de sua senha deve ser alterada. Se a senha de um usuário estiver perto de sua data de validade, o processo de logon avisa o usuário e pergunta se eles gostariam de alterar a senha. Depois que a senha tenha expirado, o usuário será obrigado a alterar a senha para completar o logon. Esta configuração regula a janela de conveniência entre o momento em que o sistema oferece ao utilizador alterar a senha, e do momento em que são necessários para alterar a senha. Para todos os perfis, o estado recomendado para essa configuração é de (5) dias.
Justificativa:
Aplicar esse controle é importante para notificar os usuários antes da expiração de sua senha evitando que inadvertidamente não completem o logon do computador quando sua senha expirar
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


- **Servidor de Rede Microsoft: Desconectar Clientes quando Horário de Logon Terminar**

Descrição:
Este controle define se desconectar de uma sessão quando o horário de logon dos usuários válidos expirar. Para todos os perfis, o estado recomendado para essa configuração estiver ativada.
Justificativa:
A menos que essa configuração é habilitada, os benefícios do horário de logon imponentes não serão realizados.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire

- **Acesso de Rede: Não Permitir o armazenamento de Credenciais ou Passaportes .NET para Autenticação de Rede**

Descrição:
Este controle define se os nomes de utilizador e senhas podem salvar credenciais de senha para uso posterior quando a autenticação de domínio é atingida. Para todos os perfis, o estado recomendado para essa configuração estiver ativada.
Justificativa:
A confidencialidade das credenciais armazenadas e, portanto, os sistemas de acesso às credenciais estão em risco se o sistema está comprometido, ou o disco rígido é descartado inseguramente.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of credentials or .NET Passports for network authentication

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	27 de 34

 Confidencialida	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


- **Acesso de Rede: Permitir que todas as Permissões possam ser Aplicadas a Usuários Anônimos**

Descrição:
Este controle define o que são atribuídas permissões adicionais para conexões anônimas ao computador. Para todos os perfis, o estado recomendado para essa configuração é Desativado.
Justificativa:
A desativação dessa configuração é importante que os usuários não autorizados possam listar anonimamente nomes de contas e recursos compartilhados, e usar as informações para tentar adivinhar senhas, executar ataques de engenharia social, ou lançar ataques DoS.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users

- **Acesso de Rede: Compartilhamento e Modelo de Segurança para Contas Locais**

Descrição:
Este controle define como logons de rede que utilizam contas locais são autenticados. Para todos os perfis, o estado recomendado para esta configuração é Clássico - os usuários locais são autenticados como eles próprios.
Justificativa:
A configuração recomendada permite o controle preciso sobre o acesso aos recursos, incluindo a capacidade de atribuir diferentes tipos de acesso para usuários diferentes para o mesmo recurso.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	28 de 34

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server


- Segurança de Rede: Requisito de Assinatura LDAP do Cliente**

Descrição:
Este controle define o nível de assinatura de dados que é solicitado em nome dos clientes que emitem solicitações LDAP BIND. Para todos os perfis, o estado recomendado para essa configuração é Negociar assinatura.
Justificativa:
Assinando solicitações do cliente LDAP irá ajudar a garantir que a integridade da consulta é preservada. Na ausência de uma consulta assinada, um atacante de rede ativa pode alterar a consulta LDAP em rota para o servidor.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements

- Console de Restauração: Permitir Logon Administrativo Automático**

Descrição:
Este controle define se a conta de administrador é automaticamente conectada ao console de recuperação. Para todos os perfis, o estado recomendado para essa configuração é Desativado.
Justificativa:
Se o logon administrativo automático estiver ativado, um usuário malicioso poderia desligar a alimentação do servidor para desligá-lo, reiniciá-lo, selecionar Console de recuperação no menu Reiniciar e assumir o controle total do servidor.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Recovery console: Allow automatic administrative logon

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18884	Instrução	1.0	Emerson Cardoso	17/08/2021	29 de 34


 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **Desligamento: Permitir que o Sistema seja Desligado sem Logon**

Descrição:
Este controle define se um computador pode ser desligado quando um usuário não está conectado. Para todos os perfis, o estado recomendado para essa configuração é Desativado.
Justificativa:
A desativação dessa configuração é importante para os sistemas de clientes de alta segurança e para os servidores como uma pessoa mal-intencionada pode desligar o sistema de forma não autorizada.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on

- **Desligamento: Limpar Arquivo de Paginação de Memória Virtual**

Descrição:
Este controle define se o arquivo de paginação de memória virtual é apagado quando o sistema é desligado. Para todos os perfis, o estado recomendado para essa configuração é Desativado.
Justificativa:
Limpar o arquivo de paginação de memória virtual no desligamento irá causar atrasos significativos na reinicialização do sistema. Estes atrasos são considerados um risco maior à disponibilidade do serviço do que o benefício percebido de limpar o conteúdo do arquivo de paginação.
Configuração/Correção:
Para estabelecer a configuração recomendada via GPO, configure o seguinte para o valor prescrito acima:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Clear virtual memory pagefile

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **Desativação do Protocolo SSL (todas as versões)**


Descrição:
O protocolo seguro SSL possui uma vulnerabilidade conhecida como PODDLE.
Justificativa:
A exploração desta vulnerabilidade neste protocolo permite que um atacante visualiza as informações seguras sendo trafegadas.
Configuração/Correção:
Desativar o protocolo de segurança SSL (todas as versões)

- **Desativar o Protocolo TLS v1.0 e v1.1**

Descrição:
O protocolo seguro TLS 1.2 dispõe de mais segurança em comparação das demais versões.
Justificativa:
As versões 1.0 e 1.1 estão vulneráveis a ataques, somente a versão 1.2 está apta a ser utilizada para assegurar a proteção das informações.
Configuração/Correção:
Desativar o protocolo de segurança TLS versão 1.0 e 1.1

- **Habilitar o Protocolo TLS v1.2**

Descrição:
O protocolo seguro TLS dispõe de mais segurança em comparação das demais versões.
Justificativa:
As versões 1.0 e 1.1 estão vulneráveis a ataques, somente a versão 1.2 está apta a ser utilizada para assegurar a proteção das informações.
Configuração/Correção:
Ativação do protocolo de segurança TLS 1.2


 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

- **Habilitar o Protocolo SNMP v3**

Descrição:
O protocolo SNMP v3 provê maior segurança na transmissão das informações de um equipamento. Esta segurança permite que as informações sejam criptografadas e acessadas apenas por pessoas autorizadas (usuário e senha).
Justificativa:
Prover maior segurança no envio das informações sensíveis dos equipamentos da empresa.
Configuração/Correção:
Ativar o protocolo SNMP v3

- **Desativar a cifragem RC4 para SSL/TLS**

Descrição:
ataque descrito é injetar um javascript malicioso no navegador da vítima que iria garantir que há múltiplas conexões sendo estabelecida com um site de destino e o mesmo cookie HTTP é enviada várias vezes para o website de forma criptografada. Isto proporciona a um invasor.
Justificativa:
Um dos motivos que RC4 ainda estava sendo usado foi ataques Besta e Lucky13 contra CBC cifras modo em SSL e TLS.
Configuração/Correção:
RC4 não deve ser utilizado quando possível

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

6.1 Aplicação de Patches


Soluções criptográficas que utilizarão os mecanismos listados abaixo para criptografia devem ser soluções que possam demonstrar pelo menos certificação FIPS140-2 ou PCI-HSM ou certificação equivalente.

Principal Categoria	Subcategoria	Mínimo Aceitável	Meta/Recomendado
Block/Bulk Ciphers	AES	128 bits	256 Bits
	Double Length TDES	112 Bits	
	Skipjack	80 Bits	Não Permitido ^[1]
	Componentes baseados em RC4 ^[2]	Utilização com Mínimo TLS/SSL	
Assinaturas Digitais (Função Hash)	DSA	L=2048, N=224	
	RSA	L=2048, N=224	
	ECDSA	L=2048, N=224	
Algoritmos de Hashing	SHA-2 ^[3]	SHA-224, SHA-256, SHA-384, SHA-512	SHA-512/224, SHA-512/256
Autenticação de Mensagem	DAC (AKA como MAC)	FIPS 113	
	HMAC	FIPS 198-1	
Segurança de Transporte	TLS	TLS 1.1	TLS 1.2
	SSL	Não Aceitável	TLS 1.2
	IPsec	IPv4	IPv6
Soluções de Direitos Adquiridos ^[4]	Bouncy Castle	V1.49	V1.49

^[1] Implantação de novos aplicativos ou extensão de utilização em aplicativos existentes não é aprovada. A utilização existente é um direito adquirido para uso aprovado.

^[2] Utilização com WEP não é aprovada. Todos os servidores DEVEM ter mitigação de ataque BEAST incluída.

^[3] Implantação de SHA-1 para novos aplicativos ou extensão de utilização em aplicativos existentes não é aprovada. A utilização existente é um direito adquirido para uso aprovado.

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Hardening para Windows Server

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Norma de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8. ANEXOS

Não aplicável;

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Nava	Segurança da Informação	Mateus Rocha

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
		Documento na versão inicial