SERVIDORES DE REDE - AMBIENTE WINDOWS - PADRONIZAÇÃO, SEGURANÇA E ADMINISTRAÇÃO

Sumário

SERVIDORES DE REDE - AMBIENTE WINDOWS - PADRONIZAÇÃO, SEGURANÇA E ADMINISTRAÇÃO

1. ASSUNTO/OBJETIVO

Estabelecer padrões de segurança para administração dos servidores Windows que compõem a rede do Tribunal de Justiça.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Garantir a padronização das configurações de segurança e administração dos computadores servidores de rede que utilizem o sistema operacional *Microsoft Windows Server*.

3. UNIDADE GESTORA

Secretaria de Informática
Coordenadoria de Suporte Técnico (CST).
Serviço de Segurança e Sistemas Básicos (SSSB).

4. PÚBLICO ALVO

Todo o Tribunal

5. RELAÇÃO COM OUTROS NORMATIVOS

Rotina e Validação de Backup

6. REGULAMENTAÇÃO UTILIZADA

Não se aplica.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Acesso Remoto - Nome atribuído ao acesso realizado a um computador por outro.

Active Directory - Serviço de diretório nativo no Windows 2008 Server que armazena contas, senhas e políticas da rede.

Antivírus - Programa utilizado para prevenir, detectar e eliminar vírus eletrônicos de computadores contaminados.

Backup - Cópia de segurança dos arquivos de um computador.

Conta de Rede - Identificação pessoal do usuário que permite acesso à rede local.

Conta de Serviço - Contas específicas, geralmente com direitos de administrador, utilizadas para iniciar serviços de produtos da Microsoft como o System Center, Exchange Server e outros sistemas.

Conta Administrator - Conta padrão comum aos servidores com sistema operacional *Windows Server* criada no momento da instalação destes que permite gerência administrativa a nível local nos servidores. A senha é de conhecimento dos administradores dos sistemas operacionais *Windows Server*.

Conta *SYSTEM* - Conta nativa dos sistemas operacionais da plataforma *Windows* utilizada para ativação de diversos serviços. Essa conta não possui senha explícita e é gerenciada pelo próprio sistema operacional.

Controlador de domínio - Computador com *Windows Server* que recebe uma cópia do banco de dados do diretório de domínio, com todas as informações de contas e políticas de segurança para o domínio, sendo que a cópia é sincronizada periodicamente com as cópias mantidas pelos outros controladores de domínio.

Domínio - Agrupamento lógico de servidores de rede e outros computadores que compartilham uma segurança comum e informações de contas de usuários. Com os domínios, os administradores criam uma conta para cada usuário que se conecta aos domínios, e não aos servidores individuais no domínio. A terminologia “domínio” é utilizada para o sistema operacional *Windows*.

Domínio de Contas - Domínio com sistema operacional *Windows* que contém contas de usuários daquele domínio.

Domínio de Recurso - Domínio com sistema operacional *Windows* que não autentica usuários apenas provê recursos.

Endereço IP - É o endereço atribuído a cada equipamento pertencente a uma rede de computadores que utiliza como protocolo de interconexão o TCP/IP.

Estação de Trabalho - Computador pelo qual é feito o acesso à rede do TJPA, utilizado por um usuário para executar aplicativos e usufruir os recursos dessa rede.

FTP - *File Transfer Protocol* – protocolo utilizado para realizar transferências de arquivos entre máquinas clientes e servidoras.

Grupo - Conjunto de usuários com permissões comuns para determinados objetos como, por exemplo, arquivos compartilhados ou tabelas de banco de dados.

Hot Fix - Atualizações do sistema operacional destinadas a correções de erros encontrados após o lançamento de um *Service Pack*.

Logoff - É o processo de encerramento da sessão de trabalho pelo usuário.

Logon - É o processo de identificação e autenticação ao qual o usuário é submetido antes de integrar-se ao sistema, software ou aplicativo.

Member Server - Servidores dedicados a tarefas específicas, como impressão ou servidores de arquivos, ou a aplicações de grandes proporções como bancos de dados que, executando o sistema operacional para servidores, não armazenam cópias do banco de dados do domínio que fazem parte, e portanto, não autenticam as contas nem recebem cópias sincronizadas desse banco de dados.

Modem - Periférico utilizado para transmitir dados e interligar um computador a um outro ou a uma rede de computadores via linha telefônica.

NTFS *- New Technology File System* - Sistema de arquivos usado em computadores com sistema operacional *Windows* que inclui recursos de segurança necessários a servidores e computadores pessoais, possibilitando definir permissões de controle de acesso a arquivos e diretórios.

PDC *– Primary Domain Controller* - Computador com *Windows Server* que autentica logons de domínio e mantém o banco de dados de diretório para um domínio, controlando as alterações feitas nas contas de todos os computadores e usuários em um domínio.

Perfil de Administrador - Funcionário efetivo ou contratado do TJPA, responsável pela administração dos recursos e serviços dos servidores *Windows* em seu domínio.

Perfil de Criação de Contas - Usuário responsável pela criação, manutenção e remoção das contas de usuários do domínio com sistemas operacionais *Windows* sob sua responsabilidade.

Perfil de Operador - Usuário com atribuição de operação do servidor.

Protocolo de Comunicação - Regras e procedimentos necessários para realizar e controlar a comunicação entre equipamentos.

Recurso - Qualquer dispositivo que possa ser compartilhado por meio da rede.

Registry - Banco de dados do sistema operacional *Windows* que mantém informações de configuração de hardware, software e usuários de um computador.

Relação de Confiança - Comunicação entre controladores de diferentes domínios através da qual os usuários que são membros do domínio que recebem direitos podem acessar serviços de outro domínio que concede direitos, sem a necessidade de efetuar logon no domínio concedente.

Service Pack - Atualizações do sistema operacional destinadas a correções de erros encontrados após o lançamento de uma versão.

Serviço - Recurso disponível no sistema operacional para a realização de tarefas específicas.

Servidor - Computador com sistema operacional *Windows Server*, no qual são disponibilizados os serviços e recursos de rede.

Sessão de Trabalho - Intervalo de tempo em que o usuário efetua logon em um servidor ou estação de trabalho até o momento em que ele efetua logoff.

Setup - É o conjunto de parâmetros inter-relacionados, utilizados pelo equipamento quando da sua inicialização e alteráveis pelo usuário para definir a configuração do hardware.

Sistema Operacional - É o software utilizado para controlar e coordenar as tarefas atribuídas ao computador.

System State - Arquivos do sistema operacional *Windows* e suas configurações que podem ser copiados e permitem a restauração de um servidor a um estado anteriormente conhecido.

Software - É um termo geral para definição de vários tipos de programas usados para operar computadores e seus componentes interligados.

Suporte - Usuário responsável pela instalação, configuração e manutenção da infra-estrutura tecnológica dos domínios com sistemas operacionais *Windows*.

TCP/IP - *Transmission Control Protocol / Internet Protocol* – conjunto de protocolos utilizado na comunicação entre equipamentos de rede.

Usuário - É o funcionário do TJPA, prestador de serviço ou estagiário autorizado a ter acesso à rede local de acordo com as permissões a ele atribuídas.

WINS – Windows Internet Naming Service - serviço da Microsoft que mapeia nomes de máquina *Windows* para os endereços IP correspondentes.

Windows Server - Sistema operacional de rede utilizado por computador que pode assumir um dos três papéis típicos de servidores: controlador de domínio ou *member server* para redes *Windows*.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

8.1 Orientações Gerais

8.1.1 A designação de usuários para desempenharem atividades de administrador, operador, suporte e criação de contas da plataforma *Windows* está de acordo com os pré-requisitos e orientações definidos nos documentos de padrões para o ambiente *Windows* de acordo com os normativos da Secretaria de Informática.

8.1.2 A unidade responsável pela especificação, instalação e gerência dos servidores centralizados e descentralizados da rede TJPA é da SSSB.

8.1.3 A unidade responsável pela manutenção física dos servidores descentralizados da rede TJPA é da CAU.

8.1.4 A elaboração de nomes de componentes da rede e contas de usuários segue os padrões e orientações para servidores definidos pela Secretaria de Informática.

8.1.5 Não é permitida a utilização de acesso remoto à rede do TJPA por meio de linha discada.

8.1.6 A recuperação dos sistemas operacionais será realizada por software de *backup* ou tecnologia de virtualização conforme o caso.

8.1.7 As alterações de configuração das partições de disco dos servidores *Windows* virtuais, geram uma nova requisição de sincronização de máquina virtual para o site sede do TJPA (Localizado na av.Almirante Barroso).

8.1.8 Os servidores *Windows* atendem aos requisitos mínimos de hardware especificados para a utilização do sistema operacional *Windows*.

8.1.9 A homologação de novos produtos ou novas versões para o sistema operacional *Windows* seguem as diretrizes estabelecidas pela Secretária de Informática.

8.2 Acesso Físico:

8.2.1 O acesso físico aos servidores é controlado pela chefia da unidade em que esses se encontram.

8.2.2 Os serviços de manutenção terceirizada dos servidores são acompanhados durante toda a sua execução por, pelo menos, um servidor do TJPA.

8.3 Acesso Lógico:

8.3.1 Os servidores Internet e Extranet que provêem serviços de acesso público ou externo com empresas de relacionamento com o TJPA são isolados da rede interna e de qualquer rede pública através da utilização de equipamentos de firewall e roteadores.

8.3.2 Os roteadores e firewalls são configurados para restringir o tráfego entre as redes públicas e os servidores do TJPA de acesso público.

8.3.3 Os roteadores e firewalls são configurados para restringir o tráfego entre os servidores da TJPA de acesso público e a rede interna.

8.3.4 Todos os servidores que permitirem acesso remoto são configurados para utilização de algoritmos de criptografia forte e chave de, no mínimo, 256 bits.

8.3.5 O número de administradores de rede com acesso aos servidores é reduzido ao mínimo imprescindível para a execução das tarefas a que se destina e controlado pela Coordenadoria de Suporte Técnico.

8.3.6 As contas dos administradores de rede são monitoradas pela SSSB.

8.4 Auditoria de Eventos:

8.4.1 Os logs de auditoria são configurados para disponibilizar o monitoramento de eventos nos servidores.

8.4.2 Os servidores são configurados com a finalidade de registrar eventos de segurança, de acordo com os parâmetros descritos neste normativo.

8.5 Alertas Administrativos:

8.5.1 Os alertas nos servidores com o sistema operacional *Windows* são configurados para permitir o envio de informações aos administradores de domínio sobre eventos do sistema, de acordo com os parâmetros descritos na sessão 10.

8.6 Contas:

8.6.1 O cadastramento de usuários nos domínios é feito quando da solicitação via formulário e requisição via chamado eletrônico e cadastro via sistema de RH (MENTOR - gerando matrícula junto ao tribunal).

8.6.2 Os usuários têm uma única conta de logon em toda a rede do TJPA, independente de sua localização física.

8.6.3 Os usuários são cadastrados somente no domínio ao qual estão vinculados.

8.6.4 As atualizações de informações dos funcionários do TJPA no cadastro de usuários, tais como alteração de função ou lotação, são feitas automaticamente com base no sistema de RH: MENTOR.

8.6.5 As atualizações de informações de prestadores de serviço no cadastro de usuários são alteradas em casos de alteração de função ou lotação de usuários.

8.6.6 Em caso de demissão do funcionário ou término de vigência do contrato de prestadores de serviço e estagiários, as contas desses serão desabilitadas de imediato.

8.6.7 É proibida a criação de contas genéricas para usuários.

8.6.8 O prestador de serviços de empresa terceirizada responsável pela manutenção dos servidores possui sua própria conta de rede e senha.

8.6.9 A conta g*uest* é mantida desabilitada.

8.6.10 A conta administrator tem uma senha de caracteres alfanuméricos, sob guarda da SSSB.

8.6.11 A conta administrator não é renomeada.

8.6.12 As contas específicas para a administração do domínio são utilizadas exclusivamente para a realização de tarefas administrativas relativas ao domínio.

8.6.13 A conta de sistema *system* é a conta utilizada para iniciar serviços, exceto nos casos em que o serviço ou a aplicação demande a utilização de contas específicas para esse fim.

8.6.14 O cadastramento de conta de usuários em servidores *Members Servers* somente é permitido quando em casos excepcionais e analisados e autorizado pelo SSSB.

8.6.14.1 O cadastramento é realizado pelo SSSB.

8.6.14.2 Usuários locais quando for o caso serão cadastrados nestes servidores face a necessidade de utilização de contas do domínio, quando devidamente autorizado pelo SSSB.

8.7 Senhas:

8.7.1 Os usuários são instruídos pelo SSSB a compor senhas a partir da combinação aleatória de caracteres alfanuméricos e sinais gráficos, com o uso de maiúsculas e minúsculas.

8.7.2 Não é permitido o acesso à rede TJPA com a utilização de senhas em branco.

8.7.3 As contas inativas por um período superior a 90 dias consecutivos terão seu acesso suspenso.

8.7.4 As contas inativas por um período superior a 180 dias consecutivos serão desabilitadas da rede.

8.7.5 As senhas das contas de usuário têm validade de, no máximo, 90 dias.

8.7.5.1 Após o período de validade das senhas das contas, o sistema obriga o usuário a trocá-la.

8.7.6 As senhas são compostas de, no mínimo, 8 caracteres.

8.7.7 As 5 últimas senhas dos usuários não podem ser reutilizadas.

8.7.8 A reativação da senha de rede é feita pelo SSSB via solicitação eletrônica por meio de requisição por chamado técnico à central de serviços.

8.7.9 As senhas das contas de serviços são definidas de modo a jamais expirarem.

8.7.9.1 Casos específicos em que haja necessidade de alteração de senha são tratados pontualmente pelo SSSB.

8.7.9.2 A guarda das senhas das contas de serviços corporativas (exemplo: contas de serviço dos aplicativos estão sob guarda da SSSB.

8.8 Configuração de Domínios Windows:

8.8.1 Somente podem ser instalados servidores controladores de domínio *Windows 2008 Server ou Windows Server 2003* nas instalações do TJPA.

8.8.1.1 A atividade é avaliada e monitorada pela SSSB.

8.8.2 Somente pode ser alterado o papel dos controladores de domínio, a quantidade ou a destinação originalmente prevista do servidor após avaliação da SSSB

8.8.3 Os demais servidores das unidades serão instalados como *member server* no domínio *Windows*.

8.9 Instalação de Servidores:

8.9.1 Os servidores ligados à Rede TJPA não possuem modem.

8.9.2 A opção de inicialização dos servidores pelo sistema operacional DOS é removida, caso exista.

8.9.3 Os *service packs* e *hot fixs* dos servidores são aplicados conforme orientações da SSSB, após sua homologação.

8.9.4 É implementada senha de *setup* da BIOS nos servidores.

8.10 Configuração de Servidores:

8.10.1 Cada unidade judiciária tem acesso a servidores de arquivos que armazenam os diretórios home dos usuários de acordo com a demanda repassada ao SSSB.

8.10.2 O idioma utilizado no sistema operacional dos servidores é o inglês.

8.10.3 Nos servidores Windows, a opção de *recovery console* deve estar ativa em todos os servidores, com solicitação de senha para acesso a console.

8.10.4 Somente os administradores possuem acesso remoto ao registro do *Windows*.

8.10.5 Os programas de antivírus devem estar atualizados nos servidores.

8.10.6 O servidor deve ser configurado de forma a que todos os arquivos nele recebidos sejam verificados quanto à contaminação por vírus eletrônico antes de sua utilização.

8.10.7 Os servidores são configurados de forma a estarem sincronizados com o seu servidor de horário corporativo com relação à data e hora.

8.11 Serviços e Protocolos de Comunicação:

8.11.1 O conjunto de protocolos de comunicação TCP/IP é o único a ser instalado nos servidores *Windows*.

8.12 Operação dos Servidores:

8.12.1 Os servidores não são utilizados como estação de trabalho.

8.12.2 Todos os servidores da rede permanecem ligados e ativos 24 horas por dia, 7 dias por semana.

8.12.3 O usuário sempre deve encerrar sua sessão de trabalho ao terminar suas tarefas no servidor.

8.12.4 Na impossibilidade de interrupção de serviços no servidor, o usuário bloqueia a sessão de trabalho.

8.12.5 O programa de antivírus está habilitado durante todo o período de funcionamento dos servidores.

8.12.6 No compartilhamento de pastas, arquivos e recursos, é especificado o grupo global ou local e os usuários que têm direito de acesso ao recurso.

8.12.7 Nos servidores, são utilizados apenas os programas homologados pelo TJPA, necessários à sua funcionalidade.

8.12.8 Nos servidores do TJPA não são instalados jogos de entretenimento.

8.12.9 A conta de acesso e sua senha são pessoais e intransferíveis.

8.12.10 A sessão de trabalho é utilizada apenas pelo usuário proprietário da conta de acesso e seu compartilhamento é proibido.

8.12.11 Os servidores do TJPA não são utilizados para navegação web, seja Intranet ou Internet, utilização de correio eletrônico, chat ou quaisquer outras atividades não relacionadas aos serviços providos pelo servidor.

8.13 Backup:

8.13.1 A realização do backup segue os padrões e orientações exigidas pela Secretaria de Informática.

8.13.2 Os procedimentos de realização do backup e da restauração de dados são formalizados por meio de documentação oficial.

8.13.3 A restauração do backup é feita somente para recompor a integridade do ambiente ou sob a solicitação formal da Secretaria de Informatica.

8.13.4 O backup dos arquivos de log do netlogon dos controladores de domínio do site central são feitos com periodicidade e prazo de retenção que garantam a continuidade dos serviços.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 Administrador

9.1.1 Desempenhar suas tarefas apenas nos servidores sob sua responsabilidade.

9.1.2 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações constantes nos normativos do TJPA.

9.1.3 Manter atualizado o software antivírus homologado pelo TJPA nos servidores *windows*.

9.1.4 Criar, manter e remover os grupos locais dos servidores do ambiente no qual é responsável, obedecendo aos padrões estabelecidos.

9.1.5 Garantir a atualização dos *service packs* e *hot fixes* homologados nos servidores.

9.1.6 Configurar a proteção de tela com a solicitação de senha para desbloqueio nos servidores, com ativação dentro de cinco minutos de inatividade, no máximo.

9.1.7 Desinstalar nos servidores os serviços e protocolos de comunicação desnecessários a sua utilização.

9.1.8 Verificar a realização do *backup* dos servidores.

9.1.9 Configurar os logs de auditoria para disponibilizar monitoramento de eventos nos servidores.

9.1.10 Verificar os *logs* de eventos dos servidores sob sua responsabilidade, atuando para solução de eventuais falhas detectadas.

9.1.11 Criar e atualizar o disco de recuperação de partição no caso de existência de partições com tolerância a falha.

9.1.12 Criar e atualizar o disco emergencial de reparos.

9.1.13 Para os servidores com sistema operacional *windows*, criar e atualizar cópia do s*ystem state*.

9.1.14 Estabelecer permissões de acesso a pastas e arquivos.

9.1.15 Garantir que somente os administradores tenham acesso remoto ao registro.

9.1.16 Monitorar a rede do TJPA de forma a inibir a instalação de modems nas máquinas da plataforma descentralizada.

9.1.17 Os usuários que possuem contas específicas para a administração do domínio, não as utilizam para a realização de tarefas diárias, pois sua utilização é exclusiva para tarefas administrativas relativas ao domínio.

9.1.18 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações estabelecidas nos normativos do TJPA.

9.2 Chefia da Unidade:

9.2.1 É de responsabilidade da chefia da unidade designar um empregado do TJPA para acompanhar qualquer pessoa que não possua atividade afim com os servidores durante toda a sua permanência na sala dos servidores.

9.2.2 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações estabelecidas nos normativos do TJPA.

9.3 Operador:

9.3.1 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações estabelecidas nos normativos do TJPA.

9.4 Suporte:

9.4.1 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações estabelecidas nos normativos do TJPA.

9.5 Usuário:

9.5.1 Compor senha de acesso à rede com, no mínimo, 06 caracteres.

9.5.2 Sempre encerrar sua sessão de trabalho ao terminar suas tarefas no servidor.

9.5.3 Bloquear a sessão de trabalho na impossibilidade de interrupção de serviços no servidor.

9.5.4 Os usuários comuns não têm acesso de logon em servidores departamentais ou corporativos.

9.5.5 Usar os recursos e informações a que tiver acesso somente para o desempenho de suas atribuições, em estrita observância às normas, padrões e orientações estabelecidas nos normativos do TJPA.

9.6 Infrações:

9.6.1 A infração às disposições estabelecidas na presente norma, devidamente apurada, implica a:

- aplicação das penas disciplinares previstas no regulamento de pessoal aos servidores do TJPA;
- aplicação das sanções previstas em contrato aos prestadores de serviço e estagiários, além dos demais procedimentos legais cabíveis.

10. PROCEDIMENTOS

10.1 Segurança Padrão dos Servidores:

10.1.1 Os servidores *Member Server* com o sistema operacional *windows 2000 advanced server* estão em uma unidade organizacional própria no serviço de diretório a*ctive directory*.

10.1.2 Os servidores controladores de domínio com o sistema operacional *windows 2000 advanced server* estão em uma unidade organizacional própria no serviço de diretório *active directory*.

10.2 Auditoria de Eventos:

10.2.1 Os servidores são configurados com a finalidade de registrar os seguintes eventos de segurança, em caso de falha ou sucesso:

- Servidores Windows 2008:
  - Tentativas de logon e logoff – Logon and Logoff;
  - Uso dos direitos de usuários – Use of User Rights;
  - Gerenciamento de grupos e usuários – User and Group Management;
  - Reinicialização do sistema – Restart, Shutdown, and System.
- Servidores Windows 2000 ou superior:
  - Auditoria de eventos de logon – Audit Logon Events;
  - Auditoria de acesso ao serviço de diretório – Audit Directory Service Access;
  - Auditoria de gerenciamento de contas – Audit Account Management;
  - Eventos de “logon” de conta de auditoria – Audit Account Logon Events;
  - Auditoria de alteração de diretivas – Audit Policy Change.

10.2.3 A opção de sobrescrita de logs devem estar configuradas para sobrescrever eventos anteriores há 7 dias.

10.2.3.1 Caso o log fique cheio antes dos 7 dias, ou seja, antes de sobrepor os eventos mais antigos, aumenta-se o tamanho do log.

10.2.4 Os logs de aplicação e sistema são verificados diariamente.

10.2.5 A limpeza do log é executada após a gravação do mesmo para o disco.

10.2.6 Os logs de eventos devem ser salvos diariamente em disco.

10.2.6.1 O período de retenção dos logs salvos é de 30 dias em disco e de 6 meses em fita.

10.3 Alertas Administrativos:

10.3.1 A configuração dos alertas administrativos é feita em cada servidor através do *Control Panel/Server*, opção *Alerts*, com a inserção das matrículas dos administradores que receberão os alertas daquele servidor.

10.3.2 Caso existam estações de administração, essas máquinas podem ser relacionadas para também receber os avisos de alerta.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Não se aplica.

12. CONSIDERAÇÕES FINAIS

Não se aplica.