 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	2
5.	RESPONSABILIDADES	3
6.	REGRAS BÁSICAS	3
7.	CONTROLE DE REGISTROS.....	14
8.	ANEXOS.....	14
9.	REGISTRO DE ALTERAÇÕES.....	14

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:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	1 de 14


 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- **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**.

4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- 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**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL Energia**.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	2 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

5. RESPONSABILIDADES

• Usuários

- ✓ O usuário titular das credenciais de acesso terá total responsabilidade pelo seu uso;
- ✓ O usuário é o responsável pela sua senha sendo pessoal e intransferível;
- ✓ Utilizar suas credenciais somente para fins designados e para os quais estiver devidamente autorizado (de acordo com as suas funções e responsabilidades);
- ✓ Substituir a senha inicial gerada pelo sistema e alterá-la periodicamente;
- ✓ Reportar imediatamente ao superior imediato e/ou ao setor responsável pela segurança da informação os casos de violação das credenciais, acidental ou não e, providenciar sua substituição;
- ✓ Notificar imediatamente ao departamento de Segurança da Informação sobre qualquer uso não autorizado de seu e-mail, conta de acesso ou qualquer outra quebra de segurança de seu conhecimento;
- ✓ Ler e praticar as normas descritas neste documento.

• Diretoria de Tecnologia da Informação

Gerenciar a segurança das informações corporativas, bem como elas são acessadas ou disponibilizadas. Analisar as solicitações recebidas e direcionar para Segurança da Informação avaliar se a solicitação é procedente ou não. Prover e manter o sistema de guarda, criação e alteração das credenciais dos usuários, além disso liberar o acesso de acordo com as normas previstas.

• Departamento de Segurança da Informação

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. Além disso cabe a Segurança da informação 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. E instalar sistemas de proteção, prevenção e detecção, para garantir a segurança das informações e dos perímetros de acesso.


6. REGRAS BÁSICAS

As regras desta norma se aplicam a todos os Servidores ou equipamentos que cumprem a função de servidor, das empresas do **Grupo CPFL Energia**.

Público-alvo

Todos os funcionários e Prestadores de Serviço do **Grupo CPFL Energia**, que façam uso de dispositivos que não são de propriedade do Grupo, e que tenham acesso a informações e/ou sistemas do Grupo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	3 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

6.1 O que é Server Hardening

O Server Hardening é o processo de aprimorar a segurança do servidor por meio de uma variedade de meios, o que resulta em um ambiente operacional de servidor muito mais seguro. Isso se deve às medidas de segurança avançadas implementadas durante o processo de proteção do servidor.

O termo "Hardening", no sentido geral, implica pegar uma superfície ou material macio e fazer alterações que resultem em que a superfície se torne mais forte e mais resistente a danos. É exatamente assim que a proteção do servidor impacta a segurança do servidor. Os servidores protegidos são mais resistentes a problemas de segurança do que os servidores não reforçados.


O Server Hardening, provavelmente uma das tarefas mais importantes a serem realizadas nos servidores, torna-se mais compreensível quando você percebe todos os riscos envolvidos. A configuração padrão da maioria dos sistemas operacionais não é projetada tendo a segurança como foco principal. Em vez disso, as configurações padrão se concentram mais na usabilidade, comunicação e funcionalidade. Para proteger os servidores o **Grupo CPFL Energia** estabelece políticas de proteção de servidor sólidas e sofisticadas.

6.2 Hardening em Servidores Linux

As práticas a seguir devem consideradas para instalação e correção dos sistemas Linux Server:

- ✓ Se a máquina for uma nova instalação, proteger do tráfego de rede hostil até a operação sistema é instalado e reforçado;
- ✓ Usar a versão mais recente do sistema operacional;
- ✓ Consultar a documentação de suporte do fornecedor para confirmar o ciclo de vida da versão. Considere tanto o principal quanto versão secundária (ou service pack) em que um fornecedor lança ambas;
- ✓ Criar um volume separado com as opções nodev, nosuid e noexec definidas para (/ tmp);
- ✓ Uma vez que (/ tmp) se destina a ser mundialmente gravável, a criação de uma partição separada para ele pode impedir o recurso exaustão. A configuração do nodev evita que os usuários criem ou usem dispositivos de blocos ou caracteres especiais. Contexto noexec impede que os usuários executem executáveis

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	4 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores


binários a partir de (/ tmp). Definir nosuid impede que os usuários criando arquivos de id de usuário definidos em (/ tmp);

- ✓ Criar volumes separados para (/ var), (/ log) e (/ home);
- ✓ O sticky bit impede os usuários com acesso de gravação ao diretório, excluindo arquivos pertencentes a outros usuários;
- ✓ Definir sticky bit em todos os diretórios que podem ser gravados por todo o mundo;
- ✓ Certificar que o sistema esteja configurado para receber atualizações de software;
- ✓ Para Red Hat Enterprise Linux (RHEL) ou SUSE Linux Enterprise Server (SLES), isso requer uma assinatura ser alocado ao sistema. Para a maioria das outras distribuições principais, esta é uma mudança simples de configuração;

As práticas a seguir devem consideradas para endurecimento dos sistemas Linux Server:

- ✓ Restringir core dumps;
- ✓ Core dumps têm como objetivo ajudar a determinar por que um programa foi abortado. Eles podem conter itens sensíveis ou dados confidenciais da memória. É recomendado que os core dumps sejam desabilitados ou restritos;
- ✓ Os serviços que fornecem / dependem de autenticação não criptografada devem ser desativados, a menos que haja motivos para uma exceção. Isso inclui telnet server; rsh, rlogin, rcp; ypserve, ypbind; tftp, tftpserver; talk e talkserver;
- ✓ Desativar todos os serviços e aplicativos iniciados por xinetd ou inetd que não estão sendo utilizado;
- ✓ O serviço inetd ou xinetd permite que programas sejam executados quando uma conexão é feita a uma rede designada porta. Todos os aplicativos inetd desnecessários devem ser desabilitados se não houver aplicativos necessários e, em seguida, desabilite;
- ✓ Desativar ou remover os serviços do servidor que não serão utilizados (por exemplo, FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP etc.);

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	5 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Verificar se o serviço syslog (rsyslog, syslog, syslogng) está em execução;
- ✓ O serviço syslog gerencia os logs em (/ var) (/ log /). A maioria das implementações de syslog modernas também oferecem suporte remoto encaminhamento de log;
- ✓ Habilitar um serviço Network Time Protocol (NTP) para garantir a precisão do relógio;
- ✓ A manutenção precisa do tempo facilita a análise dos registros do sistema quando necessário;
- ✓ Restringir o uso dos serviços cronand;
- ✓ Eles podem ser usados para executar comandos no sistema e só devem ser permitidos para contas que precisam desse acesso;


As práticas a seguir devem consideradas para acesso de usuários e gerenciamento de senhas dos sistemas Linux Server:

- ✓ Criar contas individuais para cada usuário que deve acessar o sistema;
- ✓ Evitar contas / senhas compartilhadas torna mais fácil manter uma trilha de auditoria e remover o acesso quando não mais necessário;
- ✓ Aplicar o uso da política de senhas fortes;
- ✓ As regras de segurança de senha podem ser definidas em (/etc/pam.d/passwordauth);
- ✓ Utilizar sudo para delegar acesso de administrador ao invés de conta admin/root;
 - O comando sudo permite um controle refinado de direitos para executar comandos como root (ou outros IDs de usuário).;
 - O arquivo de configuração (/ etc / sudoers) deve ser editado com o comando visudocommand;

As práticas a seguir devem consideradas para segurança de rede e acesso remoto dos sistemas Linux Server:

- ✓ Limitar as conexões a serviços em execução no host para usuários autorizados do serviço via firewalls e outras tecnologias de controle de acesso;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	6 de 14


 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ O firewall **iptables** é um componente do kernel comum a todos os sistemas Linux, mas as ferramentas usadas para gerenciar o firewall as regras diferem significativamente entre os fornecedores, portanto, verifique o guia de configuração específico da versão;
- ✓ Desativar os seguintes parâmetros do kernel em (/etc/sysctl.conf):
 - Encaminhamento de IP;
 - Enviar redirecionamentos de pacote;
 - Aceitação de pacote roteado de origem;
 - Aceitação de redirecionamento ICMP.
- ✓ Habilitar os seguintes parâmetros do kernel em (/etc/sysctl.conf):
 - Encaminhamento de IP;
 - Enviar redirecionamentos de pacote;
 - Aceitação de pacote roteado de origem;
 - Aceitação de redirecionamento ICMP.
- ✓ Na configuração do servidor SSH, certifique-se de que a versão do protocolo é definida como 2 e o LogLevel está definido como INFO;
- ✓ PermitEmptyPasswords está definido como não essas configurações são o padrão na maioria das plataformas, configurá-las com outros valores afeta a segurança do SSH servidor:
 - Desative o login de root por SSH
 - O SSH raiz com senha nunca deve ser permitido, os usuários devem se autenticar com sua própria conta e usar su ou sudo, se necessário. Os valores válidos para PermitRootSSHare não, sem senha e comandos forçados - apenas dependendo da necessidade de acesso baseado em chave;
- ✓ Implantar um Sistema de Prevenção de Intrusão (IPS), como fail2ban. O fail2ban usa o firewall iptables para bloquear sistemas remotos que geram muitas falhas de autenticação como forma de combater tentativas de senha de força bruta.

As práticas a seguir devem consideradas para Servidor Web Apache (HTTPD):

- ✓ Sempre executar o apache com uma conta de não administrador dedicada;
- ✓ A conta de usuário do sistema em que o servidor apache é executado deve ter permissão mínima no sistema para limitar o potencial para que isso seja explorado. Este é o padrão em todas as principais distribuições do Linux;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	7 de 14

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores


- ✓ Desativar todos os módulos não necessários;
- ✓ O Apache é modular em design, cada módulo oferece uma funcionalidade diferente e quase todos são opcionais para casos de uso. Em particular, procure desabilitar webdav, status, info, userdir e autoindex, a menos que estes sejam conhecidos por é necessário;
- ✓ Desativar o rastreamento de HTTP: TraceEnableOff;
- ✓ O serviço inetd ou xinetd permite que programas sejam executados quando uma conexão é feita a uma rede designada porta;
- ✓ Todos os aplicativos inetd desnecessários devem ser desabilitados se não houver aplicativos necessários e, em seguida, desabilite;
- ✓ Mozilla fornece recursos para este e outros protocolos em (https://wiki.mozilla.org/Security/Server_Side_TLS);
- ✓ Configurar o Apache para não anunciar as versões de software / sistema operacional;
- ✓ Definir "ServerTokens Prod" e "ServerSignature Off" para limitar as informações de configuração do sistema facilmente acessível;
- ✓ Negar o acesso aos arquivos por padrão permite apenas o acesso aos diretórios designados;
- ✓ Apenas os diretórios que contêm conteúdo do apache devem ser lidos por clientes remotos;

6.3 Hardening em Servidores Windows

As práticas a seguir devem consideradas para preparação do Windows Server:

- ✓ Proteger as máquinas recém-instaladas do tráfego de rede hostil até que o sistema operacional seja instalado e fortalecido. Proteja cada novo servidor em uma rede DMZ que não esteja aberta à Internet;
- ✓ Definir uma senha de BIOS / firmware para evitar alterações não autorizadas nas configurações de inicialização do servidor;
- ✓ Desativar o logon administrativo automático no console de recuperação;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	8 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Configurar a ordem de inicialização do dispositivo para evitar inicialização não autorizada de mídia alternativa;


As práticas a seguir devem consideradas para instalação do Windows Server:

- ✓ Certificar que o sistema não desligue durante a instalação;
- ✓ Utilizar o Assistente de configuração de segurança para criar uma configuração do sistema com base na função específica necessária;
- ✓ Certificar que todos os patches, hotfixes e service packs apropriados sejam aplicados imediatamente. Os patches de segurança resolvem vulnerabilidades conhecidas que os invasores poderiam explorar para comprometer um sistema. Depois de instalar o Windows Server, atualize-o imediatamente com os patches mais recentes via WSUS ou SCCM;
- ✓ Habilitar a notificação automática da disponibilidade do patch. Sempre que um patch é lançado, ele deve ser analisado, testado e aplicado em tempo hábil usando WSUS ou SCCM;

As práticas a seguir devem consideradas para proteção de segurança da conta de usuário do Windows Server:

- ✓ Certificar que suas senhas administrativas e do sistema atendam às melhores práticas de senha. Em particular, verifique se as senhas de contas privilegiadas não são baseadas em uma palavra do dicionário e têm pelo menos 15 caracteres, com letras, números, caracteres especiais e caracteres invisíveis (CTRL ^) intercalados. Certifique-se de que todas as senhas sejam alteradas a cada 90 dias.;
- ✓ Configurar a Política de Grupo de bloqueio de conta de acordo com as práticas recomendadas de bloqueio de conta;
- ✓ Impedir que os usuários criem e façam login com contas da Microsoft;
- ✓ Desativar a conta de convidado;
- ✓ Não permitir que as permissões "todos" se apliquem a usuários anônimos;
- ✓ Não permitir a enumeração anônima de contas e compartilhamentos SAM;
- ✓ Desativar a conversão anônima de SID / Nome;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	9 de 14


 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Desativar ou excluir prontamente as contas de usuário não utilizadas.

As práticas a seguir devem consideradas para configuração de segurança de rede do Windows Server:

- ✓ Habilitar o firewall do Windows em todos os perfis (domínio, privado, público) e configure-o para bloquear o tráfego de entrada por padrão;
- ✓ Executar o bloqueio de porta no nível de configuração da rede. Faça uma análise para determinar quais portas precisam ser abertas e restringir o acesso a todas as outras portas;
- ✓ Restringir a capacidade de acessar cada computador da rede apenas para usuários autenticados;
- ✓ Não conceder a nenhum usuário o direito de 'agir como parte do sistema operacional';
- ✓ Negar as contas de convidados a capacidade de fazer logon como um serviço, um trabalho em lote, localmente ou via RDP;
- ✓ Se RDP for utilizado, definir o nível de criptografia da conexão RDP como alto;
- ✓ Remover Habilitar pesquisa de LMhosts;
- ✓ Desativar o NetBIOS sobre TCP / IP;
- ✓ Remover ncacn_ip_tcp;
- ✓ Configurar o Microsoft Network Client e o Microsoft Network Server para sempre assinar digitalmente as comunicações;
- ✓ Desativar o envio de senhas não criptografadas para servidores SMB de terceiros;
- ✓ Não permitir que nenhum compartilhamento seja acessado anonimamente;
- ✓ Permitir que o sistema local use a identidade do computador para NTLM;
- ✓ Desativar o fallback de sessão NULL do sistema local;
- ✓ Configurar os tipos de criptografia permitidos para Kerberos;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	10 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Não armazenar valores de hash do LAN Manager;
- ✓ Definir o nível de autenticação do LAN Manager para permitir apenas NTLMv2 e recusar LM e NTLM;
- ✓ Remover o compartilhamento de arquivos e impressão das configurações de rede. O compartilhamento de arquivos e impressoras pode permitir que qualquer pessoa se conecte a um servidor e acesse dados críticos sem exigir um ID de usuário ou senha;


As práticas a seguir devem consideradas para configuração de segurança dos registros do Windows Server:

- ✓ Certificar que todos os administradores dediquem um tempo para entender completamente como o registro funciona e a finalidade de cada uma de suas várias chaves. Muitas das vulnerabilidades no sistema operacional Windows podem ser corrigidas alterando chaves específicas, conforme detalhado a seguir;
- ✓ Configurar as permissões do registro, proteger o registro do acesso anônimo;
- ✓ Os registros abaixo devem ter seus valores definidos como 0:
 - MaxCachedSockets (REG_DWORD);
 - SmbDeviceEnabled (REG_DWORD);
 - AutoShareServer;
 - AutoShareWks;
- ✓ Excluir todos os dados de valor DENTRO da chave NullSessionPipes;
- ✓ Excluir todos os dados de valor DENTRO da chave NullSessionShares.

As práticas a seguir devem consideradas para configurações gerais de segurança do Windows Server:

- ✓ Desativar serviços desnecessários. A maioria dos servidores tem a instalação padrão do sistema operacional, que geralmente contém serviços estranhos que não são necessários para o funcionamento do sistema e que representam uma vulnerabilidade de segurança. Portanto, é fundamental remover todos os serviços desnecessários do sistema;


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	11 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Remover os componentes desnecessários do Windows. Todos os componentes desnecessários do Windows devem ser removidos dos sistemas críticos para manter os servidores em um estado seguro;
- ✓ Habilitar o Sistema de Arquivos com Criptografia (EFS) interno com NTFS ou BitLocker no Windows Server;
- ✓ Se a estação de trabalho tiver memória de acesso aleatório (RAM) significativa, desative o arquivo de troca do Windows. Isso aumentará o desempenho e a segurança porque nenhum dado sensível pode ser gravado no disco rígido;
- ✓ Não utilizar AUTORUN. Caso contrário, o código não confiável pode ser executado sem o conhecimento direto do usuário; por exemplo, os invasores podem colocar um CD na máquina e fazer com que seu próprio script seja executado;
- ✓ Exibir um aviso legal como o seguinte antes de o usuário fazer login: "O uso não autorizado deste computador e de recursos de rede é proibido...";
- ✓ Requerer Ctrl + Alt + Del para logins interativos;
- ✓ Configurar um limite de inatividade da máquina para proteger sessões interativas ociosas;
- ✓ Certificar que todos os volumes estejam usando o sistema de arquivos NTFS;
- ✓ Configurar as permissões de arquivo / pasta local. Outro procedimento de segurança importante, mas frequentemente esquecido, é bloquear as permissões de nível de arquivo para o servidor.

Por padrão, o Windows não aplica restrições específicas a nenhum arquivo ou pasta local; o grupo Todos recebe permissões totais para a maior parte da máquina. Remova este grupo e, em vez disso, conceda acesso a arquivos e pastas usando grupos baseados em funções com base no princípio de privilégios mínimos. Todas as tentativas devem ser feitas para remover Convidado, Todos e ANONYMOUS LOGON das listas de direitos do usuário. Com esta configuração, o Windows ficará mais seguro;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	12 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

- ✓ Definir a data / hora do sistema e configure-o para sincronizar com os servidores de hora do domínio;
- ✓ Configurar uma proteção de tela para bloquear a tela do console automaticamente se não for supervisionada.

As práticas a seguir devem consideradas para configuração de política de auditoria do Windows Server:

- ✓ Habilitar a política de auditoria de acordo com as práticas recomendadas da política de auditoria. A política de auditoria do Windows define quais tipos de eventos são gravados nos logs de segurança de seus servidores Windows;
- ✓ Configurar o método de retenção do Log de eventos para sobrescrever conforme necessário e com tamanho de até 04 GB;
- ✓ Configurar o envio de log para SIEM para monitoramento;


As práticas a seguir devem consideradas para guia de segurança de software do Windows Server:

- ✓ Instalar e ativar o software antivírus. Configurar para atualizar diariamente;
- ✓ Instalar e ativar o software anti-spyware. Configurar para atualizar diariamente;
- ✓ Instalar o software para verificar a integridade dos arquivos críticos do sistema operacional. O Windows tem um recurso denominado Proteção de Recursos do Windows que verifica automaticamente determinados arquivos-chave e os substitui se forem corrompidos.

As práticas a seguir devem consideradas para finalização de configuração do Windows Server:

- ✓ Montar uma imagem de cada sistema operacional usando GHOST ou Clonezilla para simplificar ainda mais a instalação e proteção do Windows Server;
- ✓ Inserir sua chave de licença do Windows Server 2016/2012/2008/2003;
- ✓ Inserir o servidor no domínio e aplique suas políticas de grupo de domínio;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	13 de 14

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Servidores

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
Não Aplicável	Não Aplicável	Documento em versão inicial

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18888	Instrução	1.0	Emerson Cardoso	17/08/2021	14 de 14