DIRETRIZES PARA ADMINISTRAÇÃO EM EQUIPAMENTOS DE REDE DE COMUNICAÇÃO DE DADOS

Sumário

DIRETRIZES PARA ADMINISTRAÇÃO EM EQUIPAMENTOS DE REDE DE COMUNICAÇÃO DE DADOS

1. ASSUNTO/OBJETIVO

Estabelecer padrões e normas de segurança para controle de acesso, administração, funcionamento e relações entre equipamentos de comunicação de dados (roteadores, switches, firewalls e outros) dentro da dependência do TJPA.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Este normativo se aplica a todas as unidades do TJPA.

3. UNIDADE GESTORA

SECINFO – Secretaria de Informática

4. PÚBLICO ALVO

Serviço de Infraestrutura de Rede

5. RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica.

6. REGULAMENTAÇÃO UTILIZADA

- ABNT NBR ISO/IEC 17799:2005

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Ataque ARP Spoofing - consiste em passar um MAC Address (endereço MAC) falso para o sistema alvo de forma que este redirecione o tráfego para outro destino que não o legítimo.
Ataque Envenenamento (poisoning) da tabela ARP - forma de execução do ataque ARP Spoofing. Ataque de camada 2. Um atacante “A” envia um pacote ARP reply para toda a rede, informando falsamente ser dono de um par IP/MAC (que, na verdade pertence a “B”). As outras estações colocam esta informação em suas tabelas ARP, provocando o desvio de tráfego de B para A. Este tipo de ataque é utilizado para capturar dados de usuário e senha. Este ataque é usado como base para outros ataques, como por exemplo, o ataque de IP SPOOFING,

no caso de comunicação ponto-a-ponto (B<->A) e MITM (Man in the Middle) quando “B” fala com “C” tendo “A” entre eles (B <-> A <-> C).

Ataque Flooding da tabela ARP - ataque de camada 2. O atacante envia vários endereços MAC falsificados para uma mesma porta de switch, exaurindo todas as entradas disponíveis na tabela utilizada pelo switch para manter a correspondência entre endereços MAC e interfaces (a tabela CAM). Quando a tabela CAM está cheia, o switch passa a se comportar como u m hub (entra em flooding).

Ataque IP Spoofing - envio de pacotes com um endereço IP diferente daquele originalmente recebido pelo host. Consiste em trocar o endereço IP dos pacotes de comunicação a fim de se passar por outro host que por ventura tenha algum privilégio na rede (relação de confiança), por exemplo, alguma estação de trabalho que tenha acesso privilegiado a algum ativo de rede controlado por lista de acesso (access-list).

Ataque M.I.T.M. (Man in the Middle) - é um ataque onde o invasor consegue se colocar entre o emissor e o receptor sendo capaz de ler, inserir e modificar mensagens, sem que nenhum dos lados saiba que a sessão entre eles está comprometida.

Ataque Smurfing - um tipo de ataque DDoS, no qual um atacante utiliza vários hosts espalhados pelo mundo (smurfs) para atacar um determinado site (gargamel), explorando uma falha de configuração em gateways que permitem a passagem de pacotes ICMP em broadcast. Um atacante envia para o gateway vulnerável um pacote ping com destino ao endereço IP de broadcast da rede vulnerável, tendo seu endereço de origem falsificado para o endereço a ser atacado. Quando bem sucedido, todos os hosts da rede vulnerável passam a enviar pacotes ICMP echo reply para o host da vítima.

Ataque SYN Flooding - um tipo de ataque DoS, no qual um atacante inicia um grande número de conexões TCP – geralmente com endereço IP de origem falsificado - sem chegar a finalizá-las. Esse tipo de ataque exaure a tabela utilizada por servidores para manter conexões TCP que estão em processo (enbryonic) e impede que o servidor aceite novas conexões.

Ataque VLAN Hopping - forma de ataque que permite a uma estação injetar tráfego em VLAN às quais não deveria ter acesso. O tráfego gerado é unidirecional. Funcionamento: uma estação de trabalho com conexão de tronco com o switch de acesso envia pacotes 802.1q duplamente encapsulados (um pacote 802.1q dentro de outro pacote 802.1q). O switch de acesso desencapsula o pacote e interpreta o conteúdo como um pacote 802.1q que deve ser roteado para uma VLAN. Obs.: só funciona se a VLAN nativa do switch for a VLAN 1.

Ataques DDoS (Distributed Denial of Service) - mais potente que o DoS, neste tipo de ataque as tarefas de negação de serviço são distribuídas a um "exército" de máquinas escravizadas, também com a finalidade de tornar os recursos de um sistema indisponíveis para seus usuários.

Ataques DoS (Denial Of Service) - ataques do tipo DoS têm como objetivo tornar um serviço (um site na Internet, por exemplo) indisponível através da exaustão dos recursos de rede ou de CPU. Exemplos deste tipo de ataque são os ataques SYN FLOODING e SMURFING.

Ativos de Rede - todos os equipamentos de comunicação da rede, ou seja, roteadores, switches e firewalls.
Autenticação - processo de validação da identidade de uma pessoa ou objeto.
Autorização - processo de concessão de direitos de execução de determinadas ações (por exemplo: leitura de arquivos, execução de comandos num roteador etc.).
Backbone - conjunto de circuitos de comunicação WAN destinados à distribuição da malha física da rede TJPA, sem conexão com as unidades operacionais que não sejam as de "nós" de rede (SIR), independente da capacidade (banda) do circuito.
BPDU (Bridge Protocol Data Unit) - parte do protocolo spanning tree que ajuda a descrever e atribuir os atributos de uma porta de switch. Permite aos switches obterem informação de cada porta.
CAM (Content-Addressable Memory) - tabela utilizada pelos switches ethernet para associar endereços MAC acessíveis em cada uma de suas portas.
CLI (Command Line Interface) - interface de linha de comando, ou seja, é preciso entrar manualmente via acesso remoto ou console, com as linhas de comando para configuração e operação do equipamento.
CST – Coordenadoria de Suporte Técnico.
DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) - Protocolo utilizado para atribuição dinâmica de endereços IP.
DHCP SNOOPING - configuração disponível em alguns switches Cisco que permite controlar o repasse de respostas a requisições de endereços IP via DHCP, repassando apenas aquelas provenientes de interfaces confiáveis.
Endereço IP - identificador único numa rede TCP/IP, conforme definido na RFC 791, página 23 e seguintes.
EXTRANET - segmentos de rede do TJPA, dedicado a conexão com redes de terceiros (Parceiros e Clientes).
Firewall - equipamento de rede cuja função é controlar o tráfego entre duas redes diferentes, estabelecendo regras para proteção do ambiente.
Gateway - combinação de hardware e software que permite a conexão entre duas ou mais redes.
GUI (Graphic User Interface) - interface gráfica do usuário - como o próprio nome diz, existe uma interface que fornece meios gráficos para configuração e operação do equipamento. Pode receber entradas gráficas e interpretar para linhas de comando, no caso da interface via browser dos routers ou ASDM do pix, ou operar somente como única interface de configuração e operação do equipamento, como por exemplo, o Checkpoint SMARTCONSOLE.
IEEE 802.1x - padrão que define um mecanismo de autenticação do ponto de acesso a uma rede local, impedindo o tráfego caso a autenticação falhe. Pode ser utilizado tanto em redes sem fio como em redes cabeadas.
Internet - segmentos de rede do TJPA, exclusivo para comunicações realizadas através da internet.
Intranet - segmentos de rede do TJPA, dedicado à comunicação interna do TJPA.

ISO (International Organization for Standardization) - Organização internacional de padronização.
MAC Address - endereço de 6(seis) bytes gravado em dispositivos de camada 2 padrão Ethernet.
Modelo OSI (Open System Interconnection) - modelo de 7 Camadas elaborado pela ISO que estabelece uma divisão de funções para a comunicação de dados.
MPAS (Matriz de Perfis de Acesso a Sistemas) - formulário padronizado que deve ser preenchido para mapeamento das funcionalidades do sistema e seus respectivos perfis de acesso.
MPLS (Multi Protocol Label Switching) - tecnologia de infraestrutura para roteamento de pacotes.
OSPF (Open Shortest Path First) - protocolo de roteamento de redes IP, que permite aos roteadores envolvidos informarem seu estado e qual o melhor caminho a ser roteado.
Plano de endereçamento IP - conjunto de regras e definições de toda a estrutura de endereço IP a ser utilizado na rede corporativa do TJPA.
Port Security - configuração de segurança em switches que limita o número de endereços MAC que podem ser associados a uma porta de switch.
Portas - dispositivos físicos ou lógicos para conexão de dados entre dois equipamentos.
Protocolo - conjunto de regras para a realização de comunicação entre dois dispositivos.
Protocolo Seguro - protocolo que embute, no mínimo, algum mecanismo de autenticação. Pode também incluir mecanismos de autorização e auditoria (accounting).
Protocolos de Infraestrutura - protocolos projetados para coordenação do funcionamento da rede com, por exemplo, protocolos de roteamento (RIP, OSPF, etc.), sincronização de horário (NTP), coordenação da camada 2 (STP, VTP...), controle de endereços (DHCP), serviço de nomes (DNS), MPLS.
RADIUS - (Remote Authentication Dial In User Service) - protocolo descrito pela RFC 2865 que implementa controle de acesso em conexões remotas.
RIP (Routing Information Protocol) - Protocolo de vetor de distância que usa contagem de saltos (hops) como métrica.
Roteador - equipamento especificamente projetado para direcionar tráfego de camada 3, para interligação de redes diferentes.
SCP (Secure Copy) - serviço baseado no SSH, utilizado para realizar transferência segura de arquivos.
SECINFO – Secretaria de Informática.
SFTP (SSH File Transfer Protocol) - protocolo para transferência segura, baseado no SSH.
SIR – Serviço de Infraestrutura de Rede.
SNMP (Simple Network Management Protocol) - protocolo utilizado para o gerenciamento remoto de dispositivos de redes.
SSH (Secure Shell) - o SSH faz parte da suíte de protocolos TCP/IP que torna segura a administração remota.

SSSB – Serviço Segurança de Sistemas Básicos.
Sub-Rede - divisão lógica do endereçamento de uma rede IP.
Switch - equipamento projetado para encaminhar tráfego de camada 2. Eventualmente pode ter capacidade de rotear tráfego de camada 3.
Switch de Acesso - equipamento de camada 2 especificamente projetado para permitir acesso de dispositivos de rede (estações de trabalho, impressoras, servidores etc.) à rede camada 3. Dividem-se entre aqueles capazes de realizar a conexão física com ou sem cabos (wired ou wireless).
TACACS+ (Terminal Access Controller Access-Control System Plus) - protocolo descrito pela RFC 1492 que implementa controle de acesso a ativos de rede, bem como autorização e contabilização de Comandos.
TJPA – Tribunal de Justiça do Estado do Par.
VLAN - mecanismo que permite a divisão lógica de uma rede.
VPN - Virtual Private Network - uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

8.1. CONTROLES DE ACESSO

8.1.1. Todos os ativos de rede, bem como todos os servidores que provêem serviços aos ativos de rede, devem estar instalados em local com controle de acesso físico.

8.1.2. Todos os equipamentos (gateways, switches, roteadores, concentradores de VPN, balanceadores de carga e firewalls) que fizerem uso da Rede TJPA para se comunicar, trocar, enviar ou receber informações ou dados, necessariamente deverão utilizar o protocolo TCP/IP.

8.2. REDES SEM FIO

8.2.1. Deve ser habilitada autenticação via protocolo 802.1x nos pontos de acesso, com certificado digital, para usuários e login e senha para equipamentos.

8.2.2. Os pontos de acesso sem uso devem ser desligados.

8.2.3. Deve haver mecanismo que identifique pontos de acesso não autorizados.

8.3. REDES COM FIO (CABEADA)

8.3.1. As portas de todos os switches de acesso que não estiverem sendo utilizadas devem ser desabilitadas.

8.3.2. CONFIGURAÇÃO

8.3.2.1. A configuração de todos os Switches e Roteadores de rede do TJPA deve ser feita de acordo com o documento “Regras Gerais de Configuração”.

8.3.2.2. Roteadores e Switches dos ambientes Extranet e Internet possuem plano de endereçamento IP diferenciado.

8.3.2.3. O acesso ao documento “Regras Gerais de Configuração” é restrito aos técnicos responsáveis pela administração, gerenciamento e manutenção dos equipamentos, portanto, um documento com grau de sigilo.

8.3.2.3.1. O acesso ao documento deve ser solicitado através de envio de solicitação para o SIR.

8.3.2.4. A configuração de endereçamento IP da Rede TJPA deve adotar os padrões de submáscaras, endereços IP e default gateways em conformidade com os critérios estabelecidos no

8.3.2.5. Os ambientes Extranet e Internet possuem planos de endereçamento IP diferenciado.

8.3.3. Todos os firewalls devem ser configurados de forma a não permitir a divulgação dos endereços IP das redes protegidas para uma interface de rede com menor nível de segurança.

8.3.4. Deve ser mantido o histórico das últimas três configurações realizadas em todos os ativos de rede.

8.3.5. Somente as estações de trabalho e telefones IP devem ser configuradas de forma a obter o endereço IP através de um servidor DHCP.

8.3.6. Nos gateways para redes externas ao TJPA, deve ser implementado filtro de pacotes que permita acesso somente aos serviços disponibilizados.

8.3.7. Equipamentos com funcionalidade de gateway de voz e dados não podem permitir que os canais de voz aceitem as requisições de dados, portanto, as interfaces configuradas para uso com sinalização de voz não serão utilizadas com sinalização voltada para transmissão de dados.

8.3.8. O campo “Descrição” das portas de acesso deve conter o nome lógico do equipamento que está conectado à porta.

8.4. CONTROLE DE IMPLEMENTAÇÃO DA REDE

8.4.1. Deve ser implementada tecnologia que permita definição de critérios de priorização do tráfego da rede (QoS) de acordo com sua relevância e após análise criteriosa e devidamente documentada.

8.4.1.1. O item anterior não se aplica ao ambiente Extranet e Internet.

8.4.2. Toda abertura de regra nos firewalls, deve ser documentada e arquivada na unidade responsável pela administração dos ativos, ficando a disposição por mais 01 ano após a exclusão da regra.

8.4.3. Deve ser utilizado protocolo seguro de transferência de arquivos, podendo ser o SFTP ou o SCP.

8.4.4. A utilização da ferramenta TERMINAL SERVICES deve ser implementada de forma segura com criptografia de dados.

8.4.5. O protocolo HTTP deve ser desabilitado em todos os roteadores e switches.

8.4.6. O protocolo TELNET deve ser desabilitado em todos os ativos de rede que suportem o protocolo SSH ou HTTPS.

8.4.7. A implementação de solução de criptografia deve ocorrer sempre que os dados trafegarem através da rede pública (internet), devendo ser realizado estudo prévio e documentado para cada caso.

8.5. CONTROLE DE RECURSOS DISPONÍVEIS NA REDE

8.5.1. Os protocolos de infraestrutura, listados a seguir, devem ser implementados de acordo com o documento “Regras Gerais de Configuração”, respeitando as características adicionais descritas abaixo:

8.5.1.1. LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol).

8.5.1.1.1. Os protocolos de autodescoberta devem ser desabilitados nas interfaces dos ativos de rede que fazem conexão com redes externas à Rede TJPA.

8.5.1.1.2. Deve ser desabilitado em todos os ativos de rede, devendo ser mantida documentação completa das conexões (topologias de rede) e ser atualizada sempre que ocorrer uma mudança no ambiente.

8.5.1.2. STP – Spanning Tree Protocol (CISCO Systems).

8.5.1.2.1. Deve ser implementado mecanismo que impeça a divulgação de BPDU falso na rede.

8.5.1.3. VTP – VLAN Trunking Protocol

8.5.1.3.1. Deve ser implementado VTP somente com proteção por senha.

8.5.1.4. ICMP – Internet Control Message Protocol

8.5.1.4.1. Não podem ser criadas regras para ICMP dos serviços protegidos por firewall, exceto para tráfego exclusivo de gerenciamento e administração da rede.

8.5.1.5. NTP – Network Time Protocol

8.5.1.5.1. Os horários dos ativos de rede devem ser sincronizados através da implementação deste protocolo, visando à garantia de autenticidade do servidor.

8.5.2. Os protocolos de roteamento devem ser implementados de acordo com o documento “Regras Gerais de Configuração”;

8.5.2.1. O protocolo RIP (Routing Information Protocol), não deve ser implementado em nenhum ativo de rede como protocolo de roteamento principal, por não prover métodos de autenticação.

8.5.3. A comunicação entre todos os ativos de rede deve ser autenticada por ferramenta específica para essa finalidade.

8.5.4. As interfaces de switches devem ser configuradas com limitação de broadcast, após análise criteriosa e documentada de cada segmento da rede local.

8.5.5. Todo ativo de rede deve estar instalado em rack e utilizar no-break.

8.5.6. No caso dos ativos com fontes redundantes, as ligações desses equipamentos deverão estar em circuitos elétricos independentes para redução dos impactos decorrentes de problemas ou manutenções na rede elétrica.

8.5.7. Todos ativos de rede devem estar operacionalmente disponíveis 24 horas por dia, 7 dias por semana, exceto durante o período de manutenção.

8.6. SEGREGAÇÃO DE AMBIENTES

8.6.1. A rede deve ser segmentada de forma que os ambientes de rede da produção, homologação e desenvolvimento sejam pelo menos segregados logicamente.

8.6.2. O espelhamento de portas de ativos, quando necessário, deverá ser realizado único e exclusivamente para:

8.6.2.1. Resolução de problemas relacionados ao funcionamento da rede e deve ser feita de forma absolutamente controlada.

8.6.2.2. Uso para gravação de chamadas em callcenter que utiliza tecnologia VOIP nas portas onde estão as entradas dos aparelhos e terminais telefônicos.

8.6.2.3. A equipe que identificar essas necessidades deverá preparar um documento de solicitação de Espelhamento de Porta de Switch e submeter à chefia da unidade responsável pela guarda do equipamento para a devida autorização.

8.6.3. É proibida a instalação de quaisquer dispositivos de monitoração de rede, hardware ou software, que não esteja previamente autorizado pela unidade responsável pela guarda dos equipamentos.

8.6.4. Todo cabeamento da rede deve ser estruturado, seguindo as normas técnicas vigentes.

8.7. SEGURANÇA

8.7.1. Todo acesso administrativo e remoto à CLI (Command Line Interface) de ativos de rede (como por exemplo: Switches, Roteadores, Firewalls e outros), deve ser realizado por meio do protocolo SSH, através de ferramenta homologada pelo TJPA.

8.7.2. Os acessos administrativos feitos por GUI (Graphic User Interface) devem implementar criptografia em seus protocolos de comunicação com o serviço administrado e devem estar devidamente homologados.

8.7.3. Os serviços TCP/IP desnecessários à funcionalidade do ambiente ou do equipamento devem ser desabilitados nos servidores, gateways, switches, roteadores e firewalls.

8.7.4. As contas e senhas locais dos fabricantes de todos os ativos de rede devem ser alteradas e guardadas em envelope lacrado no cofre da unidade tecnológica detentora dos equipamentos, ficando sua utilização sob responsabilidade da chefia da unidade.

8.7.4.1. Quando houver necessidade de abertura do envelope que contém a senha, devem ser seguidos os procedimentos formais para abertura do cofre da unidade e após a utilização da senha, esta deve ser alterada e guardada novamente no cofre, conforme subitem anterior.

8.7.4.2. Quando tratar-se de ativos de rede do Backbone do TJPA, a unidade responsável pela alteração e autorização de utilização das senhas locais é a CST.

8.7.5. A rede deve estar configurada de modo a garantir a prevenção de ataques do tipo DoS e DDoS.

8.7.5.1. Devem ser configurados nos switches e roteadores de toda a rede do TJPA, mecanismos que impeçam as seguintes formas de tentativa de ataque:

- ARP SPOOFING
- FLOODING DA TABELA ARP
- ENVENENAMENTO DA TABELA ARP
- IP SPOOFING
- M.I.T.M. (Man in the Middle)

8.8. CONTROLE DE ACESSO LÓGICO

8.8.1. Todos os ativos de rede devem ter controle de acesso lógico habilitado e administrado por ferramenta centralizada, específica para essa finalidade.

8.8.1.1. A ferramenta de controle de acesso lógico que trata o subitem anterior deve permitir a implementação de tecnologia de Autenticação, Autorização e Auditoria de eventos (AAA).

8.8.2. A ferramenta de controle de acesso de usuários aos ativos de rede deve ser habilitada para registrar LOG dos eventos abaixo relacionados com endereço de origem, data e hora do acesso:

- Sucesso de autenticação;
- Falha de autenticação;
- Comandos de administração e
- Tentativas não autorizadas.

8.8.3. O acesso lógico aos ativos de rede só deve ser permitido após autenticação do usuário.

8.8.4. O acesso à administração, gerenciamento e manutenção dos ativos de rede deve ser restrito aos técnicos.

8.8.5. Devem ser definidos perfis de acesso para cada usuário, seguindo o critério de classificação da informação definida pela SSSB.

8.8.6. Os sistemas operacionais que servirão de plataforma para os firewalls baseados em software, devem ter controle de acesso lógico, devendo ser habilitado registro de LOG de todos os acessos.

8.8.7. O ambiente IP deve possuir documentação atualizada e armazenada em local com controle de acesso na unidade responsável pela guarda dos equipamentos de rede, sendo classificada com grau de sigilo - Confidencial.

8.8.8. A geração de uma nova documentação do ambiente IP deve ser divulgada pelo chefe da unidade responsável pelo ambiente a todos os envolvidos na sua utilização.

8.8.9. O Plano de Endereçamento IP do TJPA deve ser seguido com rigor por todas as áreas responsáveis pela administração da rede IP.

8.8.10. O descarte dos documentos referentes ao ambiente IP deve ser feito pelo chefe da unidade responsável pelo ambiente, seguindo os critérios de classificação da informação.

8.9. ADMINISTRAÇÃO

8.9.1. A administração e gerenciamento dos ativos de rede devem ocorrer somente por técnicos autorizados formalmente pela unidade responsável pelos equipamentos.

8.9.2. No caso dos ativos de redes externas ao TJPA, a administração e gerenciamento devem ocorrer somente por técnicos autorizados formalmente pela unidade responsável e regidos por Acordo de Nível de Serviços (ANS) firmado entre as partes envolvidas, com as sanções previstas em contrato, além dos demais procedimentos legais cabíveis.

8.9.3. Deve ser mantida topologia atualizada de todas as conexões físicas da rede, de modo a permitir o mapeamento imediato dos ativos dentro do ambiente tecnológico do TJPA.

8.10. MANUTENÇÃO

8.10.1. A atualização de versões do sistema operacional e do software de gerenciamento dos ativos de rede deve ser executada após homologação pela SSSB.

8.10.2. A instalação e manutenção de ativos e serviços de rede devem seguir as recomendações descritas no normativo “RECURSOS TECNOLÓGICOS – DIMENSIONAMENTO, UTILIZAÇÃO, MANUTENÇÃO E CONSERVAÇÃO”.

8.10.3. As manutenções devem ser acompanhadas por empregado da respectiva área onde será realizada.

8.11. BACKUP

8.11.1. Deve ser realizado backup da configuração dos ativos de rede diariamente.

8.11.2. O Backup da configuração dos ativos fica restrito às unidades do TJPA responsáveis pelas operações de suporte e manutenção.

8.11.2.1. O Backup deve ser armazenado em servidores próprios e exclusivos, com acessos físicos e lógicos restritos.

8.11.2.2. O Backup da configuração dos ativos deve possuir contingência, preparado para assumir todas as funcionalidades no caso de falha do servidor principal.

8.11.3. Deve ser realizado backup dos logs dos ativos semanalmente, sendo guardado pela unidade tecnológica responsável com cópia em ambiente/localidade definido pela CST.

8.12. CONTINGÊNCIA

8.12.1. A contingência deve contemplar compatibilidade atualizada de versão de software e hardware.

8.12.2. Os procedimentos de contingência devem estar documentados de forma a permitir o pronto restabelecimento da operação de disponibilidade do ambiente IP.

8.12.3. O administrador da rede IP deve restaurar a situação do ambiente após a intervenção de contingência, de modo a manter a continuidade operacional.

8.12.4. A contingência das interligações de dados, dos equipamentos e seu acionamento nas unidades, devem ser definidos pelo SIR.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1. SSSB

9.1.1. Verificar periodicamente, novas versões de software de gerenciamento e sistema operacional, para homologação.

9.1.2. Avaliar e homologar recursos tecnológicos do ambiente IP.

9.1.3. Aprovar formalmente a utilização de aplicativos que compõem a solução de conectividade.

9.1.4. Definir os serviços prioritários e sua implementação

9.1.5. Definir ferramenta de acesso remoto.

9.1.6. Executar a atualização de versões do sistema operacional e do software de gerenciamento, após homologação e aprovação da CST.

9.2. SIR

9.2.1. Estabelecer critérios e indicadores de avaliação de desempenho do ambiente IP.

9.2.2. Divulgar novas versões do documento “Regras Gerais de Configuração”.
9.2.3. Definir e divulgar o Plano de Endereçamento IP.
9.2.4. Definir os protocolos que devem ser habilitados.
9.2.5. Definir os protocolos de gerenciamento e de roteamento que devem ser utilizados.
9.2.6. Definir o padrão e ferramentas de gerenciamento.
9.2.7. Definir a contingência das interligações de dados, dos equipamentos e seu acionamento nas unidades.
9.2.8. Definir o padrão de monitoração e auditoria dos registros de LOG de todos os ativos de rede do TJPA
9.2.9. Definir a ferramenta de controle de acesso lógico a todos os ativos de rede.
9.2.10. Definir padrão de manutenção periódica das contas e senhas de acesso lógico utilizadas.
9.2.11. Definir ambiente externo onde deve ser guardado o backup das configurações dos ativos.
9.2.12. Definir níveis de acesso lógico aos roteadores.
9.2.13. Definir níveis de acesso lógico aos ativos de rede.
9.2.14. Definir as diretrizes quanto à criação de listas de controle de acessos, pertinentes aos requisitos de segurança da informação, a serem cadastrados nos roteadores.
9.2.15. Elaborar as regras de configurações e níveis de acesso lógico dos ativos de rede;
9.2.16. Administração dos circuitos Internet, intranet e Backbone.
9.2.17. Elaborar o Plano de Endereçamento IP;
9.2.18. Analisar periodicamente os arquivos de log dos ativos de rede quanto ao acesso lógico, por meio de ferramenta de software.
9.2.19. Realizar teste de restauração de backup periodicamente e fora do ambiente de produção.
9.2.20. Alterar a senha local dos ativos de rede que compõe o Backbone, quando utilizada.
9.2.21. Atuar em todos os ativos da rede de acesso do TJPA;
9.2.22. Realizar manutenção, gerenciamento da rede dos circuitos integrantes da rede de acesso.
9.2.23. Habilitar controle de acesso lógico em todos os ativos.
9.2.24. Configurar os ativos conforme documento “Regras Gerais de Configuração”.
9.2.25. Configurar todos os ativos de rede conforme Plano de Endereçamento IP.
9.2.26. Configurar as rotas e os filtros de pacotes.
9.2.27. Configurar os serviços prioritários.

9.2.28. Habilitar somente os protocolos definidos.
9.2.29. Habilitar os protocolos de roteamento e gerenciamento definidos.
9.2.30. Habilitar o protocolo de roteamento somente nos roteadores definidos.
9.2.31. Manter backup das últimas 3 configurações dos ativos de rede, guardando-o em local seguro.
9.2.32. Realizar backup da configuração dos ativos imediatamente após a instalação e a cada alteração em sua configuração.
9.2.33. Guardar o backup da configuração dos roteadores em local seguro na unidade onde os mesmos estão instalados e em ambiente externo.
9.2.34. Instalar os ativos em rack e utilizar no-break.
9.2.35. Realizar o inventário dos ativos de rede;
9.2.36. Alterar as senhas, padrão do fornecedor, das contas de acesso à administração, gerenciamento e manutenção dos ativos sob sua responsabilidade.
9.2.37. Definir os técnicos responsáveis pela administração, gerenciamento e manutenção dos ativos de rede.
9.2.38. Manter os ativos de rede operacionalmente disponíveis 24 horas por dia, 7 dias por semana, exceto durante o período de manutenção.
9.2.39. Treinar e capacitar periodicamente, os técnicos responsáveis pela administração, gerenciamento e manutenção dos ativos de rede.
9.2.40. Realizar manutenção preventiva.
9.3. ADMINISTRADOR DO AMBIENTE IP
9.3.1. Equipe com pessoal qualificado para prover adequação e administração do ambiente TCP/IP, conforme sua área de atuação: (SIR e SSSB).
9.3.2. Manter a disponibilidade de todos os ativos de rede sob sua responsabilidade.
9.3.3. Manter a disponibilidade dos arquivos de LOG de todos os ativos de rede.
9.3.4. Restaurar a situação operacional dos ativos após a intervenção de contingência.
9.3.5. Acompanhar visitantes, técnicos de manutenção e outros empregados do TJPA durante permanência no ambiente físico dos ativos.
9.3.6. Documentar e atualizar a configuração do ambiente IP.
9.3.7. Guardar a documentação do ambiente IP em local seguro.
9.3.8. Avaliar periodicamente a configuração padrão a ser utilizada nos ativos e propor atualizações.
9.4. CHEFIA DA UNIDADE TECNOLÓGICA DETENTORA DOS EQUIPAMENTOS
9.4.1. Guardar a chave de acesso ao ambiente físico onde estão instalados os ativos de rede.

9.4.2. Custodiar os equipamentos de tecnologia localizados na unidade.

9.4.3. Determinar a execução de varredura física em todo o cabeamento do ambiente em busca de dispositivos conectados e não autorizados.

10. PROCEDIMENTOS

Não se aplica.

11. RELATÓRIOS GERENCIAIS E INDICADORES

11.1. Deve ser implementado o protocolo SNMP de gerência, em todos os switches e roteadores, na versão mais atualizada, compatível com as ferramentas de gerenciamento de redes.

11.2. Deve ser habilitado serviço de LOG em todos os ativos de rede, sendo que os servidores de armazenamento devem estar localizados na própria unidade tecnológica responsável pelo suporte aos equipamentos.

11.3. Devem ser utilizados os recursos de monitoração de disponibilidade, de desempenho e de segurança do ambiente IP.

11.4. Deve haver processo de análise das informações geradas pelos serviços de LOG que permita a identificação, correção e registro imediato dos problemas no ambiente, para que sejam tomadas ações visando sua solução.

11.5. Todos os ativos de rede devem ser monitorados por ferramenta homologada pelo TJPA e específica para essa finalidade.

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos. Demais esclarecimentos devem ser dirigidos ao Secretaria de Informática.