RESOLUÇÃO Nº. 72, DE 21 DE SETEMBRO DE 2009.

Regulamenta a Política de Segurança da Informação no que se refere à utilização da Tecnologia da Informação e Comunicação pelos técnicos dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.

A SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO, no uso das atribuições que lhe conferem o artigo 93, SS 1º, inciso III, da Constituição do Estado, o artigo 2º, inciso X, da Lei Delegada nº. 126, de 25 de janeiro de 2007 e o artigo 16, do Decreto nº 44.998, de 30 de dezembro de 2008.

RESOLVE:

CAPÍTULO I - DAS DISPOSIÇÕES PRELIMINARES

Seção I

DISPOSIÇÕES PRELIMINARES

Art. 1º A padronização de estações de trabalho, a administração de firewall, a administração de roteadores e switches, a administração de servidores, a administração de rede wireless, a administração do IDS/IPS e a administração de backup no âmbito dos órgãos e entidades do Governo do Estado de Minas Gerais observam o disposto nesta Resolução.

Art. 2º Esta Resolução se aplica a todos os usuários dos órgãos e entidades do Governo do Estado de Minas Gerais.

Seção II

DAS DEFINIÇÕES

Art. 3º Para os fins desta Resolução, considera-se:

I - access point (ponto de acesso): dispositivo que atua como ponte entre uma rede sem fio e uma rede cabeada;

II - acesso remoto: conexão à distância entre um dispositivo isolado (terminal ou microcomputador) e uma rede;

III - administrador: contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

IV - análise de riscos: processo completo de análise e avaliação de riscos;

V - antispyware: programa que permite identificar e remover códigos maliciosos que se auto-instalam nos computadores;

VI - antivírus: programa que permite identificar e eliminar vírus em computadores;

VII - autenticação: mecanismo de comprovação da identidade do usuário;

VIII - autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui, certificada por instrumento ou testemunho público;

IX - backup: cópia de segurança de dados feita para salvaguardar arquivos;

X - cavalo de Tróia: programa de computador com utilidade aparente ou real que contém funções escondidas e adicionais, explorando secretamente as informações armazenadas e provocando perda da segurança da Informação;

XI - certificado digital: arquivo eletrônico, assinado digitalmente por uma Autoridade Certificadora, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. O certificado digital é armazenado em uma mídia ou em um dispositivo de hardware;

XII - chat: palavra que em português significa "conversação" e é um neologismo para designar aplicações de conversação em "tempo real";

XIII - chefia imediata: titular da área a qual está subordinado o usuário. Na sua ausência deve ser observada a ordem hierárquica superior;

XIV - confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;

XV - contas: código de acesso atribuído a cada usuário. A cada conta é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis;

XVI - contramedida: vide "controle";

XVII - 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;

XVIII - correio eletrônico: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;

XIX - crachá: identificação, pessoal e intransferível, disponibilizada ao usuário para acesso físico às dependências do órgão ou entidade;

XX - criptografia: ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, por meio de um processo de cifragem e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem;

XXI - diretrizes: regras de alto nível que representam os princípios básicos que a Organização resolveu incorporar a sua gestão de acordo com a visão estratégica da alta direção. Servem como base para que as normas e os procedimentos sejam criados e detalhados;

XXII - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes;

XXIII - domínio: identificação de nomes da Internet, utilizada para prover o acesso a endereços de computador, a qualquer programa de comunicação;

XXIV - download: transferência de um arquivo de outro computador para outro computador, por meio da Internet;

XXV - e-mail: vide "correio eletrônico";

XXVI - equipamentos móveis: equipamentos com capacidade de armazenamento e processamento de dados e de fácil locomoção, interligados, ou não, à rede corporativa do órgão ou entidade, tais como notebooks e Personal Digital Assistants (PDAs);

XXVII - estação de trabalho: computadores, notebooks e PDAs do órgão ou entidade interligados ou não na rede corporativa;

XXVIII - ferramenta de auditoria: software que armazena os eventos gerados no ambiente computacional, permitindo a rastreabilidade da configuração e da utilização dos sistemas;

XXIX - hardware: todo e qualquer dispositivo físico em um computador;

XXX - hotfix(es): vide patch(es);

XXXI - IDS (Intrusion Detection System): sistema de detecção de intrusão que permite identificar atividades suspeitas na rede;

XXXII - IPS (Intrusion Prevention System): sistema de prevenção de ataques que permite que atividades suspeitas na rede sejam bloqueadas de forma preventiva;

XXXIII - incidente de Segurança da Informação: um ou mais eventos de segurança da informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XXXIV - integridade: salvaguarda da exatidão e completeza da informação;

XXXV - internet: rede mundial de computadores;

XXXVI - intranet: rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os usuários possam acessar as informações dos seus respectivos Órgãos Públicos;

XXXVII - licença de software: direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes;

XXXVIII - log: arquivos que contenham informações sobre eventos de qualquer natureza em um sistema computacional com o objetivo de permitir o rastreamento de atividades;

XXXIX - login: identificação do usuário para acesso aos sistemas e serviços;

XL - logon: processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema;

XLI - logout: processo de saída de um usuário dos sistemas e serviços;

XLII - mecanismos de segurança: recursos utilizados para proteger arquivos de acessos indevidos;

XLIII - mídias: meio físico utilizado para armazenar dados;

XLIV - modem: equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações;

XLV - normas: especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégica definida nas diretrizes;

XLVI - órgão público: qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas;

XLVII - Patch(es) - é um programa criado para atualizar ou corrigir um software.

XLVIII - Peer-to-Peer ou P2P (Ponto a Ponto): tecnologia que possibilita a distribuição de arquivos em rede e que tem como característica permitir o acesso de qualquer usuário desta a um nó, ou a outro usuário (peer) de forma direta;

XLIX - política de segurança: conjunto de definições, diretrizes, restrições e requisitos que servem para nortear o uso de boas práticas no trato com os ambientes, recursos e ativos computacionais, em aspectos físicos, lógicos e de pessoal, com a finalidade de proporcionar maior segurança às informações;

L - procedimentos: detalham no plano operacional configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas;

LI - proteção: vide "controle";

LII - recursos computacionais recursos tecnológicos que suportam as informações do órgão ou entidade;

LIII - rede corporativa: computadores e outros dispositivos interligados que compartilham informações ou recursos do órgão ou entidade;

LIV - restore: recuperação de dados armazenados em cópias de segurança;

LV - risco: combinação da probabilidade de um evento e de suas conseqüências;

LVI - segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, legalidade e confiabilidade, podem também estar envolvidas;

LVII - senha: conjunto de caracteres utilizado para permitir a validação da identidade do usuário, a fim de tornar possível seu acesso a um sistema de informação ou serviço de uso restrito;

LVIII - serviço: ferramenta de trabalho, como correio eletrônico e acesso à Internet e intranet, disponibilizada na rede do órgão ou entidade;

LIX - servidor: computador responsável pelo compartilhamento de recursos e execução de serviços solicitados pelos demais computadores a ele conectados;

LX - sistema: vide "sistema de informação automatizado";

LXI - sistema de informação automatizado: conjunto de programas empregado para coletar, processar, transmitir e disseminar dados que representam informação para o usuário. Nesta Resolução será empregada a palavra sistema com o sentido de sistema de informação automatizado;

LXII - sistema operacional: programa ou conjunto de programas que responde pelo controle da alocação dos recursos do computador;

LXIII - site: vide "sítio";

LXIV - sítio: local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia;

LXV - software: programa de computador;

LXVI - software de comunicação instantânea: aplicação que permite o envio e recebimento de mensagens de texto em instantes;

LXVII - spam: mensagem de correio eletrônico não solicitada, enviada em larga escala para uma lista de e-mails, fóruns ou grupos de discussão;

LXVIII - spyware: programa espião que monitora a atividade de um computador podendo transmitir estas informações a um receptor na Internet;

LXIX - streaming: tecnologia que permite o envio de informação multimídia (áudio e vídeo) por meio de pacotes, utilizando redes de computadores, sobretudo a Internet;

LXX - terceiro: pessoa jurídica ou física contratada pelo órgão ou entidade para realizar serviços;

LXXI - trilha de auditoria: histórico das transações dos sistemas contendo registro dos usuários que as efetuaram e das tentativas de acesso indevido;

LXXII - unidade administrativa: cada área que compõe a estrutura organizacional do órgão ou entidade;

LXXIII - upload: transferência de um arquivo, de qualquer natureza, do computador do usuário, para algum equipamento da Internet;

LXXIV - URL (Universal Resource Locator): link ou endereço de uma página web;

LXXV - userid: identificação do usuário no recurso computacional;

LXXVI - usuário: todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em Órgão ou Entidade da Administração Pública Estadual direta ou indireta;

LXXVII - vírus: programa desenvolvido com intenção nociva que, se inserido em um computador, pode causar queda do seu desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos;

LXXVIII - VPN (Virtual Private Network) - forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infra-estrutura as redes públicas, tal como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação;

LXXIX - webmail: interface web do correio eletrônico;

LXXX - wireless: sistema de comunicação que não requer fios para transportar sinais; e

LXXXI - worms: programa ou algoritmo que replica a si próprio através da rede e, normalmente, executa ações maliciosas, tais quais utilizar os recursos computacionais, podendo fazer com que a máquina fique indisponível.

CAPÍTULO II - DA PADRONIZAÇÃO DE ESTAÇÕES DE TRABALHO

Art. 4º Inventário (hardware e software) atualizado e automatizado das estações de trabalho dos órgãos e entidades do Governo do Estado deve ser mantido pelo setor competente.

Art. 5º Todos os equipamentos de informática, alugados e emprestados, devem ser identificados conforme legislação em vigor.

Parágrafo Único. Todas as estações de trabalho devem ser patrimoniadas. O número do patrimônio deve ser parte da identificação lógica do equipamento.

Art. 6º Todas as estações de trabalho devem ter lacres nas tampas de acesso ao interior das mesmas, que só podem ser manipulados ou removidos pela área de TIC ou pelo responsável por realização de manutenção nas estações de trabalho.

Art. 7º A habilitação de portas de comunicação e a instalação de periféricos nas estações de trabalho devem ser realizadas considerando as necessidades específicas das atividades do usuário, mediante justificativa e com avaliação da área de TIC.

Art. 8º Somente softwares homologados pela área de TIC devem ser instalados nas estações de trabalho.

Art. 09º Toda estação de trabalho deve ter antivírus instalado, ativado e atualizado.

Art. 10. As últimas versões de correções liberadas pelo fabricante do sistema operacional devem ser instaladas nas estações de trabalho.

Art. 11. As identificações com perfil de convidado devem ser desabilitadas nas estações de trabalho.

Art. 12. Sempre que existir o recurso, o sistema operacional deve ser configurado para:

I - exigir autenticação dos usuários;

II - impedir instalação e desinstalação de software pelo usuário;

III - ativar o bloqueio da estação de trabalho após o período de inatividade estabelecido; e

IV - configurar a geração de log de segurança, registrando, no mínimo, logon e logout válidos e inválidos.

Art. 13. Deve-se utilizar a ferramenta de geração de imagem das estações de trabalho na manutenção e na instalação de novos equipamentos, causando, assim, o mínimo de indisponibilidade dos equipamentos.

Art. 14. A configuração de rede das estações de trabalho deve ser alterada quando for necessário realizar manutenções externas.

Art. 15. Quando necessário, o descarte de HDs deve ser feito conforme procedimento específico.

Art. 16. As estações de trabalho devem ser instaladas, autorizadas, homologadas e configuradas de acordo com os padrões e perfis

definidos para cada área sendo os mesmos estabelecidos pela área de TIC em conjunto com a área de Segurança da Informação. Somente essas estações podem ser utilizadas a serviço do órgão ou entidade e/ou em uso em seu espaço físico.

CAPÍTULO III - DA ADMINISTRAÇÃO DE FIREWALL

Seção I

DISPOSIÇÕES PRELIMINARES

Art. 17. Toda manutenção nos firewalls deve ser documentada.

Art. 18. Um serviço configurado de forma idêntica ao ambiente de Produção, para efeito de contingência, deve ser mantido, nos casos em que o recurso de clusterização não estiver em uso.

Art. 19. Realizar um backup diário automaticamente das rotas e das configurações das interfaces dos módulos barreira.

Seção II

DA INFRAESTRUTURA DE FIREWALL

Art. 20. Os equipamentos de hardware de firewall considerados críticos pela área de Segurança da Informação devem estar instalados em um local de acesso físico restrito e a infraestrutura física deve estar de acordo com as recomendações do fabricante do hardware e com as demais normas aplicáveis.

Art. 21. O hardware e o software utilizados para o firewall devem ser homologados pela área de TIC em conjunto com a área de Segurança da Informação.

Art. 22. Todo hardware desnecessário ao funcionamento da configuração definida para o firewall, tais como portas USB, PS2, placas de fax-modem, entre outros, deve ser desabilitado.

Art. 23. Senhas para o setup e para o boot do equipamento devem ser configuradas, sendo estas de conhecimento apenas da área TIC.

Art. 24. O boot do firewall deve ser realizado somente pelo dispositivo de armazenamento interno.

Art. 25. Deve ser mantido um ambiente de teste devidamente documentado para avaliação de impactos decorrentes de alterações na configuração, de manutenções e instalações de software e de hardware. As exceções devem ser autorizadas pela área de

Segurança da Informação, após análise de risco devidamente documentada.

Art. 26. As últimas versões de correções liberadas pelos fabricantes do firewall e do sistema operacional devem ser instaladas no ambiente de produção, observando a disposição citada no tópico anterior, conforme procedimento específico.

Art. 27. O sistema de arquivos recomendado pelo fabricante do sistema operacional deve ser utilizado.

Seção III

DA CONFIGURAÇÃO DO FIREWALL

Art. 28. O firewall deve prover apenas serviços necessários ao seu funcionamento, tais como filtragem de pacotes, protocolos e portas, VPN, entre outros. As exceções devem ser autorizadas pela área de Segurança da Informação, após análise de risco e devidamente documentada.

Art. 29. O firewall deve ser acessado somente para tarefas administrativas e liberado somente para IPs pré-definidos.

Art. 30. A realização de manutenções e a inclusão de novas regras devem estar de acordo com procedimento específico.

Art. 31. Todos os serviços que não sejam utilizados pelo firewall devem ser desabilitados.

Art. 32. A funcionalidade auto-run do sistema operacional deve ser desabilitada.

Art. 33. Somente os protocolos estritamente necessários ao funcionamento do firewall devem ser habilitados em suas interfaces de rede.

Art. 34. O servidor de firewall deve ser configurado para sincronizar o horário com um servidor de NTP (Network Time Protocol) adotado pelo órgão ou entidade.

Art. 35. Os logs de dados do sistema operacional devem ser habilitados e devem ser armazenados por pelo menos 3 (três) anos.

Seção IV

DAS REGRAS DE FIREWALL

Art. 36. A inclusão, exclusão e modificação de regras no firewall devem ser realizadas mediante procedimento específico. As regras criadas devem ser comentadas.

Art. 37. A documentação das configurações do firewall deve ser mantida atualizada e seu acesso restrito à área de TIC e à área de Segurança da Informação.

Art. 38. Os logs de dados gerados pelo firewall devem ser armazenados em partição/filesystem diferentes do sistema operacional.

Art. 39. Os logs de dados de tráfego gerados pelo firewall devem ser consolidados em banco de dados, conforme procedimento específico.

Art. 40. Todos os logs de dados devem ser verificados diariamente, pela área de TIC.

Art. 41. A performance das aplicações de firewall deve ser monitorada periodicamente.

Art. 42. Os controles existentes na ferramenta de análise de riscos adotada pelo órgão ou entidade devem ser aplicados e avaliados no máximo anualmente. As correções dos controles considerados de alta criticidade devem ser realizadas, após deliberação conjunta das áreas de TIC e de Segurança da Informação.

CAPÍTULO IV - ADMINISTRAÇÃO DE ROTEADORES E SWITCHES

Seção I

DA CONFIGURAÇÃO E INSTALAÇÃO

Art. 43. Os equipamentos e os softwares dos roteadores e dos switches no órgão ou entidade devem ser homologados pela área de TIC.

Art. 44. Os roteadores e os switches devem ser instalados em um local de acesso físico restrito, autorizado somente aos analistas de suporte da área de TIC.

Art. 45. A entrada e saída de usuários às salas onde os roteadores e switches estão instalados devem ser registradas e controladas de acordo com procedimentos específicos.

Art. 46. Os roteadores e switches devem ser administrados remotamente somente por estações de trabalho pré-definidas e os acessos as mesmas deve ser restrito e controlado.

Art. 47. As configurações dos roteadores e dos switches, administrados pelo órgão ou entidade, devem ser documentadas, atualizadas e armazenadas em locais restritos aos administradores da rede.

Art. 48. Toda alteração de configuração nos roteadores deve ser realizada somente após a realização de backup das configurações ativas.

Art. 49. Para toda alteração que gerar impacto, conforme análise de risco, deve ser realizado em ambiente de teste antes de sua alteração.

Art. 50. A última versão de correções liberadas para os softwares dos roteadores e switches devem ser instaladas observando a disposição citada no tópico anterior.

Art. 51. Todos os serviços desnecessários para administração remota dos roteadores e switches devem ser desabilitados

Art. 52. Somente os protocolos necessários ao funcionamento da rede corporativa devem ser configurados. Os protocolos não utilizados devem ser retirados da configuração.

Seção II

DO CONTROLE DE ACESSO

Art. 53. O acesso ao roteador e ao switch deve ser realizado somente por meio de login e senha pessoal e intransferível.

Art. 54. A concessão de acesso deve seguir procedimento específico.

Art. 55. A criação de identificações de acesso com privilégios administrativos deve ser restrita, controlada e concedida apenas a usuários que necessitem deste direito para a realização de suas atividades profissionais de suporte ao equipamento.

Art. 56. Devem ser criadas logins com acesso somente à leitura para fins de auditoria.

Seção III

DA ESPECIFICAÇÕES DE FILTRAGENS

Art. 57. Os roteadores e switches não devem enviar pacotes dos protocolos de roteamento e de redundância para interfaces ou portas que estejam ligadas a servidores e estações de trabalho.

Art. 58. O filtro anti-spoofing deve ser configurado nos roteadores e switches considerados críticos pela área de TIC, quando existir este recurso nos equipamentos.

Art. 59. Utilizar os serviços ACL (Access Control List) para restringir acessos.

Seção IV

DO MONITORAMENTO

Art. 60. Todos os roteadores e switches devem ter habilitados logs que permitam a auditoria de configuração e seu backup deve ser guardado por pelo menos 3 (três) anos.

Art. 61. Os logs gerados pelos roteadores e pelos switches, com as devidas proteções de acesso ao conteúdo das informações registradas, devem ser armazenados em servidores de logs.

Art. 62. Os registros de logs gerados devem ser auditados, no máximo, a cada 12 (doze) meses pela área de Segurança da Informação.

Art. 63. Os controles existentes na ferramenta de análise de riscos adotada pelo órgão ou entidade devem ser aplicados e avaliados no máximo anualmente. As correções dos controles considerados de alta criticidade devem ser realizadas, após deliberação conjunta da áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação.

Seção V

DA SEGURANÇA

Art. 64. O backup da configuração dos roteadores e dos switches deve seguir procedimento específico.

CAPÍTULO V - ADMINISTRAÇÃO DE SERVIDORES

Seção I

DAS DISPOSIÇÕES PRELIMINARES

Art. 65. Todos os servidores do órgão ou entidade devem ser identificados com placa de patrimônio e identificação lógica única.

Art. 66. Um ambiente de teste com arquitetura idêntica ao ambiente de produção, devidamente documentado, deve ser mantido para

simulação e avaliação de impactos decorrentes de manutenções, da instalação de dispositivos, patches, upgrades e hotfixes nos servidores em produção e em seus sistemas e programas de computador.

Art. 67. As últimas versões de correções devem ser instaladas observando a disposição citada no item acima.

Art. 68. Deve ser mantida documentação atualizada, dos servidores do órgão ou entidade, contendo características do hardware, sistema operacional, utilitários, aplicativos e serviços disponibilizados, parâmetros de configuração, endereço IP, MAC e usuários responsáveis pela administração. A documentação dos servidores do órgão ou entidade deve ser protegida e seu acesso restrito à área de TIC.

Art. 69. Todos os servidores do órgão ou entidade devem possuir contratos de manutenção, quando fora do período de garantia.

Seção II

DO ACESSO FÍSICO

Art. 70. As instalações dos servidores do órgão ou entidade devem considerar a segurança física quanto à localização, cabeamento, controle de temperatura, rede elétrica e combate a incêndio, e devem observar o cumprimento dos padrões de segurança do trabalho, recomendações dos parceiros e normas técnicas emanadas dos órgãos competentes.

Art. 71. Todos os servidores do órgão ou entidade devem ser instalados em ambiente físico segregado e restrito a seus usuários administradores e a pessoas autorizadas pela área de TIC.

Art. 72. A entrada e a saída de usuários das salas de servidores do órgão ou entidade devem ser registradas e arquivadas para fins de auditoria.

Art. 73. Atividades realizadas por terceiros nas salas de servidores do órgão ou entidade devem ser autorizadas e acompanhadas pela área de TIC.

Art. 74. Atividades realizadas pelo pessoal dos serviços gerais devem ser acompanhadas por um técnico da área de TIC.

Seção III

DAS CONFIGURAÇÕES

Art. 75. Nos servidores do órgão ou entidade devem ser instalados somente aplicativos e serviços necessários às suas finalidades.

Art. 76. Ativar o bloqueio do console do servidor após o período de inatividade estabelecido.

Art. 77. Todas as conexões anônimas devem ser bloqueadas.

Art. 78. Para servidores de arquivos, um limite de utilização de espaço em disco para os usuários deve ser definido e configurado.

Art. 79. Todos os servidores deverão ter um antivírus instalado, atualizado e ativado.

Art. 80. Todo recurso disponível nos servidores deve ser monitorado e sua utilização acompanhada pela área de TIC.

Art. 81. Todos os softwares instalados nos servidores do órgão ou entidade devem ser homologados pela área de TIC, observando os direitos autorais.

Art. 82. Os servidores do órgão ou entidade devem ser configurados para sincronizar o relógio com servidor de NTP (Network Time Protocol) do órgão ou entidade.

Art. 83. A identificação de acesso dos usuários "convidado/guest" e demais usuários que venham definidos pelo fabricante desnecessários para o sistema, devem ser bloqueados.

Art. 84. Todos os servidores devem ter backups periódicos, conforme procedimento específico.

Art. 85. As configurações dos sistemas operacionais devem ser protegidas e seu acesso restrito e controlado.

Art. 86. As permissões de acesso aos arquivos e diretórios compartilhados devem ser protegidas com senhas.

Art. 87. A criação de identificações de acesso com privilégios administrativos deve ser restrita, controlada e concedida apenas a usuários que necessitem deste direito para a realização de suas atividades profissionais de suporte ao equipamento.

Seção IV

DAS TRILHAS DE AUDITORIA

Art. 88. Todos os servidores do órgão ou entidade devem ter logs de acesso habilitados e demais logs implementadas de acordo com as necessidades de cada serviço disponível no servidor.

Parágrafo Único. Os logs dos servidores devem ser analisados periodicamente, por meio de procedimento automatizado, pela área de TIC.

CAPÍTULO VI - DA ADMINISTRAÇÃO DE REDE WIRELESS

Seção I

DAS DISPOSIÇÕES PRELIMINARES

Art. 89. A rede wireless, disponibilizada no órgão ou entidade, deve utilizar access point.

Art. 90. Somente hardwares e softwares homologados pela área de TIC podem ser utilizados na rede wireless.

Seção II

DA INSTALAÇÃO FÍSICA

Art. 91. As instalações dos equipamentos access point devem considerar a segurança física quanto à localização, cabeamento estruturado e rede elétrica.

Art. 92. A área de abrangência da rede wireless deve ser testada no momento da instalação de novos equipamentos access point.

Art. 93. Os controles existentes na ferramenta de análise de riscos adotada pelo órgão ou entidade devem ser aplicados e avaliados no máximo anualmente. As correções dos controles considerados de alta criticidade devem ser realizadas, após deliberação conjunta da áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação.

Seção III

DA CONFIGURAÇÃO

Art. 94. O acesso para configuração do access point, via rede wireless, deve ser desabilitado. A administração do access point da rede wireless deve ser realizada somente por meio da rede cabeada.

Art. 95. A rede deve ser configurada com segurança por obscuridade (mecanismo utilizado para ocultar as configurações da rede quando do acesso e tentativa de captura).

Art. 96. O access point deve ser configurado em modo ponte (bridge).

Art. 97. Os endereços IPs e MAC dos access points, configurados por padrão pelos fabricantes, devem ser modificados na instalação da rede quando o equipamento tiver o recurso.

Art. 98. Uma faixa de endereços IP deve ser previamente definida para utilização na rede wireless.

Art. 99. Os endereços MAC das estações de trabalho devem ser associados ao endereço IP disponibilizado para o usuário.

Seção IV

DOS MECANISMOS DE SEGURANÇA

Art. 100. Toda comunicação realizada pela rede wireless deve utilizar criptografia.

Art. 101. Ferramentas de segurança como firewall, IDS/IPS, antivírus, antispyware devem ser instaladas no servidor interligado, via cabo, ao access point.

Seção V

DO MONITORAMENTO/TRILHAS DE AUDITORIA

Art. 102. Os logs de acesso aos serviços e sistemas do órgão ou entidade, via rede wireless, devem ser habilitados, contendo, no mínimo, endereço IP, endereço MAC, login do usuário, logon e logout, válidos e inválidos, data e hora de entrada e saída. Os logs devem ser verificados periodicamente.

Art. 103. As informações geradas pelo sistema de detecção de intrusão devem ser analisadas periodicamente.

Seção VI

DA MANUTENÇÃO

Art. 104. A configuração dos equipamentos access point deve ser eliminada quando for necessário o seu envio para manutenções externas ou quando o equipamento for desativado.

Seção VII

DA DOCUMENTAÇÃO

Art. 105. Uma documentação atualizada das configurações da rede wireless deve ser mantida, contendo no mínimo equipamentos, fabricantes, endereço MAC, endereço IP e usuários administradores.

Art. 106. O acesso à documentação da rede wireless deve ser restrito aos usuários administradores.

CAPÍTULO VII - DA ADMINISTRAÇÃO DO IDS/IPS

Seção I

DA INFRAESTRUTURA

Art. 107. Todo hardware e/ou software utilizados para o IDS/IPS devem ser homologados pela área de TIC (network IDS/IPS) em conjunto com a área responsável pela Segurança da Informação.

Art. 108. Senhas para o setup e para o boot do equipamento devem ser configuradas, sendo estas senhas de conhecimento apenas da área de TIC.

Art. 109. O boot do IDS/IPS deve ser realizado somente pelo dispositivo de armazenamento interno.

Art. 110. Deve ser mantido um ambiente de teste devidamente documentado para avaliação de impactos decorrentes de alterações na configuração, de manutenções de assinaturas, de software e de hardware. As exceções devem ser autorizadas pela área responsável pela Segurança da Informação, após análise de risco devidamente documentada.

Art. 111. A instalação das últimas correções e as atualizações de assinaturas de software e hardware devem ser realizadas no ambiente de produção, observando a disposição citada no tópico anterior, conforme procedimento específico.

Art. 112. O backup das configurações dos IDS/IPS deve seguir o procedimento específico.

Art. 113. HOSTS IDS devem ser instalados nos servidores determinados pela área de TIC, após a realização de uma análise de riscos.

Art. 114. A área responsável pela Segurança da Informação deve homologar a instalação de HOST IDS.

Art. 115. Os hardwares do network IDS/IPS, considerados críticos pela área responsável pela Segurança de Informação, devem estar instalados em um local de acesso físico restrito e a infra-estrutura física deve estar de acordo com as recomendações do fabricante do hardware e com as demais normas aplicáveis.

Art. 116. Todo hardware desnecessário ao funcionamento do network IDS/IPS, tais como portas USB, PS2, placas de fax-modem, entre outros, deve ser desabilitado.

Art. 117. A localização do network IDS/IPS na rede deve ser determinada a partir de uma análise de risco realizada pela área responsável pela Segurança da Informação.

Seção II

DA ADMINISTRAÇÃO

Art. 118. O network IDS/IPS deve ser acessado somente para tarefas de administração e o acesso liberado somente para IPs pré-definidos.

Art. 119. A criação de login com privilégios de administrador nos networks IDS/IPS deve seguir os seguintes critérios:

I - todo login deve ser autorizado pela área responsável pela Segurança da Informação;

II - A quantidade de login deve ser limitada a um número restrito de funcionários da área de TIC;

III - concessão restrita a funcionários da área de TIC que necessitem destas permissões para execução de suas atividades profissionais; e

IV - os parâmetros para criação e gerenciamento das senhas devem seguir a norma "Acesso Lógico e Utilização de Senhas".

Art. 120. A senha do login, criada por padrão na instalação do network IDS/IPS, deve ser alterada e de conhecimento somente da área de TIC.

Art. 121. A senha do login, criada por padrão na instalação do HOST IDS, deve ser alterada e de conhecimento somente da área de Suporte Técnico.

Seção III

DA CONFIGURAÇÃO

Art. 122. O IDS/IPS deve ser configurado para sincronizar o horário com um servidor de NTP (Network Time Protocol) adotado pelo órgão ou entidade.

Art. 123. Todos os serviços dos networks IDS/IPS que não sejam necessários devem ser desabilitados.

Art. 124. Somente os protocolos estritamente necessários ao funcionamento dos networks IDS/IPS devem ser habilitados.

Art. 125. Network IDS/IPS instalado em servidor:

I - deve ser utilizado o sistema de arquivos recomendado pelo fabricante do sistema operacional;

II - os serviços disponibilizados no servidor do IDS/IPS devem se resumir ao estritamente necessário. Deve ser evitada a instalação de compiladores, clients (TFTP, FTP, SSH, TELNET, BROWSERS, correio) e ferramentas de rede (DIG, NSLOOKUP, TCPDUMP, TRACEROUTE, PING);

III - a funcionalidade auto-run do sistema operacional deve ser desabilitada; e

IV - O IDS/IPS deve realizar somente tarefas destinadas à detecção de intrusão. As exceções devem ser autorizadas pela área responsável pela Segurança da Informação e após análise de risco devidamente documentada.

Seção IV

DA DOCUMENTAÇÃO

Art. 126. A documentação das configurações do IDS/IPS deve ser mantida atualizada e seu acesso restrito a área de TIC e à área responsável pela Segurança da Informação.

Art. 127. Todas as alterações relativas a assinaturas, respostas, regras e políticas implementadas em produção devem estar devidamente documentadas.

Seção V

DO MONITORAMENTO

Art. 128. Toda e qualquer captura ou armazenamento de dados realizada pelo IDS/IPS deve se restringir a evidências ou provas de tentativas de intrusão.

Art. 129. O acesso aos dados coletados deve ser restrito a área responsável pela Segurança da Informação e à área de TIC.

Art. 130. Os eventos gerados pelo IDS/IPS devem ser armazenados em servidores de log.

Art. 131. O log do IDS/IPS deve ser verificado diariamente.

Seção VI

DA ANÁLISE DE RISCO

Art. 132. Os controles existentes na ferramenta de análise de riscos, adotada pelo órgão ou entidade, devem ser aplicados e avaliados a cada 6 (seis) meses. Todas as correções devem ser realizadas após autorização da área responsável pela Segurança da Informação. As correções dos controles, considerados de alta criticidade devem ser realizadas imediatamente.

CAPÍTULO VIII - BACKUP

Seção I

DAS DISPOSIÇÕES PRELIMINARES

Art. 133. Todos os dados e informações vitais para o pleno funcionamento do órgão ou entidade devem ser mantidos com cópias de segurança.

Art. 134. Toda implantação, implementação e configuração de soluções e sistemas de backup/restore devem considerar as recomendações apresentadas em procedimento específico.

Art. 135. Todo backup/restore deve ser planejado e dimensionado pela área de TIC junto às áreas solicitantes.

Art. 136. Todos os acessos às mídias, aos equipamentos, procedimentos e programas que implementem os sistemas de backups/restores do órgão ou entidade, devem ser controlados, documentados e restritos aos técnicos das área de TIC e responsável pela Segurança da Informação.

Art. 137. As cópias de segurança devem permitir:

I - a recuperação dos dados e informações em caso de perda ou indisponibilidade;

II - a manutenção de versões e históricos de configurações de equipamentos e programas de computador; e

III - o arquivamento de dados e informações por período de tempo definido em legislações específicas ou requisitos de segurança aplicáveis.

Seção II

DOS SISTEMAS OPERACIONAIS

Art. 138. Todo servidor de produção deve ter rotina de backup/restore diária do seu sistema operacional definido, documentado e implementado.

Art. 139. Os backups/restores dos sistemas operacionais devem ser realizados com finalidade exclusiva de salvaguarda das configurações e dos dados e informações pertinentes ao sistema e ao equipamento onde esteja instalado.

Art. 140. Os servidores dos ambientes de desenvolvimento ou de homologação devem possuir procedimento de backup/restore no mínimo quinzenal.

Seção III

DOS BANCOS DE DADOS E ARMAZÉNS DE INFORMAÇÃO

Art. 141. Devem existir procedimentos diferenciados para o backup/restore dos bancos de dados e para os armazéns de informações.

Art. 142. Todas rotinas de backup/restore dos bancos de dados e dos armazéns de informação devem ser executados pela área de TIC.

Art. 143. Apenas os administradores de banco de dados podem colocar efetivas as cópias, recuperadas pelos processos de restore da produção.

Art. 144. Todo banco de dados e armazéns de informação em produção deve ter rotina de backup/restore definida, documentada e implementada.

§ 1º Os backups/restores de banco de dados e armazéns de informação são realizados com finalidade exclusiva de salvaguarda

dos dados para os incidentes/acidentes que exijam a recuperação plena desses bancos ou armazéns.

SS 2º Deve existir procedimento de backup/restore específico para os bancos de dados e armazéns de informações dos ambientes de desenvolvimento ou de homologação.

Seção IV

DOS SISTEMAS APLICATIVOS

Art. 145. As áreas do desenvolvimento e manutenção de sistemas são responsáveis pela definição das necessidades e pelo planejamento das rotinas e procedimentos que envolvam as cópias de segurança dos dados e informações manipuladas por seus programas de computador, estando ou não armazenados em bancos de dados. Se as necessidades e o planejamento não forem compatíveis com as disponibilizadas pela área de produção, as áreas de desenvolvimento e manutenção de sistemas serão responsáveis por implementar a rotina nas próprias aplicações.

§ 1º A área de TIC deve homologar e executar os procedimentos de backup/restore definidos pela área de desenvolvimento responsável pelo sistema aplicativo.

§ 2º Todos os procedimentos de backup/restore dos aplicativos devem estar em conformidade com as legislações pertinentes às suas especialidades.

§ 3º Os gestores dos dados e informações devem determinar o período de retenção das mídias utilizadas pelos procedimentos de backup/restore dos seus sistemas aplicativos.

§ 4º Ao determinar o período de retenção, os gestores dos dados e informações devem estar atentos aos aspectos legais e judiciais envolvidos.

Seção V

DOS PROGRAMAS FONTE

Art. 146. Os sistemas de arquivos e os bancos de dados que contenham programas fontes devem possuir rotinas especificas de backup/restore.

§ 1º Os sistemas e os programas de computador utilizados para o controle de versão de programas fonte no órgão ou entidade devem

ser contemplados por rotina de backup/restore bem definido e documentado.

§ 2º O período mínimo de retenção das mídias dos procedimentos de backup/restore dos programas fonte e dos sistemas e programas de computador responsável pelo controle de versão não devem ser inferiores a 180 dias. Deve ser observada, também, a definição do sistema de controle de versão adotado pelo órgão ou entidade.

§ 3º Devem ser mantidas cópias anuais de todos os programas fontes em produção e dos sistemas e programas de computador responsáveis pelos controles de versão do órgão ou entidade.

§4º Enquanto o programa fonte estiver em produção devem ser mantidas suas cópias de segurança.

Seção VI

DOS EQUIPAMENTOS DE CONECTIVIDADE

Art. 147. Deve ser implementado procedimento automático (sistema aplicativo) para a coleta e armazenamento das configurações dos equipamentos de conectividade em um servidor que esteja contemplado pelas rotinas de backup/restore do órgão ou entidade.

Art. 148. A área de TIC deve acompanhar e executar os procedimentos de backup/restore dos dados e informações coletados pelo aplicativo implementado.

Seção VII

DA INSTALAÇÃO E CONFIGURAÇÃO DOS SISTEMAS DE BACKUP/RESTORE

Art. 149. Os equipamentos especializados e programas de computadores que componham os sistemas de backup do órgão ou entidade devem ser instalados e configurados de maneira a garantir as seguintes premissas:

§ 1º Não fiquem localizados nas imediações (mesmo edifício, quarteirão, bloco, vizinhança) do ambiente de Produção do DataCenter, e distantes das principais informações relevantes do órgão ou entidade; ficando protegido:

I - dos desastres naturais que possam atingir o ambiente de Produção, como: quedas de raio, inundações, desmoronamentos, e outros;

II - de eventos que possam atingir o ambiente de Produção, ou dificultar seu acesso, como: levantes, greves, revoltas, atentados, incêndios, quedas de aeronaves, e outros tipos de desastres e eventos que possam tornar o local de inacessível;

III - de queda de energia devido à falha em uma única subestação da CEMIG.

SS2º Façam parte de uma rede especializada de Backup onde não haja concorrência com os demais serviços de Produção e possuam recursos de segurança específicos para as atividades de Backup/Restore.

SS 3º Fiquem em ambiente especializado de maneira que possua:

I - controle e registro de acesso;

II - iluminação adequada;

III - isolamento físico;

IV - apenas equipamentos específicos para a rede de backup/restore;

V - segurança contra furto ou roubo;

VI - mecanismos para a detecção e controle de incêndios;

VII - mecanismos para o controle de temperatura; e

VIII - proteção contra ameaças naturais: raios, inundação e outros.

SS 4º Todos os equipamentos de gravação/restauração das mídias de backup/restore (Unidades de Fita, Autoloaders, Robôs, JukeBox, e outros), que possuam recursos para a conexão em redes, devem ser instalados em conformidade com as premissas anteriormente apresentadas. Exceções devem ser autorizadas pela área responsável pela segurança da informação e pelas áreas responsáveis pelos dados e informações envolvidas.

Art. 150. Os equipamentos que realizem backup/restore e que não possuam conexões com a rede especializada de backup devem ser instalados de maneira a permitir o maior distanciamento possível dos dados e informações que serão copiadas.

Parágrafo Único. As mídias manipuladas por esses equipamentos devem ser enviadas e mantidas no ambiente de backup/restore especificado anteriormente. A periodicidade de envio e manutenção

das mídias gravadas deve seguir os critérios definidos pela área de Produção e de acordo com a solicitação do backup.

Art. 151. Todo sistema de backup/restore deve ser configurado, quando houver o recurso, de maneira a manter trilhas de auditoria.

Art. 152. A utilização da compactação de dados pelos sistemas de backup/restore deve ser configurada e utilizada.

Parágrafo Único. Apenas por meio de comprovado impacto na disponibilidade e desempenho do sistema de backup/restore a compactação deve ser desativada.

Art. 153. A geração das cópias de segurança dos sistemas de backups deve ser realizada preferencialmente em horários que minimizem o impacto à execução dos serviços e ao desempenho da Rede Corporativa do órgão ou entidade.

Parágrafo Único. A área de TIC deve determinar os melhores horários e dias para a realização das cópias de segurança dos sistemas de backup/restore.

Art. 154. Sempre que houver a viabilidade, as soluções de backup/restore devem ser configuradas para que se permita a recuperação das cópias de segurança independentes da infraestrutura de backup/restore adotadas pelo ambiente de produção.

Art. 155. Cabe à configuração dos sistemas de backup/restore para que se permita a recuperação das cópias sem a necessidade efetiva do próprio sistema de backup/restore.

Art. 156. Deve existir processo de "disaster recovery" para o servidor de backup/restore, ou para o servidor que contenha os programas de computador que executam e administram as funções de backup/restore do órgão ou entidade.

Art. 157. Todos os equipamentos e programas de computador diretamente relacionados com os sistemas de backup/restore do órgão ou entidade devem ser atualizados de maneira continua e permanente.

Art. 158. Toda instalação ou atualização, de equipamentos ou programas de computador, relacionada diretamente com os sistemas de backup/restore deve ser homologada antes de ser implantada em produção.

SS 1º Nenhuma atualização ou instalação de novo equipamento ou programa relacionado diretamente com os sistemas de backup/restore deve afetar a disponibilidade das mídias já gravadas.

SS2º Caso ocorra risco de indisponibilidade das mídias, com a implantação de atualizações, ou a instalação de novos equipamentos e programas de computador, os dados e informações deverão ser transferidos para outro meio de armazenamento.

Seção VIII

DAS MÍDIAS

Art. 159. As mídias utilizadas devem ser trimestralmente testadas e avaliadas em relação a sua vida útil.

Art. 160. Deve ser mantida documentação em papel sobre as mídias e seus conteúdos. Esta documentação deve ser atualizada a cada execução do backup/restore e ser armazenada segundo as especificações anteriormente definidas nesse manual.

Art. 161. A área de produção deve manter procedimento de administração de todas as mídias utilizadas pelos diferentes sistemas de backup/restore do órgão ou entidade.

Art. 162. As mídias utilizadas pelos sistemas de backup/restore devem seguir as recomendações estabelecidas pelo fabricante, bem como considerar o tempo de vida útil da mesma.

Art. 163. Recomenda-se que sejam retiradas imediatamente dos sistemas de backup/restore todas as mídias com data de vida útil (validade) vencidas.

Art. 164. As mídias armazenadas por prazo acima do período de vida útil ou obsolescência devem ser substituídas e os dados nela contidos que estejam dentro do período de retenção devem ser transferidos para outra mídia.

Art. 165. A área de TIC deve ser responsável pelo controle das datas de validade das mídias e pelo processo de transferências de dados entre as mídias.

Art. 166. O prazo de validade das mídias deve estar registrado em um sistema de controle de mídias, ou gerenciado pelos sistemas de backup/restore utilizados.

Seção IX

DO TRANSPORTE DE MÍDIAS

Art. 167. O transporte de mídias deve ter controles que garantam a segurança, tais como:

I - definição formal dos portadores autorizados;

II - embalagem com proteção contra danos físicos, de acordo com a especificação dos fabricantes;

III - utilização de recipientes lacrados;

IV - escolta quando a classificação da informação exigir; e

V - criptografia de seu conteúdo segundo a classificação das informações.

Seção X

DO DESCARTE DE MÍDIAS

Art. 168. Todo descarte de mídias (Fitas, CDs, DVDs e outros), utilizados pelos sistemas de backup/restore, deve estar em conformidade com o procedimento específico.

Art. 169. O prazo de retenção das mídias de backup deve ser acompanhado pela área de TIC para possibilitar o descarte das mesmas.

Art. 170. No caso de vencimento do período de vida útil, vencimento do limite de reutilização, substituição por obsolescência ou danificação, as mídias de backup devem ser destruídas de forma que não seja possível qualquer recuperação dos dados.

Art. 171. A área de TIC deve presenciar e registrar o descarte, de acordo com o procedimento de descarte de mídia.

Seção XI

DOS TESTES DE INTEGRIDADE, RECUPERAÇÃO E VALIDAÇÃO

Art. 172. Os procedimentos para testes de integridade, recuperação e validação backup/restore dos sistemas aplicativos devem ser definidos, implementados e determinados com a participação dos gestores das informações, considerando a periodicidade de testes de restauração definida pela área de TIC.

Art. 173. Recomenda-se que semanalmente seja realizado um procedimento de restore aleatório de dados e informações anteriormente copiadas para avaliação do tempo de recuperação e das mídias envolvidas.

Art. 174. Recomenda-se que semestralmente seja realizada simulação de recuperação integral de um site, ou um grupo de sites, para a validação de todo o processo de recuperação implementado no órgão ou entidade.

Art. 175. Os testes de restauração e simulação de recuperação dos dados devem ser realizados em servidores diferentes do ambiente de produção.

Art. 176. Caso não exista infraestrutura apropriada no órgão ou entidade, recomenda-se que seja viabilizado recurso externo.

Art. 177. Os testes de restauração e simulação de recuperação parcial ou integral dos dados devem ser devidamente registrados.

Parágrafo Único. Caso não tenha sucesso, os procedimentos de geração deverão ser imediatamente revistos e realizadas as adequações necessárias.

Art. 178. Recomenda-se que todo novo equipamento instalado no órgão ou entidade, seja antes utilizado para testes de integridade, recuperação e validação dos sistemas de backup/restore, simulando processo de "disaster recovery".

Art. 179. Os dados restaurados para verificação da integridade e simulação de recuperação de dados devem ser eliminados do equipamento ao final do teste, garantindo que não haverá qualquer possibilidade de recuperação dos arquivos armazenados no equipamento de teste.

Seção XII

DOS ARQUIVOS PARA AUDITORIA E LOGS

Art. 180. A configuração, geração e manipulação de todos os tipos de arquivos para auditoria e LOGs devem estar em conformidade com procedimento específico.

Art. 181. As rotinas backup/restore dos arquivos para auditoria e LOGs devem ser configuradas de acordo com as premissas técnicas e legais para cada tipo de arquivo de auditoria e para cada tipo de LOG.

Art. 182. O tempo de retenção das mídias envolvidas com as cópias dos arquivos para auditoria e LOGs deve determinar o tipo de mídia a ser utilizada.

CAPÍTULO IX - DO GERENCIAMENTO DE ACESSO LÓGICO À REDE

Seção I

DO CONTROLE DE ACESSOS

Art. 183. O controle de conexão na rede corporativa dos órgãos e entidades deve ser realizado por mecanismo de segurança, de forma que apenas usuários autorizados e com identificação reconhecida possam acessar os recursos compartilhados.

Art. 184. Toda liberação de login para acesso à rede corporativa, para funcionários e terceiros, deve ser realizada mediante autorização da área de TIC conforme procedimento específico.

Art. 185. Os acessos à rede, realizados pelos usuários devem ter como finalidade exclusiva a realização de suas atividades profissionais.

Seção II

DO CONTROLE DE CONEXÕES

Art. 186. Somente equipamentos dos órgãos e entidades ou equipamentos autorizados pela área de segurança da informação poderão se conectar à rede corporativa.

Art. 187. A conexão de equipamentos de terceiros na rede corporativa deve ser liberada somente com solicitação formal da área responsável pelo acompanhamento do serviço e com aprovação da área de TIC conforme procedimento específico.

Art. 188. As conexões wireless (sem fio) devem seguir o capítulo "Rede Wireless".

Seção III

DO ACESSO REMOTO

Art. 189. Todo acesso remoto a rede corporativa deverá ser documento e disponibilizado mediante solicitação formal e somente após emissão de laudo e aprovação.

Art. 190. Quando estabelecido a partir de qualquer ponto externo à rede corporativa deve ser controlado e efetuado por canal seguro.

Seção IV

DA DOCUMENTAÇÃO

Art. 191. A documentação referente à topologia da rede deve ser atualizada pela área de TIC e seu acesso disponibilizado somente à área de segurança da informação.

Seção V

DA CONFIGURAÇÃO DA REDE

Art. 192. Somente endereços IPs privativos (inválidos) devem ser usados na rede corporativa.

Parágrafo Único. As exceções devem ser autorizadas pela área de segurança da informação.

Art. 193. Serviços desnecessários devem ser desabilitados em todos os equipamentos da rede corporativa.

Art. 194. Todas as portas de diagnóstico remoto dos equipamentos da rede corporativa devem ser identificadas e bloqueadas.

Parágrafo Único. As exceções devem ser documentadas e autorizadas pela área de segurança da informação.

CAPÍTULO X - DAS VEDAÇÕES

Art. 195. É vedado aos usuários:

I - instalar servidores com dual boot;

II - conectar dispositivo não autorizado pela área responsável pela Segurança da Informação e homologado pela área de TIC aos servidores do órgão ou entidade;

III - permitir o uso de servidor do órgão ou entidade por pessoa não autorizada;

IV - o usar os logins de administradores (root, administrator, dentre outros) e logins que não sejam individuais, para acesso aos servidores;

V - acessar os servidores do órgão ou entidade por meio de utilitários que não adotam recursos de criptografia sempre que possível;

VI - permitir a permanência de terceiros dentro das salas de servidores sem o acompanhamento de um técnico da área de TIC;

VII - utilizar o IDS/IPS como ferramenta para auditar, registrar ou coletar dados pessoais.

VIII - criar regras no firewall que possibilitem o tráfego de pacotes com a cláusula ANY no campo que especifica o serviço.

Parágrafo Único. As exceções devem ser liberadas somente após análise de risco e laudo emitido pela área de Segurança da Informação.

CAPÍTULO XI - DAS RESPONSABILIDADES

Art. 196. Compete ao usuário reportar incidentes de Segurança da Informação à área de segurança da informação.

Art. 197. Compete à área de TIC:

I - administrar a rede corporativa;

II - Manter a documentação da topologia da rede atualizada e controlar seu acesso;

III - autorizar acessos à rede;

IV - instalar, configurar e manter os ambientes operacionais dos firewalls. (Sistema Operacional nos servidores, bem como os produtos e as correções e atualizações de versão);

V - disponibilizar e administrar a infraestrutura dos recursos para administração do firewall;

VI - manter atualizadas as documentações relativas aos firewalls;

VII - instalar, manter e configurar todos os servidores dos órgãos e entidades;

VIII - definir os administradores de sistemas dos ambientes, assim como providenciar substitutos capacitados para os mesmos;

IX - realizar atualizações tecnológicas e manutenção dos dados e aplicativos armazenados nos servidores do órgão e entidade;

X - acompanhar a realização de manutenção corretiva, ou preventiva, dos servidores do órgão e entidade sob sua responsabilidade, quando a manutenção for realizada por terceiros no ambiente do órgão ou entidade;

XI - realizar a remoção das informações armazenadas nos servidores, no caso de manutenção externa ao órgão e entidade;

XII - realizar o backup das informações armazenadas nos servidores do órgão e entidade;

XIII - instalar, manter e configurar todos os servidores que contenham os serviços de Firewall de Rede e IDS de Rede;

XIV - exceção para os servidores que possuam Firewall e IDS locais e que atuem apenas para a segurança específica do próprio servidor onde se encontrem instalados;

XV - manter a documentação do ambiente informatizado atualizada;

XVI - homologar os roteadores e switches para uso dos órgãos e entidades;

XVII - manter a documentação dos roteadores e switches atualizada;

XVIII - prover o ambiente físico necessário para instalação dos roteadores e switches;

XIX - avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação adotada pelo órgão ou entidade.

Art. 198. Compete à área de Segurança da Informação:

I - autorizar a conexão de equipamentos de prestadores de serviço na Rede Corporativa e ao backbone;

II - autorizar, quando necessário, a liberação de portas de diagnóstico remotas;

III - autorizar acessos à rede;

IV - analisar incidentes de segurança e recomendar correções à área de TIC;

V - realizar análise de risco para criação de regras no firewall e gerar laudo técnico;

VI - analisar os logs dos servidores do órgão e entidade periodicamente, em caso de inconformidades a área de suporte deverá ser acionada.

CAPÍTULO XII - PENALIDADES

Art. 199. Aquele que não cumprir as normas estabelecidas nessa Resolução estará sujeito às penalidades previstas em Lei.

CAPÍTULO XIII - DISPOSIÇÕES FINAIS

Art. 200. Os Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional deverão adequar-se ao disposto nesta Resolução no período máximo de 1 (um) ano a partir de sua publicação.

Parágrafo Único. Compete à Secretaria de Estado de Planejamento e Gestão - Seplag, por meio da Superintendência Central de Governança Eletrônica, fornecer as orientações necessárias ao fiel cumprimento das regras dessa Resolução, além de verificar a conformidade das práticas com o estabelecido nesta Resolução e recomendar as correções necessárias.

Art. 201. Fica facultada, às Empresas Públicas e Sociedades de Economia Mista, a aplicação das regras contidas na presente Resolução, observada a conveniência e a oportunidade administrativas.

Art. 202. Caberá à Secretaria de Estado de Planejamento e Gestão, por meio da Subsecretaria de Gestão, esclarecer os casos omissos a esta Resolução.

Art. 203. Esta Resolução entra em vigor na data de sua publicação.

Belo Horizonte, aos 21 de setembro de 2009.

RENATA VILHENA

Secretária de Estado de Planejamento e Gestão