MINAS GERAIS
ÓRGÃO OFICIAL DOS PODERES DO ESTADO
DIÁRIO DO EXECUTIVO, LEGISLATIVO E PUBLICAÇÕES DE TERCEIROS
CADERNO I, SEXTA-FEIRA, 28 DE DEZEMBRO DE 2018
PÁG. 35 – COL. 04

SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO
RESOLUÇÃO SEPLAG Nº 107, DE 26 DE DEZEMBRO DE 2018

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

O SECRETÁRIO DE ESTADO DE PLANEJAMENTO E GESTÃO, no uso das atribuições que lhe conferem o artigo 93, § 1º, inciso III, da Constituição do Estado e o artigo 6º, §2º do Decreto estadual nº. 46.765, de 26 de maio de 2015,
RESOLVE:
CAPÍTULO I – DAS DISPOSIÇÕES GERAIS
Seção I
DISPOSIÇÕES PRELIMINARES
Art 1º O acesso lógico à rede corporativa, a concessão de acesso remoto à rede corporativa, a utilização de senhas dos sistemas e serviços, o armazenamento de informações, a utilização de dispositivos móveis, a utilização do correio eletrônico, a utilização das estações de trabalho, a utilização da Internet e a conduta dos usuários de informações no âmbito dos órgãos e entidades do Governo do Estado de Minas Gerais observam o disposto nesta Resolução.
Art 2º É constituída por um conjunto de diretrizes e regras que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas por suas unidades administrativas e visa atender aos seguintes princípios:
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas devidamente autorizadas;
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Autenticidade: garantia da identidade de quem está enviando a informação;
- Legalidade: Garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;
Art 3º Aplica-se a presente resolução a todos os usuários dos órgãos e entidades do Governo do estado de Minas Gerais, seja ele nomeado, designado, contratado ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública. Aplica-se também a fornecedores no desempenho de alguma atividade internamente no órgão ou entidade do Governo do estado.
Seção II
DAS DEFINIÇÕES
Art 4º 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 entre dispositivos (microcomputadores, servidores, etc), por meio da rede de comunicação de dados corporativa. Quando se tratar de redes corporativas distintas o mesmo deverá ser realizado por meio de VPN;
III .administrador: contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configurados, normalmente não disponíveis a todos os usuários;
IV .análise de riscos: processo completo de análise dos pontos críticos que possam oferecer ameaças ao ambiente tecnológico;
V .antimalware: ferramenta destinada a detecção, anulação e remoção de códigos maliciosos (malware).
VI .*antispyware:* programa que permite identificar e remover códigos maliciosos que se auto instalam nos computadores;
VII .antivírus: programa que permite identificar e eliminar vírus em computadores;
VIII .ataque do tipo negação de serviço – DoS do inglês Denial of Service): um ataque de negação de serviço é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Não se trata de uma invasão do sistema, mas sim de provocar a sua indisponibilidade por sobrecarga.
IX .ataque distribuído por negação de serviço - DDoS, do inglês Distributed Denial-of-Service attack): definição semelhante ao Ataque do tipo Negação de Serviço (DoS) sendo que a diferença básica entre um ataque de DoS e de DDoS é que neste último, os ataques são realizados por diversas máquinas simultaneamente, o que aumenta a possibilidade de êxito. As máquinas utilizadas nos ataques de DDoS são denominadas zumbis.
X .autenticação: é um processo de verificação da identidade que consta em um sistema, ou seja, o sistema verifica as credenciais de quem está tentando acessar, com as que constam na base de dados, caso positivo, o sistema é liberado pois as credenciais foram validadas.
XI .autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui, certificada por instrumento ou testemunho público;
XII .*backup*: significa cópia de segurança. Serve para copiar dados de um dispositivo de armazenamento para outra fonte segura que poderá ser utilizada futuramente.
XIII .BYOD - Bring your own device (BYOD): refere-se à política de permitir que os empregados possam trazer dispositivos de propriedade pessoal (laptops, tablets e telefones inteligentes) para seu local de trabalho e usar esses dispositivos para acessar informações e aplicações dos Órgãos e Entidades;
XIV .certificado digital: arquivo eletrônico, assinado digitalmente por uma Autoridade Certificadora, que contém dados de uma pessoa física ou jurídica, utilizados para comprovar sua identidade. O certificado digital é armazenado em uma mídia ou em um dispositivo de hardware;
XV .*chat*: palavra que em português significa "conversação" e é um neologismo para designar aplicações de conversação em "tempo real";
XVI .chefia imediata: titular da área a qual está subordinado o usuário. Na sua ausência deve ser observada a ordem hierárquica superior;
XVII .computação em nuvem: fornecimento de recursos computacionais pela internet (nuvem), sob demanda, por meio de uma plataforma de serviços;
XVIII .confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;
XIX .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;
XX .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;
XXI .correio eletrônico: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;
XXII .crachá: identificação, pessoal e intransferível, disponibilizada ao usuário para acesso físico às dependências do órgão ou entidade;

XXIII .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;
XXIV .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;
XXV .disponibilidade: garantia de que os usuários autorizados obtenham acesso tempestivo (no momento da solicitação) à informação e aos ativos correspondentes;
XXVI .dispositivo móvel: equipamentos com capacidade de armazenamento e processamento de dados, de fácil locomoção, interligados ou não à rede corporativa do órgão ou entidade, tais como notebooks, smartphones, Tablets e Coletores de Dados;
XXVII .domínio: identificação de nomes da Internet, utilizada para prover o acesso a endereços de computador, a qualquer programa de comunicação;
XXVIII .*download:* transferência de um arquivo de um computador para outro por meio da Internet;
XXIX .e-mail: vide "correio eletrônico";
XXX .estação de trabalho: computadores e notebooks do órgão ou entidade interligados ou não à rede corporativa;
XXXI .ferramenta de auditoria: software que armazena os eventos gerados no ambiente computacional, permitindo a rastreabilidade da configuração e da utilização dos sistemas;
XXXII .firewall: é um sistema de segurança de rede que monitora e controla o tráfego de entrada e de saída da rede com base em regras de segurança pré-determinadas. Um firewall geralmente estabelece uma barreira de segurança entre uma rede interna confiável e outra rede externa, como a Internet, que se assume não segura ou confiável.
XXXIII .hardware: todo e qualquer dispositivo físico em um computador;
XXXIV .IDS (*Intrusion Detection System*): sistema de detecção de intrusão que permite identificar atividades suspeitas na rede;
XXXV .incidente de segurança da informação: um ou mais eventos de segurança da informação, indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
XXXVI .integridade: salvaguarda da exatidão e completeza da informação;
XXXVII .internet: rede mundial de computadores;
XXXVIII .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;
XXXIX .IOT (*Internet of Things*): também conhecida como Internet das coisas, permite a detecção e controle remoto de objetos por meio de infraestrutura de rede existente, possibilitando a integração do mundo físico com sistemas baseados em computadores. Engloba tecnologias como as redes inteligentes, casas inteligentes, transporte inteligente e cidades inteligentes.
XL .IPS .(*Intrusion Prevention System*): sistema de prevenção de ataques que permite que atividades suspeitas na rede sejam bloqueadas de forma preventiva;
XLI .licença de software: direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes;
XLII .*log*: arquivos que contenham informações sobre eventos de qualquer natureza em um sistema computacional com o objetivo de permitir o rastreamento de atividades;
XLIII .*login*: identificação do usuário para acesso aos sistemas e serviços;
XLIV .*logon:* processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema;
XLV .*logout:* processo de saída de um usuário dos sistemas e serviços;
XLVI .malware: Software malicioso destinado a extração/alteração de informações de forma ilícita.
XLVII .mecanismos de segurança: conjunto de hardwares e softwares utilizados na implantação de regras de segurança para o ambiente.
XLVIII .mídias: meio físico utilizado para armazenar dados;
XLIX .modem: equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações;
L .normas: especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes;
LI .órgão ou entidade pública: qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas;
LII .*patch(es)* - é um programa criado para atualizar ou corrigir um software.
LIII .*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;
LIV .phishing: investida de cibercriminosos almejando a obtenção de informações pessoais, geralmente identidades online, por meio de e-mails falsos ou redirecionamentos a sites ilusórios.
LV .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;
LVI .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;
LVII .proteção: vide "controle";
LVIII .ransomware: É um tipo de malware (software malicioso) que tem a capacidade de tornar dados disponíveis no equipamento totalmente inacessíveis através de criptografia e, em seguida, solicita o pagamento de resgate em troca da chave de decodificação que é necessária para recuperar as informações contidas nos arquivos criptografados;
LIX .recursos computacionais: recursos tecnológicos que suportam as informações do órgão ou entidade;
LX .rede corporativa: computadores e outros dispositivos interligados que compartilham informações ou recursos do órgão ou entidade;
LXI .*restore*: recuperação de dados armazenados em cópias de segurança;
LXII .risco: combinação da probabilidade de um evento e de suas consequências;
LXIII .roteador: dispositivo de rede responsável por encaminhar pacotes de dados entre redes distintas criando um conjunto de redes de sobreposição;
LXIV .segurança da informação: A segurança da informação (SI) está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.
LXV .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
LXVI .serviço: sistemas e ferramenta de trabalho disponibilizados ao usuários de TIC, como correio eletrônico e acesso à Internet e intranet, acessível na rede do órgão ou entidade;
LXVII .servidor: computador responsável pelo compartilhamento de recursos e execução de serviços solicitados pelos demais computadores a ele conectados;
LXVIII .sistema: vide "sistema de informação automatizado";

LXIX .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;
LXX .sistema operacional: programa ou conjunto de programas que responde pelo controle da alocação dos recursos do computador
LXXI .*site*: vide "sítio";
LXXII .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;
LXXIII .software: programa de computador;
LXXIV .software de comunicação instantânea: aplicação que permite o envio e recebimento de documentos diversos, imagens, mensagens de texto, vídeo e voz em tempo real;
LXXV .*spam*: mensagem de correio eletrônico não solicitada, enviada em larga escala para uma lista de e-mails, fóruns ou grupos de discussão;
LXXVI .*spyware:* programa espião que monitora a atividade de um computador podendo transmitir estas informações a um receptor na Internet, sem o conhecimento e consentimento do usuário;
LXXVII .*streaming*: tecnologia que permite a transmissão contínua de informação multimídia (áudio e vídeo) por meio de pacotes, utilizando redes de computadores, sobretudo a Internet;
LXXVIII .Switch: dispositivo utilizado para interconexão de computadores, possibilitando o encaminhamento de pacotes entre os diversos nós da rede.
LXXIX .terceiro: pessoa jurídica ou física contratada pelo órgão ou entidade para realizar serviços;
LXXX .trilha de auditoria: histórico das transações dos sistemas contendo registro dos usuários que as efetuaram e das tentativas de acesso indevido;
LXXXI .unidade administrativa: cada área que compõe a estrutura organizacional do órgão ou entidade;
LXXXII .*upload*: transferência de um arquivo, de qualquer natureza, do computador do usuário, para algum equipamento da Internet;
LXXXIII .URL (*Universal Resource Locator*): *link* ou endereço de uma página *web*;
LXXXIV .*userid*: identificação do usuário no recurso computacional;
LXXXV .usuário: todo aquele que possui permissão de acesso à rede corporativa e 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;
LXXXVI .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;
LXXXVII .VPN (*Virtual Private Network*) – forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tal como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação;
LXXXVIII .*webmail*: interface web do correio eletrônico;
LXXXIX .wireless*:* sistema de comunicação que não requer fios, funcionando por meio de equipamentos que usam radiofrequência ou comunicação via ondas de rádio para transportar sinais;
XC .*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.
XCI .atividades profissionais: atividades necessárias e suficientes ao desempenho das tarefas do agente público no órgão ou entidade.

CAPÍTULO II – DO ACESSO À REDE CORPORATIVA DO ÓRGÃO OU ENTIDADE

Seção I

DISPOSIÇÕES PRELIMINARES

Art 5º A concessão de acesso à rede corporativa do órgão ou entidade será realizada mediante solicitação formal dos responsáveis pela área do usuário.
Art 6º O referido acesso permitirá ao usuário utilizar os equipamentos e os recursos disponíveis aos demais usuários com o mesmo perfil.
Art 7º As conexões realizadas e os serviços disponibilizados na rede corporativa do órgão ou entidade serão limitados, controlados e autorizados pela área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.
Art 8º Os acessos autorizados para os usuários restringir-se-ão às atividades profissionais pertinentes aos processos e negócios do órgão ou entidade.

Seção II

DO BLOQUEIO, ALTERAÇÃO E CANCELAMENTO DE ACESSOS

Art 9º Os acessos dos usuários desligados deverão ser bloqueados ou revogados no momento em que o desligamento for informado pela área de Recursos Humanos ou chefia imediata.
Art 10 Deverão ter seus acessos bloqueados os usuários em licença ou afastamento.
Art 11 A cessão, a alteração e o cancelamento de acesso com privilégio de administrador na rede corporativa e nas estações de trabalho serão realizados somente mediante autorização da área de Segurança da Informação do Órgão ou Entidade. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.

Seção III

DO MONITORAMENTO

Art 12 Documentar-se-ão as informações dos usuários cadastrados e seus acessos à rede corporativa do Órgão ou Entidade, sendo o nome completo e CPF ou MASP/Matrícula o mínimo necessário.
Parágrafo Único - Registrar-se-á por meio de logs todo acesso à rede corporativa e às redes externas, sendo que a guarda dos mesmos deverá ser realizada por no mínimo 1 ano.

Seção IV

DO ACESSO REMOTO À REDE CORPORATIVA

Art 13 Disponibilizar-se-á ao usuário o acesso remoto somente por meio de VPN e para a execução de atividades relacionadas ao órgão ou entidade.
Parágrafo Único - O órgão ou entidade reserva para si o direito de monitorar a utilização do acesso remoto disponibilizado.

CAPÍTULO III – SENHAS

Art 14 As identificações e as senhas para acesso à rede corporativa são de uso pessoal e intransferível.
§1º Na liberação da identificação para o usuário será fornecida uma senha temporária, que dever ser alterada no primeiro acesso.
§2º A senha de acesso deverá seguir as seguintes regras:
- Deve conter pelo menos 8 (oito) caracteres;
- Deve ser composta de caracteres de 3 das 4 categorias abaixo:
- Ao menos um caractere maiúsculo (A-Z);
- Ao menos um caractere minúsculo (a-z);
- Ao menos um digito (0-9);
- Ao menos um caractere não alfabético (do teclado)(ex !$@%...).
- Não conter mais de 2 caracteres idênticos consecutivos;
§3º A senha deverá ser trocada sempre que existir qualquer indício de comprometimento da rede corporativa ou da própria senha ou, no máximo, a cada 90 dias.

§4º É proibida a reutilização, pelo usuário, das últimas 05 (cinco) senhas.
§5º A manutenção do sigilo da senha é de responsabilidade do usuário.
§6º As senhas para acesso ao mainframe devem respeitar as particularidades da tecnologia deste ambiente.
Art 15 As senhas para acesso à rede corporativa serão armazenadas e transmitidas criptografadas.
Art 16 O acesso será bloqueado automaticamente após 03 (três) tentativas incorretas e consecutivas de *logon* a rede.
Parágrafo único. O acesso é desbloqueado mediante solicitação do usuário à área de Segurança da Informação ou a área de TIC responsável pelo controle de usuários. O desbloqueio ocorrerá somente após comprovação de dados pessoais.
CAPÍTULO IV – DO ARMAZENAMENTO DE INFORMAÇÕES
Art 17 Os servidores de arquivos disponibilizados na rede corporativa serão utilizados exclusivamente para armazenamento de arquivos que contenham informações relacionadas a atividades profissionais pertinentes aos processos e negócios do órgão ou entidade.
§1º A utilização do espaço nos servidores de arquivo da rede do órgão ou entidade é limitada, controlada e monitorada.
§2º O órgão ou entidade reserva para si o direito de auditar a utilização do espaço disponibilizado a fim de identificar arquivos em desacordo com as diretrizes supracitadas e consequentemente, tomar as devidas providências administrativas para apuração de responsabilidade.
Art 18 As informações corporativas deverão ser armazenadas em diretórios disponibilizados nos servidores da rede do órgão ou entidade, com acesso restrito ao grupo de usuários que as utilizam.
CAPÍTULO V – UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS PARTICULARES
Seção I
DOS DISPOSITIVOS PARTICULARES
Art 19 Entende-se por equipamento particular todo o dispositivo que não foi fornecido pelo órgão ou entidade para o desenvolvimento das atividades profissionais.
Art 20 A guarda e manutenção de dispositivos particulares não é responsabilidade do órgão ou entidade.
§1º É permitida a utilização de dispositivo móvel particular e da conexão à rede coorporativa do órgão ou entidade, desde que haja uma solicitação da chefia imediata e a autorização da área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.
§2º O órgão ou entidade deve definir os recursos ou dados corporativos disponíveis nos dispositivos móveis particulares;
§3º O órgão ou entidade não se responsabiliza pelo uso de softwares sem licenças, instalação de hardwares e manutenções nos dispositivos móveis particulares conectados à rede corporativa do órgão ou entidade.
§4º É de inteira responsabilidade do usuário a configuração do dispositivo particular conforme as regras de segurança definidas pelo órgão ou entidade. Para efeitos de gestão, os dispositivos particulares deverão ser recadastrados periodicamente. O período de recadastramento não deve ultrapassar o prazo máximo de 1 (um) ano considerando o cadastro anterior.
§5º O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo particular com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.
§6º Por se tratar de dispositivo particular, é de inteira e exclusiva responsabilidade do proprietário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.
Seção II
DOS DISPOSITIVOS DE PROPRIEDADE OU ALUGADOS PELO ÓRGÃO OU ENTIDADE
Art 21 O dispositivo móvel será de uso e responsabilidade de seu usuário, nos termos do formulário específico assinado no momento de entrega.
Art 22 O dispositivo móvel utilizado também fora do órgão ou entidade, deve ter suas informações armazenadas e protegidas contra acesso indevido, se possível, por meio de criptografia.
Parágrafo único. Os arquivos deverão possuir cópia no servidor do órgão ou entidade, sendo armazenados no diretório reservado à área a qual pertence o usuário responsável pelo equipamento.
Art 23 O usuário é responsável pelos danos decorrentes do mau uso dos dispositivos móveis sob sua responsabilidade.
Art 24 É de inteira responsabilidade do setor de TIC a configuração do dispositivo conforme as regras de segurança definidas pelo órgão ou entidade. Para efeitos de gestão, os dispositivos cedidos ou alugados pelo órgão ou entidade deverão ser avaliados periodicamente.
Art 25 O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo cedido ou alugado com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.
Art 26 Por se tratar de dispositivo cedido ou alugado, é de inteira e exclusiva responsabilidade do usuário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.
CAPÍTULO VI – DA UTILIZAÇÃO DE VÍDEO CONFERÊNCIA
Art 27 É vedada a participação em vídeo conferência utilizando a Internet, exceto quando se tratar de assuntos corporativos e previamente autorizadas pela área de TIC do Órgão ou Entidade.
CAPÍTULO VII – DA UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO
Seção I
DOS DISPOSITIVOS
Art 28 A estação de trabalho será disponibilizada após o usuário assinar o Termo de Responsabilidade.
§1º A utilização das estações de trabalho é permitida apenas a usuários autorizados, mediante a utilização de um login e uma senha, individual e intransferível.
§2º Todo usuário deverá bloquear sua estação de trabalho ou efetuar *logout* da rede corporativa antes de se ausentar do seu local de trabalho.
§3º O usuário deverá desligar a sua estação de trabalho no final do expediente. As exceções devem ser devidamente autorizadas pela área de TIC.
§4º O armazenamento de arquivos pessoais nas estações de trabalho deve ser evitado. Uma vez armazenados, a responsabilidade por tais arquivos é exclusivamente do usuário.
Art 29 Somente equipamentos autorizados pela área de TIC poderão se conectar à rede corporativa do órgão ou entidade.
Art 30 Toda estação de trabalho deverá validar o seu processo de *logon* em um controlador de domínio da rede corporativa do órgão ou entidade, não sendo permitidos acessos por usuários locais.
§1º Em casos excepcionais ou onde não houver controladores de domínio, a área responsável pela segurança da informação deve criar o ambiente priorizando as demais regras de segurança explicitadas nessa resolução.
Seção II
DA INSTALAÇÃO E REMOÇÃO DE SOFTWARES E COMPONENTES

Art 31 Instalações e remoções de softwares deverão ser efetuadas pela área de TIC do órgão ou Entidade destinada a estes fins, a qual detém a guarda das credenciais de administrador dos equipamentos, e somente mediante prévia autorização da chefia imediata do usuário.
§1º Todo software instalado deve ser corretamente licenciado.
§2º Somente softwares homologados pela área responsável pela segurança da informação devem ser instalados nas estações de trabalho. Em caso de inexistência da área responsável pela segurança da informação, a área de TIC do órgão ou entidade fará a devida homologação.
§3º Toda estação de trabalho deverá ter instalado um software anti-malware ou antivírus.
Art 32 Os softwares sem utilização nas estações de trabalho deverão ser desinstalados.
Parágrafo Único. Em caso de necessidades específicas, a instalação poderá ser efetuada mediante justificativa do usuário e com autorização da área de Segurança da Informação ou setor de TIC.
Art 33 Os serviços de expansão, substituição, configuração ou manutenção das estações de trabalho deverão ser executados somente pela área de TIC.
Art 34 Os acessos às estações de trabalho com privilégios de administrador são restritos à área responsável pelo suporte.
Art 35 As exceções à regra do caput deste artigo deverão ser solicitadas justificadamente pela chefia imediata do usuário e liberada após avaliação e autorização da área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.
Seção III
DO BACKUP DAS INFORMAÇÕES
Art 36 O *backup* e a guarda das informações armazenadas nas estações de trabalho são de responsabilidade do usuário. Na existência de um servidor de arquivos administrado pela área de TIC do órgão ou entidade, este deve ser utilizado como ponto central para armazenamento das informações pertinentes à atividade exercida.
CAPÍTULO VIII - DA UTILIZAÇÃO DA INTERNET
Seção I
DOS DISPOSITIVOS GERAIS
Art 37 O serviço de Internet é disponibilizado pelo órgão ou entidade para execução das atividades profissionais dos usuários.
§1º O usuário deverá utilizar a Internet em conformidade com a lei, a moral, os bons costumes aceitos, à ordem pública e com o código de conduta do órgão ou entidade, caso exista.
§2º É facultado ao usuário o emprego da Internet para a melhoria de sua qualificação profissional ou para acesso a serviços, tais como Internet Banking e similares.
§3º O acesso às ferramentas interativas da WEB 2.0 foi regulamentado por meio do decreto 45.241 de 10/12/2009.
Art 38 É vedada a realização de *upload* de qualquer software ou dados de propriedade do órgão ou entidades do governo do Estado sem a autorização expressa da área de Segurança da Informação.
Art 39 O acesso à Internet deverá ser efetuado somente por equipamentos autorizados pela área de TIC e pela rede corporativa do órgão ou entidade. O tempo de acesso poderá ser disponibilizado por meio de cota.
Seção II
DAS CONDIÇÕES PARA ACESSAR A INTERNET
Art 40 É vedada a utilização de modem de banda larga no ambiente dos órgãos e entidades que disponibilizam acesso à rede corporativa.
Parágrafo Único. Mediante solicitação do usuário, a área de Segurança da Informação poderá autorizar a utilização de outras conexões, desde que não haja comprometimento da segurança da rede do órgão ou entidade.
Seção III
DO MONITORAMENTO E BLOQUEIO DE SÍTIOS
Art 41 O órgão ou entidade reserva para si o direito de monitorar o uso da Internet disponibilizada implantando recursos e programas de computador que registrem cada acesso à Internet e que permitam a avaliação do conteúdo dos pacotes de rede, enviados e recebidos e que transitem entre a rede do órgão/entidade e a Internet.
Parágrafo único. O órgão ou entidade deverá possuir mecanismos de autenticação que determinem a titularidade de todos os acessos à Internet realizados por seus usuários.
Art 42 Na provisão de conexão à internet, cabe ao administrador de sistema o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano.
§1° A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
§2° Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Lei 12.965/2014.
Art 43 O órgão ou entidade poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, bem como, que exponham a rede a riscos de segurança.
Parágrafo Único. O desbloqueio de site cujo conteúdo esteja de acordo com esta norma poderá ser realizado pela área de TIC mediante solicitação do usuário informando a URL indevidamente bloqueada.
CAPÍTULO IX – PRIVACIDADE DOS DADOS
Art 44 Recomenda-se que os órgãos e entidades estejam em conformidade a Lei Geral de Proteção de Dados, Lei Nº 13.709 de 14 de agosto de 2018, com o objetivo de garantir a privacidade dos dados pessoais das pessoas e permitir um maior controle sobre eles.
CAPÍTULO X – RECOMENDAÇÕES
Art 45 Recomenda-se:
I .O acesso remoto à rede corporativa do órgão ou entidade em locais públicos deverá ser evitado.
II .Toda informação do órgão ou entidade deverá ser armazenada nos servidores da rede do órgão ou entidade.
III .A senha de acesso aos sistemas e serviços do órgão ou entidade não deverá ser utilizada em sistemas externos.
IV .Não abrir mensagem de correio eletrônico cujo assunto ou remetente sejam de origem desconhecida ou suspeita.
V .Não executar arquivos e anexos de origem desconhecida ou suspeita.
VI .Manter sua mesa de trabalho sempre limpa, sem papéis e mídias expostos.
VII .Evitar discutir assuntos relacionados às atividades profissionais em locais públicos.
VIII .Não divulgar o endereço eletrônico, fornecido pelo órgão ou entidade, para recebimento de mensagens particulares, de entidades alheias aos interesses ou atividades do órgão ou entidade.
IX .Evitar alimentar e ingerir líquidos próximo às estações de trabalho.
X .Não deixar os dispositivos móveis desprotegidos em locais de alto risco de furto e roubo, tais como locais públicos, eventos, hotéis, veículos e outros.
XI .Evitar utilizar outro serviço de correio eletrônico que não seja o institucional nos equipamentos conectados à rede corporativa.
CAPÍTULO XI – DAS VEDAÇÕES
Art 46 É vedado aos usuários:
I .instalar qualquer hardware ou software sem a autorização formal da área de TIC;

II .emprestar o dispositivo móvel corporativo a terceiros ou divulgar dados de configuração de acesso da rede corporativa do órgão ou entidade;
III .acessar, armazenar, divulgar ou repassar qualquer material ligado à pornografia e de conteúdo ilícito, tais como racismo e pedofilia;
IV .armazenar, acessar, divulgar ou repassar qualquer conteúdo que implique na violação de quaisquer leis ou incentive crimes;
V .acessar, propagar ou armazenar qualquer tipo de conteúdo malicioso, *malware*, vírus, *worms*, cavalos de tróia ou programas de controle de outros computadores;
VI .utilizar softwares de comunicação instantânea, mensageiros instantâneos ou programas de computador que permitam a comunicação imediata e direta entre usuários e grupos de usuários por meio da Internet, tais como Facebook, Whatsapp, Allo, Instagram e afins, exceto o mensageiro instantâneo corporativo ou quando solicitado e autorizado pela área de Segurança da Informação;
VII .fazer download de softwares, cópias não autorizadas, vídeos ou áudios não ligados às atividades profissionais;
VIII .utilizar programas de computador, ferramentas, utilitários ou artifícios quaisquer para burlar os mecanismos de segurança dos órgãos ou entidade;
IX .violar os lacres das estações de trabalho, ou de qualquer outro equipamento, ou ainda, abrir equipamentos mesmo que estejam sem lacres;
X .registrar senha em papel ou em qualquer outro meio que coloque em risco a sua confidencialidade;
XI .fornecer a senha de acesso à qualquer sistema/serviço do órgão ou entidade para outro usuário;
XII .acessar qualquer sistema/serviço do órgão ou entidade por meio da identificação de outro usuário;
XIII .tentar obter acesso não autorizado, como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta de acesso. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
XIV .utilizar senhas compartilhadas para acesso a qualquer recurso computacional do órgão ou entidade, exceto nos casos em que seja impossível a implantação de senha individual e devidamente autorizado pela área responsável;
XV .tentar interferir nos serviços de qualquer outro usuário, servidor ou rede, inclusive ataques do tipo negação de serviço - DoS e DDoS, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar ou invadir um servidor.
XVI .conectar equipamentos particulares à rede corporativa sem prévia autorização.
XVII .acessar as estações de trabalho sem autorização do responsável pela unidade.
XVIII .movimentar as estações de trabalho, periféricos e ou equipamentos de rede sem autorização do responsável pelo setor de TIC.
XIX .incluir senhas em processos automáticos, como por exemplo, em arquivos de dados, programas de computador, macros, scripts, ferramentas, teclas de função ou outros, exceto se autorizado pela área de Segurança da Informação e desde que, comprovadamente, não haja comprometimento à segurança da informação.
XX .armazenar informações corporativas do Estado em diretórios (pastas) públicos (as).
Art 47 É vedada a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio como *Access Points*, modem ou qualquer outra solução que estabeleça conexão simultânea com a rede local e outras redes.
Parágrafo Único. Em casos justificados de uso destes equipamentos, o órgão ou entidade deverá prover segmento de rede independente, através de VLAN, para este fim, de forma a permitir o compartilhamento de sua infra-estrutura de TI sem o comprometimento do desempenho e da segurança da rede local.
CAPÍTULO XII – DAS RESPONSABILIDADES
Art 48 Compete ao usuário:
I .obedecer e cumprir a Política de Segurança da Informação do Governo do Estado;
II .notificar à área responsável pela Segurança da Informação casos de suspeita ou violação das regras ou de falhas de segurança da informação;
III .sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;
IV .utilizar e manter o crachá em local visível durante sua permanência nas instalações do órgão ou entidade;
V .avisar à chefia imediata ou ao superior a perda, furto ou o desaparecimento de crachás.
VI .informar à chefia imediata ou ao superior a presença de pessoas sem identificação nas instalações da órgão ou entidade.
VII .devolver o crachá ao término do contrato de trabalho nos casos de exoneração de cargo efetivo, aposentadoria ou desligamento do órgão ou entidade.
VIII .responder pelo uso de seu login de acesso aos sistemas e serviços do órgão ou entidade;
IX .zelar pelas informações, sistemas, serviços e recursos de tecnologia da informação sob sua responsabilidade;
X .não realizar alterações na configuração da estação de trabalho;
XI .utilizar adequadamente os recursos computacionais;
XII .conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade e privacidade;
XIII .alterar a senha no momento em que receber as informações da criação de sua conta;
XIV .manter sigilo de seu *login* e de sua senha de acesso aos sistemas e serviços do órgão ou entidade;
XV. trocar a senha sempre que houver indícios de comprometimento do sistema ou da própria senha;
XVI .guardar as mídias removíveis, contendo dados, em armários com chaves;
XVII .guardar os documentos em papel que contenham informações sigilosas de forma segura e em local fechado;
XVIII .não reproduzir documento sem a autorização do responsável pela informação;
XIX .imprimir documentos, caso sejam sigilosos, utilizando impressoras com proteção por meio de senhas ou permanecer próximo à impressora, no momento de sua emissão;
XX .não reutilizar documentos em papel que possuam conteúdos sigilosos, devendo estes serem descartados por meio de fragmentação;
XXI .eliminar os arquivos desnecessários armazenados nos servidores da rede do órgão ou entidade;
XXII .responder pelo uso de dispositivos particulares no ambiente do órgão ou entidade;
XXIII .solicitar à chefia imediata a utilização e a conexão do dispositivo móvel na rede corporativa justificando a sua necessidade;
XXIV .evitar armazenar informações confidenciais em dispositivos móveis usados fora do órgão ou entidade. Havendo necessidade, tais informações deverão ser transferidas para um local de armazenamento seguro logo que possível;
XXV .ser responsável pelos dispositivos móveis, e pelos dados armazenados nos mesmos, disponibilizados para uso dentro e fora das instalações do órgão ou entidade;
XXVI .não deixar os dispositivos móveis desprotegidos em locais de alto risco, tais como locais públicos, eventos, hotéis, veículos, dentre outros;

XXVII .apresentar em caso de furto, roubo ou extravio do dispositivo móvel a Ocorrência Policial, no prazo máximo de 48 horas do fato ocorrido, à área responsável pelo patrimônio do órgão ou entidade;
XXVIII .apresentar o dispositivo móvel para a área responsável pelo atendimento ao usuário, quando requisitado, ou ao cessar as atividades que motivaram sua solicitação;
XXIX .zelar pela guarda do dispositivo de armazenamento do certificado e pela senha de acesso ao dispositivo.
XXX .requisitar a revogação do certificado digital caso ele seja perdido, roubado ou extraviado, informando imediatamente o fato à área responsável.
Art 49 Compete à área de TIC:
I .cumprir e fazer cumprir a Política de Segurança da Informação;
II .manter os sistemas computacionais e de comunicação em conformidade com a Política de Segurança da Informação;
III .disponibilizar os recursos necessários à implantação da Política de Segurança da Informação;
IV .manter os dados cadastrais dos usuários da rede corporativa, bem como do correio eletrônico, atualizados;
V .reportar incidentes de segurança da informação à área responsável pela Segurança da Informação;
VI .monitorar os logs dos sistemas;
VII .acompanhar a realização de manutenção, corretiva ou preventiva, dos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade quando a manutenção for realizada por terceiros no ambiente do órgão ou entidade;
VIII .prestar suporte ao usuário quando solicitado;
IX .solicitar apoio e consultoria de segurança à área responsável pela Segurança da Informação quando se fizer necessário;
X .solicitar a assinatura do Termo de Responsabilidade do usuário pela estação de trabalho;
XI .instalar e configurar as estações de trabalho;
XII .manter um inventário atualizado das estações de trabalho e dos softwares;
XIII .desenvolver e manter um padrão de instalação e configuração de estações de trabalho aderente aos critérios estabelecidos nesta resolução;
XIV .configurar os programas de computador e equipamentos para garantir a utilização dos critérios relativos às senhas de acesso definidos pela área de Segurança da Informação;
XV .manter o antivírus, anti-spam e as correções de segurança dos servidores e estações de trabalho atualizados;
XVI .lacrar os microcomputadores;
XVII .documentar toda a infraestrutura de TIC do órgão ou entidade, tais como tipo de equipamento, patrimônio, localização física, data da aquisição, prazo de garantia, etc;
XVIII .controlar e descartar os Hard Disks (HDs) e mídias removíveis, quando necessário;
XIX .disponibilizar e administrar a infraestrutura necessária para armazenamento de dados;
XX .disponibilizar e administrar os recursos de acesso à Internet;
XXI .monitorar o uso da Internet;
XXII .registrar os acessos indevidos à Internet;
XXIII .orientar os usuários em relação à proteção adequada dos dispositivos móveis;
XXIV .configurar os dispositivos móveis disponibilizados para os usuários do órgão ou entidade;
XXV .instalar, homologar, manter, atualizar e configurar todos os servidores, subsistemas de armazenamento e programas de computador que componham as soluções de backup e restore utilizadas no órgão ou entidade;
XXVI .manter a documentação dos servidores, subsistemas de armazenamento, e programas de computador diretamente vinculados às soluções de backup e restore;
XXVII .realizar o backup e a remoção das informações armazenadas nos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade, no caso de manutenção externa ao órgão ou entidade;
XXVIII .definir os recursos e ferramentas que serão utilizados em cada procedimento de backup e restore;
XXIX .documentar os procedimentos de backup e restore;
XXX .eliminar e substituir as mídias de backup e restore próximas de perderem sua funcionalidade segundo a vida útil informada pelo fornecedor;
XXXI .eliminar o conteúdo das mídias que serão descartadas;
XXXII .executar os procedimentos de backup e restore;
XXXIII .gerenciar e controlar os recursos computacionais e as mídias utilizadas pelos sistemas de backup e restore do órgão ou entidade;
XXXIV .manter mapa atualizado das mídias e seus conteúdos para todos os procedimentos de backup e restore do órgão ou entidade;
XXXV .planejar junto às áreas solicitantes os procedimentos de backup e restore;
XXXVI .realizar testes de validação e desempenho das cópias de segurança realizadas;
XXXVII .disponibilizar os recursos necessários para a execução das funções de auditoria;
XXXVIII .garantir a proteção adequada das trilhas de auditoria;
XXXIX .aprovar e registrar a utilização das ferramentas de monitoramento e acesso às estações de trabalho;
XL .analisar e despachar os expedientes relativos a solicitações de usuários encaminhadas pelos respectivos responsáveis por suas unidades;
XLI .administrar o acesso remoto à rede do órgão ou entidade;
XLII .definir os softwares autorizados que deverão ser instalados nas estações de trabalho;
XLIII .administrar as redes corporativas do órgão ou entidade;
XLIV .manter a documentação da topologia da rede atualizada e controlar o acesso ao seu conteúdo;
XLV .prover o ambiente físico necessário para instalação dos roteadores e switches;
XLVI .homologar e administrar os roteadores e switches do órgão ou entidade;
XLVII .manter a documentação (topologia, configurações, etc) dos roteadores e switches atualizada;
XLVIII .administrar as regras dos firewalls;
XLIX .instalar, configurar e manter os ambientes operacionais dos firewalls - sistema operacional nos servidores, bem como os produtos e as correções e atualizações de versão;
L .aplicar, anualmente, os controles disponibilizados pela ferramenta de gestão de riscos nos ativos em que estejam instalados os firewalls;
LI .manter atualizadas as documentações (configurações) relativas aos firewalls;
LII .disponibilizar a infraestrutura necessária para o funcionamento da solução de network IDS/IPS;
LIII .instalar e administrar o network IDS/IPS;
LIV .analisar periodicamente as logs dos Networks IDS em busca de incidentes de Segurança da Informação;
LV .avaliar, no mínimo trimestralmente, o desempenho do network IDS/IPS em relação à quantidade de ataques detectados, falsos positivos (alarme falso), carga da rede, entre outros;
LVI .manter a documentação do network IDS/IPS atualizada;

LVII .instalar, homologar, manter e configurar todos os equipamentos de conectividade que componham as soluções de backup e restore utilizadas no órgão ou entidade;
LVIII .definir e implementar rotina automatizada para a cópia das configurações e dados dos equipamentos de conectividade para um servidor de arquivos contemplado por uma das rotinas de backup/restore;
LIX .analisar e emitir parecer sobre as solicitações da área de segurança da informação;
LX .atualizar os controles da ferramenta de análise de risco de Segurança da Informação;
LXI .avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação;
LXII .elaborar e manter atualizado um procedimento de instalação e configuração da rede;
LXIII .administrar a cessão, a alteração, o bloqueio e o cancelamento de acessos à rede corporativa;
LXIV .revisar, pelo menos 1 (uma) vez por ano, os direitos de acesso dos usuários da rede corporativa e realizar as alterações necessárias;
LXV .revisar, pelo menos a cada 6 (seis) meses, os direitos de acesso com privilégios de administrador e realizar as alterações necessárias;
LXVI .definir, homologar, implementar e disponibilizar a infra-estrutura e os mecanismos de segurança para utilização da rede wireless;
LXVII .realizar semestralmente análise de risco na rede wireless;
LXVIII .disponibilizar relatório as conexões remotas realizadas.
LXIX .solicitar a autorização para movimentação patrimonial de ativos (hardware e software) à área de TIC;
Art 50 Compete ao setor de auditoria:
I .realizar a auditoria nos sistemas do órgão ou entidade;
II .verificar a conformidade com o estabelecido nesta norma e recomendar as ações necessárias;
III .definir parâmetros de geração e retenção das trilhas de auditoria, juntamente com a área responsável pela Segurança da Informação, para fins de controle interno;
IV .gerar e manter atualizada a documentação das ferramentas e auditorias realizadas;
V .manter a área responsável pela Segurança da Informação informada sobre as ferramentas utilizadas;
VI .monitorar a utilização das userid de auditoria.
Art 51 Compete à área de recursos humanos informar, mensalmente, à equipe de Segurança da Informação, a movimentação de pessoal no órgão ou entidade.
Art 52 Compete à direção das unidades administrativas:
I .orientar os usuários sob sua coordenação sobre o cumprimento desta resolução e zelar pelo acesso aos sistemas e serviços do órgão ou entidade;
II .cumprir e fazer cumprir a Política de Segurança da Informação em relação aos seus subordinados;
III .monitorar as atividades de parceiros e contratados sob sua responsabilidade;
IV .colaborar com a área responsável pela Segurança da Informação na elaboração da Política de Segurança da Informação;
V .propor mudanças na Política de Segurança da Informação de acordo com as necessidades iminentes detectadas na sua área de atuação;
VI .reportar, de imediato, à área responsável pela Segurança da Informação, qualquer incidente de segurança detectado ou, até mesmo, qualquer suspeita ou ameaça de incidentes;
VII .avaliar a necessidade de utilização de dispositivo móvel particular e da conexão à rede corporativa do órgão ou entidade;
VIII .solicitar à área de TIC qualquer alteração nas condições autorizadas para a utilização de dispositivo móvel;
IX .solicitar as permissões de acesso para usuários sob sua subordinação à área executora que detenha o controle de acesso ao respectivo recurso computacional;
X .solicitar, com a devida justificativa, para área de TIC a instalação de softwares.
Art 53 Compete à área responsável pela Segurança da Informação:
I .elaborar a Política de Segurança da Informação;
II .verificar o cumprimento desta Resolução e recomendar as ações preventivas e ou corretivas necessárias;
III .administrar, controlar e dar tratamento aos incidentes de segurança da informação;
IV .analisar e autorizar solicitação para conexão na rede corporativa de mídias ou dispositivo móvel particular nas dependências do órgão ou entidade;
V .autorizar, quando necessário, a criação de regras no firewall, considerando a análise de risco realizada;
VI .analisar e emitir parecer sobre as informações de incidentes de segurança ou inconformidades;
VII .aprovar controle de segurança;
VIII .avaliar e apresentar pareceres a respeito das exceções requeridas pelos responsáveis de unidades administrativas do órgão ou entidade;
IX .avaliar, periodicamente, a Segurança da Informação, por meio de análise de indicadores e recomendar ações corretivas e preventivas;
X .definir e padronizar os critérios das senhas de acesso à rede;
XI .elaborar campanhas e programas de treinamento e de conscientização em Segurança da Informação;
XII .elaborar relatórios gerenciais sobre o acesso à Internet;
XIII .elaborar, propor e coordenar projetos, ações e soluções de segurança da informação;
XIV .emitir relatório de alerta e incidente de segurança quando detectado acesso indevido à Internet;
XV .especificar padrão de configuração de segurança destinada a acesso remoto à rede corporativa;
XVI .garantir a implementação dos projetos e soluções de segurança da informação aprovados, atuando permanentemente em busca de parcerias com os diversos responsáveis pelos processos, visando à redução do índice de riscos do órgão ou entidade;
XVII .homologar junto à área de TIC os procedimentos de backup e restore;
XVIII .homologar padrões definidos pela área de redes;
XIX .homologar parâmetros de configuração dos IDS/IPS;
XX .homologar, autorizar e validar o uso de equipamentos e programas de computador nas estações de trabalho quando não existir licença de uso ou o software solicitado for desconhecido ou passível de risco de segurança;
XXI .priorizar as ações de segurança;
XXII .prover apoio técnico consultivo para as unidades administrativas do órgão ou entidade nas questões relativas à segurança da informação;
XXIII .recomendar a adoção de soluções emergenciais sobre segurança da informação;
XXIV .recomendar soluções, ferramentas ou recursos que viabilizem o monitoramento e o registro dos acessos à internet;
XXV .realizar análise de riscos em equipamentos, infraestrutura e pessoas;
XXVI .avaliar o nível de segurança alcançado, emitindo relatórios periódicos de Análise de Riscos à Diretoria e ao Comitê Gestor;
XXVII .definir e acompanhar a execução do Plano Estratégico para implantação da Política de Segurança da Informação;
XXVIII .definir e aprovar junto à alta gestão, os procedimentos e penalidades para se fazer cumprir a Política de Segurança;

XXIX .definir e solicitar os recursos necessários para implantação da Política de Segurança;
XXX .efetuar mudanças na Política de Segurança da Informação sempre que houver alteração no ambiente computacional ou atualizações tecnológicas, visando à manutenção e melhora do nível de segurança;
XXXI .realizar análise de risco para criação de regras no firewall e gerar laudo técnico;
XXXII .dar tratamento aos casos de exceção e aqueles não previstos nas normas relativas à segurança da informação.
XXXIII .aprovar, quando devido, as solicitações de acessos à rede corporativa com privilégios de administrador;
XXXIV .analisar os incidentes de segurança da informação e recomendar ações corretivas e preventivas;
XXXV .realizar, no mínimo anualmente, uma análise crítica dos direitos de acesso dos usuários sob sua coordenação e solicitar as alterações necessárias;
XXXVI .monitorar a utilização de mídias particulares para armazenamento de informações do órgão ou entidade;
XXXVII .tomar as providências cabíveis em caso de descumprimento da Política de Segurança da Informação por seus subordinados;
XXXVIII .analisar permanentemente os acessos remotos realizados por seus subordinados, através de relatório disponibilizado pela área de TIC;
XXXIX .receber, analisar e encaminhar a solicitação de permissão e revogação de acesso para o empregado ou prestador de serviço sob sua subordinação à área de TIC;
XL .informar, em caso de solicitações temporárias, o período em que a utilização da conexão permanecerá liberada, para visitantes e demais usuários;
XLI .avaliar as solicitações para o uso de dispositivo móvel de propriedade ou alugado pelo órgão ou entidade e requerer à área de TIC;
XLII .autorizar, quando necessário, a liberação de portas de diagnóstico remotas;
XLIII .autorizar acessos à rede;
XLIV .informar à Companhia de Tecnologia da Informação do Estado de Minas Gerais – Prodemge, pelo menos 2 gestores de segurança, que terão a função de tratar qualquer assunto relacionado a segurança da informação.
XLV .manter e publicar anualmente um programa de conscientização sobre a segurança da informação;
XLVI .informar anualmente à Superintendência Central de Governança Eletrônica - SCGE da Secretaria de Estado de Planejamento e Gestão - SEPLAG quais as ferramentas de segurança possuem, descrevendo pelo menos, a função, o fabricante, a versão utilizada e a indicação da existência de contrato de manutenção.
CAPÍTULO XIII – PENALIDADES
Art 54 O usuário que não cumprir as normas estabelecidas nessa Resolução estará sujeito às penalidades previstas em Lei.
CAPÍTULO XIV – DISPOSIÇÕES FINAIS
Art 55 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 56 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 57 Caberá à Secretaria de Estado de Planejamento e Gestão, por meio da Subsecretaria de Gestão, esclarecer os casos omissos a esta Resolução.
Art 58 Este Decreto entra em vigor na data de sua publicação, revogada a Resolução SEPLAG n° 73 de 21 de setembro de 2009.
Belo Horizonte, aos 26 de dezembro de 2018.

HELVÉCIO MIRANDA MAGALHÃES JUNIOR
Secretário de Estado de Planejamento e Gestão

26 1179282 – 1

GOVERNO DO ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO
Gabinete

N.1500.01.0026293/2018-87 /2018

RESOLUÇÃO SEPLAG Nº 107, DE 26 DE DEZEMBRO DE 2018

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

O SECRETÁRIO DE ESTADO DE PLANEJAMENTO E GESTÃO, no uso das atribuições que lhe conferem o artigo 93, § 1º, inciso III, da Constituição do Estado e o artigo 6º, §2º do Decreto estadual nº. 46.765, de 26 de maio de 2015,

RESOLVE:

CAPÍTULO I – DAS DISPOSIÇÕES GERAIS
Seção I
DISPOSIÇÕES PRELIMINARES

Art 1º O acesso lógico à rede corporativa, a concessão de acesso remoto à rede corporativa, a utilização de senhas dos sistemas e serviços, o armazenamento de informações, a utilização de dispositivos móveis, a utilização do correio eletrônico, a utilização das estações de trabalho, a utilização da Internet e a conduta dos usuários de informações no âmbito dos órgãos e entidades do Governo do Estado de Minas Gerais observam o disposto nesta Resolução.

Art 2º É constituída por um conjunto de diretrizes e regras que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas por suas unidades administrativas e visa atender aos seguintes princípios:
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas devidamente autorizadas;
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Autenticidade: garantia da identidade de quem está enviando a informação;
- Legalidade: Garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

Art 3º Aplica-se a presente resolução a todos os usuários dos órgãos e entidades do Governo do estado de Minas Gerais, seja ele nomeado, designado, contratado ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública. Aplica-se também a fornecedores no desempenho de alguma atividade internamente no órgão ou entidade do Governo do estado.

Seção II
DAS DEFINIÇÕES

Art 4º 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 entre dispositivos (microcomputadores, servidores, etc), por meio da rede de comunicação de dados corporativa. Quando se tratar de redes corporativas distintas o mesmo deverá ser realizado por meio de VPN;
III .administrador: contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configurados, normalmente não disponíveis a todos os usuários;
IV .análise de riscos: processo completo de análise dos pontos críticos que possam oferecer ameaças ao ambiente tecnológico;
V .antimalware: ferramenta destinada a detecção, anulação e remoção de códigos maliciosos (malware).
VI .*antispyware:* programa que permite identificar e remover códigos maliciosos que se auto instalam nos computadores;
VII .antivírus: programa que permite identificar e eliminar vírus em computadores;
VIII .ataque do tipo negação de serviço – DoS do inglês Denial of Service): um ataque de negação de serviço é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Não se trata de uma invasão do sistema, mas sim de provocar a sua indisponibilidade por sobrecarga.
IX .ataque distribuído por negação de serviço - DDoS, do inglês Distributed Denial-of-Service attack): definição semelhante ao Ataque do tipo Negação de Serviço (DoS) sendo que a diferença básica entre um ataque de DoS e de DDoS é que neste último, os ataques são realizados por diversas máquinas simultaneamente, o que aumenta a possibilidade de êxito. As máquinas utilizadas nos ataques de DDoS são denominadas zumbis.
X .autenticação: é um processo de verificação da identidade que consta em um sistema, ou seja, o sistema verifica as credenciais de quem está tentando acessar, com as que constam na base de dados, caso positivo, o sistema é liberado pois as credenciais foram validadas.
XI .autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui, certificada por instrumento ou testemunho público;
XII .*backup*: significa cópia de segurança. Serve para copiar dados de um dispositivo de armazenamento para outra fonte segura que poderá ser utilizada futuramente.
XIII .BYOD - Bring your own device (BYOD): refere-se à política de permitir que os empregados possam trazer dispositivos de propriedade pessoal (laptops, tablets e telefones inteligentes) para seu local de trabalho e usar esses dispositivos para acessar informações e aplicações dos Órgãos e Entidades;
XIV .certificado digital: arquivo eletrônico, assinado digitalmente por uma Autoridade Certificadora, que contém dados de uma pessoa física ou jurídica, utilizados para comprovar sua identidade. O certificado digital é armazenado em uma mídia ou em um dispositivo de hardware;
XV .*chat*: palavra que em português significa "conversação" e é um neologismo para designar aplicações de conversação em "tempo real";
XVI .chefia imediata: titular da área a qual está subordinado o usuário. Na sua ausência deve ser observada a ordem hierárquica superior;
XVII .computação em nuvem: fornecimento de recursos computacionais pela internet (nuvem), sob demanda, por meio de uma plataforma de serviços;
XVIII .confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;
XIX .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;
XX .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;
XXI .correio eletrônico: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;
XXII .crachá: identificação, pessoal e intransferível, disponibilizada ao usuário para acesso físico às dependências do órgão ou entidade;
XXIII .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;
XXIV .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;
XXV .disponibilidade: garantia de que os usuários autorizados obtenham acesso tempestivo (no momento da solicitação) à informação e aos ativos correspondentes;
XXVI .dispositivo móvel: equipamentos com capacidade de armazenamento e processamento de dados, de fácil locomoção, interligados ou não à rede corporativa do órgão ou entidade, tais como notebooks, smartphones, Tablets e Coletores de Dados;
XXVII .domínio: identificação de nomes da Internet, utilizada para prover o acesso a endereços de computador, a qualquer programa de comunicação;
XXVIII .*download:* transferência de um arquivo de um computador para outro por meio da Internet;
XXIX .e-mail: vide "correio eletrônico";
XXX .estação de trabalho: computadores e notebooks do órgão ou entidade interligados ou não à rede corporativa;
XXXI .ferramenta de auditoria: software que armazena os eventos gerados no ambiente computacional, permitindo a rastreabilidade da configuração e da utilização dos sistemas;
XXXII .firewall: é um sistema de segurança de rede que monitora e controla o tráfego de entrada e de saída da rede com base em regras de segurança pré-determinadas. Um firewall geralmente estabelece uma barreira de segurança entre uma rede interna confiável e outra rede externa, como a Internet, que se assume não segura ou confiável.
XXXIII .hardware: todo e qualquer dispositivo físico em um computador;
XXXIV .IDS (*Intrusion Detection System*): sistema de detecção de intrusão que permite identificar atividades suspeitas na rede;
XXXV .incidente de segurança da informação: um ou mais eventos de segurança da informação, indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
XXXVI .integridade: salvaguarda da exatidão e completeza da informação;
XXXVII .internet: rede mundial de computadores;
XXXVIII .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;
XXXIX .IOT (*Internet of Things*): também conhecida como Internet das coisas, permite a detecção e controle remoto de objetos por meio de infraestrutura de rede existente, possibilitando a integração do mundo físico com sistemas baseados em computadores. Engloba tecnologias como as redes inteligentes, casas inteligentes, transporte inteligente e cidades inteligentes.
XL .IPS .(*Intrusion Prevention System*): sistema de prevenção de ataques que permite que atividades suspeitas na rede sejam bloqueadas de forma preventiva;
XLI .licença de software: direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes;
XLII .*log*: arquivos que contenham informações sobre eventos de qualquer natureza em um sistema computacional com o objetivo de permitir o rastreamento de atividades;
XLIII .*login*: identificação do usuário para acesso aos sistemas e serviços;
XLIV .*logon:* processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema;
XLV .*logout:* processo de saída de um usuário dos sistemas e serviços;
XLVI .malware: Software malicioso destinado a extração/alteração de informações de forma ilícita.
XLVII .mecanismos de segurança: conjunto de hardwares e softwares utilizados na implantação de regras de segurança para o ambiente.
XLVIII .mídias: meio físico utilizado para armazenar dados;
XLIX .modem: equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações;
L .normas: especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes;
LI .órgão ou entidade pública: qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas;
LII .*patch(es)* - é um programa criado para atualizar ou corrigir um software.
LIII .*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;
LIV .phishing: investida de cibercriminosos almejando a obtenção de informações pessoais, geralmente identidades online, por meio de e-mails falsos ou redirecionamentos a sites ilusórios.
LV .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;
LVI .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;
LVII .proteção: vide "controle";
LVIII .ransomware: É um tipo de malware (software malicioso) que tem a capacidade de tornar dados disponíveis no equipamento totalmente inacessíveis através de criptografia e, em seguida, solicita o pagamento de resgate em troca da chave de decodificação que é necessária para recuperar as informações contidas nos arquivos criptografados;
LIX .recursos computacionais: recursos tecnológicos que suportam as informações do órgão ou entidade;
LX .rede corporativa: computadores e outros dispositivos interligados que compartilham informações ou recursos do órgão ou entidade;
LXI .*restore*: recuperação de dados armazenados em cópias de segurança;
LXII .risco: combinação da probabilidade de um evento e de suas consequências;
LXIII .roteador: dispositivo de rede responsável por encaminhar pacotes de dados entre redes distintas criando um conjunto de redes de sobreposição;
LXIV .segurança da informação: A segurança da informação (SI) está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.

LXV .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
LXVI .serviço: sistemas e ferramenta de trabalho disponibilizados ao usuários de TIC, como correio eletrônico e acesso à Internet e intranet, acessível na rede do órgão ou entidade;
LXVII .servidor: computador responsável pelo compartilhamento de recursos e execução de serviços solicitados pelos demais computadores a ele conectados;
LXVIII .sistema: vide "sistema de informação automatizado";
LXIX .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;
LXX .sistema operacional: programa ou conjunto de programas que responde pelo controle da alocação dos recursos do computador
LXXI .*site*: vide "sítio";
LXXII .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;
LXXIII .software: programa de computador;
LXXIV .software de comunicação instantânea: aplicação que permite o envio e recebimento de documentos diversos, imagens, mensagens de texto, vídeo e voz em tempo real;
LXXV .*spam*: mensagem de correio eletrônico não solicitada, enviada em larga escala para uma lista de e-mails, fóruns ou grupos de discussão;
LXXVI .*spyware:* programa espião que monitora a atividade de um computador podendo transmitir estas informações a um receptor na Internet, sem o conhecimento e consentimento do usuário;
LXXVII .*streaming*: tecnologia que permite a transmissão contínua de informação multimídia (áudio e vídeo) por meio de pacotes, utilizando redes de computadores, sobretudo a Internet;
LXXVIII .Switch: dispositivo utilizado para interconexão de computadores, possibilitando o encaminhamento de pacotes entre os diversos nós da rede.
LXXIX .terceiro: pessoa jurídica ou física contratada pelo órgão ou entidade para realizar serviços;
LXXX .trilha de auditoria: histórico das transações dos sistemas contendo registro dos usuários que as efetuaram e das tentativas de acesso indevido;
LXXXI .unidade administrativa: cada área que compõe a estrutura organizacional do órgão ou entidade;
LXXXII .*upload*: transferência de um arquivo, de qualquer natureza, do computador do usuário, para algum equipamento da Internet;
LXXXIII .URL (*Universal Resource Locator*): *link* ou endereço de uma página *web*;
LXXXIV .*userid*: identificação do usuário no recurso computacional;
LXXXV .usuário: todo aquele que possui permissão de acesso à rede corporativa e 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;
LXXXVI .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;
LXXXVII .VPN (*Virtual Private Network*) – forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tal como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação;
LXXXVIII .*webmail*: interface web do correio eletrônico;
LXXXIX .wireless*:* sistema de comunicação que não requer fios, funcionando por meio de equipamentos que usam radiofrequência ou comunicação via ondas de rádio para transportar sinais;
XC .*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.
XCI .atividades profissionais: atividades necessárias e suficientes ao desempenho das tarefas do agente público no órgão ou entidade.

CAPÍTULO II – DO ACESSO À REDE CORPORATIVA DO ÓRGÃO OU ENTIDADE

Seção I
DISPOSIÇÕES PRELIMINARES

Art 5º A concessão de acesso à rede corporativa do órgão ou entidade será realizada mediante solicitação formal dos responsáveis pela área do usuário.

Art 6º O referido acesso permitirá ao usuário utilizar os equipamentos e os recursos disponíveis aos demais usuários com o mesmo perfil.

Art 7º As conexões realizadas e os serviços disponibilizados na rede corporativa do órgão ou entidade serão limitados, controlados e autorizados pela área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.

Art 8º Os acessos autorizados para os usuários restringir-se-ão às atividades profissionais pertinentes aos processos e negócios do órgão ou entidade.

Seção II
DO BLOQUEIO, ALTERAÇÃO E CANCELAMENTO DE ACESSOS

Art 9º Os acessos dos usuários desligados deverão ser bloqueados ou revogados no momento em que o desligamento for informado pela área de Recursos Humanos ou chefia imediata.

Art 10 Deverão ter seus acessos bloqueados os usuários em licença ou afastamento.

Art 11 A cessão, a alteração e o cancelamento de acesso com privilégio de administrador na rede corporativa e nas estações de trabalho serão realizados somente mediante autorização da área de Segurança da Informação do Órgão ou Entidade. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.

Seção III
DO MONITORAMENTO

Art 12 Documentar-se-ão as informações dos usuários cadastrados e seus acessos à rede corporativa do Órgão ou Entidade, sendo o nome completo e CPF ou MASP/Matrícula o mínimo necessário.
Parágrafo Único - Registrar-se-á por meio de logs todo acesso à rede corporativa e às redes externas, sendo que a guarda dos mesmos deverá ser realizada por no mínimo 1 ano.

Seção IV
DO ACESSO REMOTO À REDE CORPORATIVA

Art 13 Disponibilizar-se-á ao usuário o acesso remoto somente por meio de VPN e para a execução de atividades relacionadas ao órgão ou entidade.
Parágrafo Único - O órgão ou entidade reserva para si o direito de monitorar a utilização do acesso remoto disponibilizado.

CAPÍTULO III – SENHAS

Art 14 As identificações e as senhas para acesso à rede corporativa são de uso pessoal e intransferível.
§1º Na liberação da identificação para o usuário será fornecida uma senha temporária, que dever ser alterada no primeiro acesso.
§2º A senha de acesso deverá seguir as seguintes regras:
- Deve conter pelo menos 8 (oito) caracteres;
- Deve ser composta de caracteres de 3 das 4 categorias abaixo:
- Ao menos um caractere maiúsculo (A-Z);
- Ao menos um caractere minúsculo (a-z);
- Ao menos um digito (0-9);
- Ao menos um caractere não alfabético (do teclado)(ex !$@%...).
- Não conter mais de 2 caracteres idênticos consecutivos;
§3º A senha deverá ser trocada sempre que existir qualquer indício de comprometimento da rede corporativa ou da própria senha ou, no máximo, a cada 90 dias.
§4º É proibida a reutilização, pelo usuário, das últimas 05 (cinco) senhas.
§5º A manutenção do sigilo da senha é de responsabilidade do usuário.
§6º As senhas para acesso ao mainframe devem respeitar as particularidades da tecnologia deste ambiente.

Art 15 As senhas para acesso à rede corporativa serão armazenadas e transmitidas criptografadas.

Art 16 O acesso será bloqueado automaticamente após 03 (três) tentativas incorretas e consecutivas de *logon* a rede.

Parágrafo único. O acesso é desbloqueado mediante solicitação do usuário à área de Segurança da Informação ou a área de TIC responsável pelo controle de usuários. O desbloqueio ocorrerá somente após comprovação de dados pessoais.

CAPÍTULO IV – DO ARMAZENAMENTO DE INFORMAÇÕES

Art 17 Os servidores de arquivos disponibilizados na rede corporativa serão utilizados exclusivamente para armazenamento de arquivos que contenham informações relacionadas a atividades profissionais pertinentes aos processos e negócios do órgão ou entidade.
§1º A utilização do espaço nos servidores de arquivo da rede do órgão ou entidade é limitada, controlada e monitorada.
§2º O órgão ou entidade reserva para si o direito de auditar a utilização do espaço disponibilizado a fim de identificar arquivos em desacordo com as diretrizes supracitadas e consequentemente, tomar as devidas providências administrativas para apuração de responsabilidade.

Art 18 As informações corporativas deverão ser armazenadas em diretórios disponibilizados nos servidores da rede do órgão ou entidade, com acesso restrito ao grupo de usuários que as utilizam.

CAPÍTULO V – UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS PARTICULARES

Seção I
DOS DISPOSITIVOS PARTICULARES

Art 19 Entende-se por equipamento particular todo o dispositivo que não foi fornecido pelo órgão ou entidade para o desenvolvimento das atividades profissionais.

Art 20 A guarda e manutenção de dispositivos particulares não é responsabilidade do órgão ou entidade.
§1º É permitida a utilização de dispositivo móvel particular e da conexão à rede coorporativa do órgão ou entidade, desde que haja uma solicitação da chefia imediata e a autorização da área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.
§2º O órgão ou entidade deve definir os recursos ou dados corporativos disponíveis nos dispositivos móveis particulares;
§3º O órgão ou entidade não se responsabiliza pelo uso de softwares sem licenças, instalação de hardwares e manutenções nos dispositivos móveis particulares conectados à rede corporativa do órgão ou entidade.
§4º É de inteira responsabilidade do usuário a configuração do dispositivo particular conforme as regras de segurança definidas pelo órgão ou entidade. Para efeitos de gestão, os dispositivos particulares deverão ser recadastrados periodicamente. O período de recadastramento não deve ultrapassar o prazo máximo de 1 (um) ano considerando o cadastro anterior.
§5º O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo particular com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.
§6º Por se tratar de dispositivo particular, é de inteira e exclusiva responsabilidade do proprietário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.

Seção II
DOS DISPOSITIVOS DE PROPRIEDADE OU ALUGADOS PELO ÓRGÃO OU ENTIDADE

Art 21 O dispositivo móvel será de uso e responsabilidade de seu usuário, nos termos do formulário específico assinado no momento de entrega.

Art 22 O dispositivo móvel utilizado também fora do órgão ou entidade, deve ter suas informações armazenadas e protegidas contra acesso indevido, se possível, por meio de criptografia.
Parágrafo único. Os arquivos deverão possuir cópia no servidor do órgão ou entidade, sendo armazenados no diretório reservado à área a qual pertence o usuário responsável pelo equipamento.

Art 23 O usuário é responsável pelos danos decorrentes do mau uso dos dispositivos móveis sob sua responsabilidade.

Art 24 É de inteira responsabilidade do setor de TIC a configuração do dispositivo conforme as regras de segurança definidas pelo órgão ou entidade. Para efeitos de gestão, os dispositivos cedidos ou alugados pelo órgão ou entidade deverão ser avaliados periodicamente.

Art 25 O órgão ou entidade poderá, sem aviso prévio, suspender a conexão do dispositivo cedido ou alugado com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas.

Art 26 Por se tratar de dispositivo cedido ou alugado, é de inteira e exclusiva responsabilidade do usuário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall.

CAPÍTULO VI – DA UTILIZAÇÃO DE VÍDEO CONFERÊNCIA

Art 27 É vedada a participação em vídeo conferência utilizando a Internet, exceto quando se tratar de assuntos corporativos e previamente autorizadas pela área de TIC do Órgão ou Entidade.

CAPÍTULO VII – DA UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

Seção I
DOS DISPOSITIVOS

Art 28 A estação de trabalho será disponibilizada após o usuário assinar o Termo de Responsabilidade.
§1º A utilização das estações de trabalho é permitida apenas a usuários autorizados, mediante a utilização de um login e uma senha, individual e intransferível.
§2º Todo usuário deverá bloquear sua estação de trabalho ou efetuar *logout* da rede corporativa antes de se ausentar do seu local de trabalho.
§3º O usuário deverá desligar a sua estação de trabalho no final do expediente. As exceções devem ser devidamente autorizadas pela área de TIC.
§4º O armazenamento de arquivos pessoais nas estações de trabalho deve ser evitado. Uma vez armazenados, a responsabilidade por tais arquivos é exclusivamente do usuário.
Art 29 Somente equipamentos autorizados pela área de TIC poderão se conectar à rede corporativa do órgão ou entidade.

Art 30 Toda estação de trabalho deverá validar o seu processo de *logon* em um controlador de domínio da rede corporativa do órgão ou entidade, não sendo permitidos acessos por usuários locais.
§1º Em casos excepcionais ou onde não houver controladores de domínio, a área responsável pela segurança da informação deve criar o ambiente priorizando as demais regras de segurança explicitadas nessa resolução.

Seção II
DA INSTALAÇÃO E REMOÇÃO DE SOFTWARES E COMPONENTES

Art 31 Instalações e remoções de softwares deverão ser efetuadas pela área de TIC do órgão ou Entidade destinada a estes fins, a qual detém a guarda das credenciais de administrador dos equipamentos, e somente mediante prévia autorização da chefia imediata do usuário.
§1º Todo software instalado deve ser corretamente licenciado.
§2º Somente softwares homologados pela área responsável pela segurança da informação devem ser instalados nas estações de trabalho. Em caso de inexistência da área responsável pela segurança da informação, a área de TIC do órgão ou entidade fará a devida homologação.
§3º Toda estação de trabalho deverá ter instalado um software anti-malware ou antivírus.

Art 32 Os softwares sem utilização nas estações de trabalho deverão ser desinstalados.
Parágrafo Único. Em caso de necessidades específicas, a instalação poderá ser efetuada mediante justificativa do usuário e com autorização da área de Segurança da Informação ou setor de TIC.

Art 33 Os serviços de expansão, substituição, configuração ou manutenção das estações de trabalho deverão ser executados somente pela área de TIC.

Art 34 Os acessos às estações de trabalho com privilégios de administrador são restritos à área responsável pelo suporte.

Art 35 As exceções à regra do caput deste artigo deverão ser solicitadas justificadamente pela chefia imediata do usuário e liberada após avaliação e autorização da área responsável pela segurança da informação. Caso não exista a referida área, as regras serão analisadas pela área de TIC do Órgão.

Seção III

DO BACKUP DAS INFORMAÇÕES

Art 36 O *backup* e a guarda das informações armazenadas nas estações de trabalho são de responsabilidade do usuário. Na existência de um servidor de arquivos administrado pela área de TIC do órgão ou entidade, este deve ser utilizado como ponto central para armazenamento das informações pertinentes à atividade exercida.

CAPÍTULO VIII - DA UTILIZAÇÃO DA INTERNET

Seção I

DOS DISPOSITIVOS GERAIS

Art 37 O serviço de Internet é disponibilizado pelo órgão ou entidade para execução das atividades profissionais dos usuários.
§1º O usuário deverá utilizar a Internet em conformidade com a lei, a moral, os bons costumes aceitos, à ordem pública e com o código de conduta do órgão ou entidade, caso exista.
§2º É facultado ao usuário o emprego da Internet para a melhoria de sua qualificação profissional ou para acesso a serviços, tais como Internet Banking e similares.
§3º O acesso às ferramentas interativas da WEB 2.0 foi regulamentado por meio do decreto 45.241 de 10/12/2009.

Art 38 É vedada a realização de *upload* de qualquer software ou dados de propriedade do órgão ou entidades do governo do Estado sem a autorização expressa da área de Segurança da Informação.

Art 39 O acesso à Internet deverá ser efetuado somente por equipamentos autorizados pela área de TIC e pela rede corporativa do órgão ou entidade. O tempo de acesso poderá ser disponibilizado por meio de cota.

Seção II

DAS CONDIÇÕES PARA ACESSAR A INTERNET

Art 40 É vedada a utilização de modem de banda larga no ambiente dos órgãos e entidades que disponibilizam acesso à rede corporativa.
Parágrafo Único. Mediante solicitação do usuário, a área de Segurança da Informação poderá autorizar a utilização de outras conexões, desde que não haja comprometimento da segurança da rede do órgão ou entidade.

Seção III

DO MONITORAMENTO E BLOQUEIO DE SÍTIOS

Art 41 O órgão ou entidade reserva para si o direito de monitorar o uso da Internet disponibilizada implantando recursos e programas de computador que registrem cada acesso à Internet e que permitam a avaliação do conteúdo dos pacotes de rede, enviados e recebidos e que transitem entre a rede do órgão/entidade e a Internet.
Parágrafo único. O órgão ou entidade deverá possuir mecanismos de autenticação que determinem a titularidade de todos os acessos à Internet realizados por seus usuários.

Art 42 Na provisão de conexão à internet, cabe ao administrador de sistema o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano.
§1° A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
§2° Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Lei 12.965/2014.

Art 43 O órgão ou entidade poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, bem como, que exponham a rede a riscos de segurança.
Parágrafo Único. O desbloqueio de site cujo conteúdo esteja de acordo com esta norma poderá ser realizado pela área de TIC mediante solicitação do usuário informando a URL indevidamente bloqueada.

CAPÍTULO IX – PRIVACIDADE DOS DADOS

Art 44 Recomenda-se que os órgãos e entidades estejam em conformidade a Lei Geral de Proteção de Dados, Lei Nº 13.709 de 14 de agosto de 2018, com o objetivo de garantir a privacidade dos dados pessoais das pessoas e permitir um maior controle sobre eles.

CAPÍTULO X – RECOMENDAÇÕES

Art 45 Recomenda-se:
I .O acesso remoto à rede corporativa do órgão ou entidade em locais públicos deverá ser evitado.
II .Toda informação do órgão ou entidade deverá ser armazenada nos servidores da rede do órgão ou entidade.
III .A senha de acesso aos sistemas e serviços do órgão ou entidade não deverá ser utilizada em sistemas externos.
IV .Não abrir mensagem de correio eletrônico cujo assunto ou remetente sejam de origem desconhecida ou suspeita.
V .Não executar arquivos e anexos de origem desconhecida ou suspeita.
VI .Manter sua mesa de trabalho sempre limpa, sem papéis e mídias expostos.
VII .Evitar discutir assuntos relacionados às atividades profissionais em locais públicos.
VIII .Não divulgar o endereço eletrônico, fornecido pelo órgão ou entidade, para recebimento de mensagens particulares, de entidades alheias aos interesses ou atividades do órgão ou entidade.
IX .Evitar alimentar e ingerir líquidos próximo às estações de trabalho.
X .Não deixar os dispositivos móveis desprotegidos em locais de alto risco de furto e roubo, tais como locais públicos, eventos, hotéis, veículos e outros.
XI .Evitar utilizar outro serviço de correio eletrônico que não seja o institucional nos equipamentos conectados à rede corporativa.

CAPÍTULO XI – DAS VEDAÇÕES

Art 46 É vedado aos usuários:
I .instalar qualquer hardware ou software sem a autorização formal da área de TIC;
II .emprestar o dispositivo móvel corporativo a terceiros ou divulgar dados de configuração de acesso da rede corporativa do órgão ou entidade;
III .acessar, armazenar, divulgar ou repassar qualquer material ligado à pornografia e de conteúdo ilícito, tais como racismo e pedofilia;
IV .armazenar, acessar, divulgar ou repassar qualquer conteúdo que implique na violação de quaisquer leis ou incentive crimes;
V .acessar, propagar ou armazenar qualquer tipo de conteúdo malicioso, *malware*, vírus, *worms*, cavalos de tróia ou programas de controle de outros computadores;
VI .utilizar softwares de comunicação instantânea, mensageiros instantâneos ou programas de computador que permitam a comunicação imediata e direta entre usuários e grupos de usuários por meio da Internet, tais como Facebook, Whatsapp, Allo, Instagram e afins, exceto o mensageiro instantâneo corporativo ou quando solicitado e autorizado pela área de Segurança da Informação;
VII .fazer download de softwares, cópias não autorizadas, vídeos ou áudios não ligados às atividades profissionais;
VIII .utilizar programas de computador, ferramentas, utilitários ou artifícios quaisquer para burlar os mecanismos de segurança dos órgãos ou entidade;
IX .violar os lacres das estações de trabalho, ou de qualquer outro equipamento, ou ainda, abrir equipamentos mesmo que estejam sem lacres;
X .registrar senha em papel ou em qualquer outro meio que coloque em risco a sua confidencialidade;
XI .fornecer a senha de acesso à qualquer sistema/serviço do órgão ou entidade para outro usuário;
XII .acessar qualquer sistema/serviço do órgão ou entidade por meio da identificação de outro usuário;
XIII .tentar obter acesso não autorizado, como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta de acesso. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
XIV .utilizar senhas compartilhadas para acesso a qualquer recurso computacional do órgão ou entidade, exceto nos casos em que seja impossível a implantação de senha individual e devidamente autorizado pela área responsável;
XV .tentar interferir nos serviços de qualquer outro usuário, servidor ou rede, inclusive ataques do tipo negação de serviço - DoS e DDoS, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar ou invadir um servidor.
XVI .conectar equipamentos particulares à rede corporativa sem prévia autorização.
XVII .acessar as estações de trabalho sem autorização do responsável pela unidade.
XVIII .movimentar as estações de trabalho, periféricos e ou equipamentos de rede sem autorização do responsável pelo setor de TIC.
XIX .incluir senhas em processos automáticos, como por exemplo, em arquivos de dados, programas de computador, macros, scripts, ferramentas, teclas de função ou outros, exceto se autorizado pela área de Segurança da Informação e desde que, comprovadamente, não haja comprometimento à segurança da informação.
XX .armazenar informações corporativas do Estado em diretórios (pastas) públicos (as).

Art 47 É vedada a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio como *Access Points*, modem ou qualquer outra solução que estabeleça conexão simultânea com a rede local e outras redes.
Parágrafo Único. Em casos justificados de uso destes equipamentos, o órgão ou entidade deverá prover segmento de rede independente, através de VLAN, para este fim, de forma a permitir o compartilhamento de sua infra-estrutura de TI sem o comprometimento do desempenho e da segurança da rede local.

CAPÍTULO XII – DAS RESPONSABILIDADES

Art 48 Compete ao usuário:
I .obedecer e cumprir a Política de Segurança da Informação do Governo do Estado;
II .notificar à área responsável pela Segurança da Informação casos de suspeita ou violação das regras ou de falhas de segurança da informação;
III .sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;
IV .utilizar e manter o crachá em local visível durante sua permanência nas instalações do órgão ou entidade;
V .avisar à chefia imediata ou ao superior a perda, furto ou o desaparecimento de crachás.
VI .informar à chefia imediata ou ao superior a presença de pessoas sem identificação nas instalações da órgão ou entidade.
VII .devolver o crachá ao término do contrato de trabalho nos casos de exoneração de cargo efetivo, aposentadoria ou desligamento do órgão ou entidade.
VIII .responder pelo uso de seu login de acesso aos sistemas e serviços do órgão ou entidade;
IX .zelar pelas informações, sistemas, serviços e recursos de tecnologia da informação sob sua responsabilidade;
X .não realizar alterações na configuração da estação de trabalho;
XI .utilizar adequadamente os recursos computacionais;
XII .conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade e privacidade;
XIII .alterar a senha no momento em que receber as informações da criação de sua conta;
XIV .manter sigilo de seu *login* e de sua senha de acesso aos sistemas e serviços do órgão ou entidade;
XV. trocar a senha sempre que houver indícios de comprometimento do sistema ou da própria senha;
XVI .guardar as mídias removíveis, contendo dados, em armários com chaves;
XVII .guardar os documentos em papel que contenham informações sigilosas de forma segura e em local fechado;
XVIII .não reproduzir documento sem a autorização do responsável pela informação;
XIX .imprimir documentos, caso sejam sigilosos, utilizando impressoras com proteção por meio de senhas ou permanecer próximo à impressora, no momento de sua emissão;
XX .não reutilizar documentos em papel que possuam conteúdos sigilosos, devendo estes serem descartados por meio de fragmentação;
XXI .eliminar os arquivos desnecessários armazenados nos servidores da rede do órgão ou entidade;
XXII .responder pelo uso de dispositivos particulares no ambiente do órgão ou entidade;
XXIII .solicitar à chefia imediata a utilização e a conexão do dispositivo móvel na rede corporativa justificando a sua necessidade;
XXIV .evitar armazenar informações confidenciais em dispositivos móveis usados fora do órgão ou entidade. Havendo necessidade, tais informações deverão ser transferidas para um local de armazenamento seguro logo que possível;
XXV .ser responsável pelos dispositivos móveis, e pelos dados armazenados nos mesmos, disponibilizados para uso dentro e fora das instalações do órgão ou entidade;
XXVI .não deixar os dispositivos móveis desprotegidos em locais de alto risco, tais como locais públicos, eventos, hotéis, veículos, dentre outros;
XXVII .apresentar em caso de furto, roubo ou extravio do dispositivo móvel a Ocorrência Policial, no prazo máximo de 48 horas do fato ocorrido, à área responsável pelo patrimônio do órgão ou entidade;
XXVIII .apresentar o dispositivo móvel para a área responsável pelo atendimento ao usuário, quando requisitado, ou ao cessar as atividades que motivaram sua solicitação;
XXIX .zelar pela guarda do dispositivo de armazenamento do certificado e pela senha de acesso ao dispositivo.
XXX .requisitar a revogação do certificado digital caso ele seja perdido, roubado ou extraviado, informando imediatamente o fato à área responsável.

Art 49 Compete à área de TIC:
I .cumprir e fazer cumprir a Política de Segurança da Informação;
II .manter os sistemas computacionais e de comunicação em conformidade com a Política de Segurança da Informação;
III .disponibilizar os recursos necessários à implantação da Política de Segurança da Informação;
IV .manter os dados cadastrais dos usuários da rede corporativa, bem como do correio eletrônico, atualizados;
V .reportar incidentes de segurança da informação à área responsável pela Segurança da Informação;
VI .monitorar os logs dos sistemas;
VII .acompanhar a realização de manutenção, corretiva ou preventiva, dos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade quando a manutenção for realizada por terceiros no ambiente do órgão ou entidade;
VIII .prestar suporte ao usuário quando solicitado;
IX .solicitar apoio e consultoria de segurança à área responsável pela Segurança da Informação quando se fizer necessário;
X .solicitar a assinatura do Termo de Responsabilidade do usuário pela estação de trabalho;
XI .instalar e configurar as estações de trabalho;
XII .manter um inventário atualizado das estações de trabalho e dos softwares;
XIII .desenvolver e manter um padrão de instalação e configuração de estações de trabalho aderente aos critérios estabelecidos nesta resolução;
XIV .configurar os programas de computador e equipamentos para garantir a utilização dos critérios relativos às senhas de acesso definidos pela área de Segurança da Informação;
XV .manter o antivírus, anti-spam e as correções de segurança dos servidores e estações de trabalho atualizados;
XVI .lacrar os microcomputadores;
XVII .documentar toda a infraestrutura de TIC do órgão ou entidade, tais como tipo de equipamento, patrimônio, localização física, data da aquisição, prazo de garantia, etc;
XVIII .controlar e descartar os Hard Disks (HDs) e mídias removíveis, quando necessário;
XIX .disponibilizar e administrar a infraestrutura necessária para armazenamento de dados;
XX .disponibilizar e administrar os recursos de acesso à Internet;
XXI .monitorar o uso da Internet;
XXII .registrar os acessos indevidos à Internet;
XXIII .orientar os usuários em relação à proteção adequada dos dispositivos móveis;
XXIV .configurar os dispositivos móveis disponibilizados para os usuários do órgão ou entidade;
XXV .instalar, homologar, manter, atualizar e configurar todos os servidores, subsistemas de armazenamento e programas de computador que componham as soluções de backup e restore utilizadas no órgão ou entidade;
XXVI .manter a documentação dos servidores, subsistemas de armazenamento, e programas de computador diretamente vinculados às soluções de backup e restore;
XXVII .realizar o backup e a remoção das informações armazenadas nos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade, no caso de manutenção externa ao órgão ou entidade;
XXVIII .definir os recursos e ferramentas que serão utilizados em cada procedimento de backup e restore;
XXIX .documentar os procedimentos de backup e restore;
XXX .eliminar e substituir as mídias de backup e restore próximas de perderem sua funcionalidade segundo a vida útil informada pelo fornecedor;
XXXI .eliminar o conteúdo das mídias que serão descartadas;
XXXII .executar os procedimentos de backup e restore;
XXXIII .gerenciar e controlar os recursos computacionais e as mídias utilizadas pelos sistemas de backup e restore do órgão ou entidade;
XXXIV .manter mapa atualizado das mídias e seus conteúdos para todos os procedimentos de backup e restore do órgão ou entidade;
XXXV .planejar junto às áreas solicitantes os procedimentos de backup e restore;
XXXVI .realizar testes de validação e desempenho das cópias de segurança realizadas;
XXXVII .disponibilizar os recursos necessários para a execução das funções de auditoria;
XXXVIII .garantir a proteção adequada das trilhas de auditoria;
XXXIX .aprovar e registrar a utilização das ferramentas de monitoramento e acesso às estações de trabalho;
XL .analisar e despachar os expedientes relativos a solicitações de usuários encaminhadas pelos respectivos responsáveis por suas unidades;
XLI .administrar o acesso remoto à rede do órgão ou entidade;
XLII .definir os softwares autorizados que deverão ser instalados nas estações de trabalho;
XLIII .administrar as redes corporativas do órgão ou entidade;
XLIV .manter a documentação da topologia da rede atualizada e controlar o acesso ao seu conteúdo;
XLV .prover o ambiente físico necessário para instalação dos roteadores e switches;

XLVI .homologar e administrar os roteadores e switches do órgão ou entidade;
XLVII .manter a documentação (topologia, configurações, etc) dos roteadores e switches atualizada;
XLVIII .administrar as regras dos firewalls;
XLIX .instalar, configurar e manter os ambientes operacionais dos firewalls - sistema operacional nos servidores, bem como os produtos e as correções e atualizações de versão;
L .aplicar, anualmente, os controles disponibilizados pela ferramenta de gestão de riscos nos ativos em que estejam instalados os firewalls;
LI .manter atualizadas as documentações (configurações) relativas aos firewalls;
LII .disponibilizar a infraestrutura necessária para o funcionamento da solução de network IDS/IPS;
LIII .instalar e administrar o network IDS/IPS;
LIV .analisar periodicamente as logs dos Networks IDS em busca de incidentes de Segurança da Informação;
LV .avaliar, no mínimo trimestralmente, o desempenho do network IDS/IPS em relação à quantidade de ataques detectados, falsos positivos (alarme falso), carga da rede, entre outros;
LVI .manter a documentação do network IDS/IPS atualizada;
LVII .instalar, homologar, manter e configurar todos os equipamentos de conectividade que componham as soluções de backup e restore utilizadas no órgão ou entidade;
LVIII .definir e implementar rotina automatizada para a cópia das configurações e dados dos equipamentos de conectividade para um servidor de arquivos contemplado por uma das rotinas de backup/restore;
LIX .analisar e emitir parecer sobre as solicitações da área de segurança da informação;
LX .atualizar os controles da ferramenta de análise de risco de Segurança da Informação;
LXI .avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação;
LXII .elaborar e manter atualizado um procedimento de instalação e configuração da rede;
LXIII .administrar a cessão, a alteração, o bloqueio e o cancelamento de acessos à rede corporativa;
LXIV .revisar, pelo menos 1 (uma) vez por ano, os direitos de acesso dos usuários da rede corporativa e realizar as alterações necessárias;
LXV .revisar, pelo menos a cada 6 (seis) meses, os direitos de acesso com privilégios de administrador e realizar as alterações necessárias;
LXVI .definir, homologar, implementar e disponibilizar a infra-estrutura e os mecanismos de segurança para utilização da rede wireless;
LXVII .realizar semestralmente análise de risco na rede wireless;
LXVIII .disponibilizar relatório as conexões remotas realizadas.
LXIX .solicitar a autorização para movimentação patrimonial de ativos (hardware e software) à área de TIC;

Art 50 Compete ao setor de auditoria:
I .realizar a auditoria nos sistemas do órgão ou entidade;
II .verificar a conformidade com o estabelecido nesta norma e recomendar as ações necessárias;
III .definir parâmetros de geração e retenção das trilhas de auditoria, juntamente com a área responsável pela Segurança da Informação, para fins de controle interno;
IV .gerar e manter atualizada a documentação das ferramentas e auditorias realizadas;
V .manter a área responsável pela Segurança da Informação informada sobre as ferramentas utilizadas;
VI .monitorar a utilização das userid de auditoria.

Art 51 Compete à área de recursos humanos informar, mensalmente, à equipe de Segurança da Informação, a movimentação de pessoal no órgão ou entidade.

Art 52 Compete à direção das unidades administrativas:
I .orientar os usuários sob sua coordenação sobre o cumprimento desta resolução e zelar pelo acesso aos sistemas e serviços do órgão ou entidade;
II .cumprir e fazer cumprir a Política de Segurança da Informação em relação aos seus subordinados;
III .monitorar as atividades de parceiros e contratados sob sua responsabilidade;
IV .colaborar com a área responsável pela Segurança da Informação na elaboração da Política de Segurança da Informação;
V .propor mudanças na Política de Segurança da Informação de acordo com as necessidades iminentes detectadas na sua área de atuação;
VI .reportar, de imediato, à área responsável pela Segurança da Informação, qualquer incidente de segurança detectado ou, até mesmo, qualquer suspeita ou ameaça de incidentes;
VII .avaliar a necessidade de utilização de dispositivo móvel particular e da conexão à rede corporativa do órgão ou entidade;
VIII .solicitar à área de TIC qualquer alteração nas condições autorizadas para a utilização de dispositivo móvel;
IX .solicitar as permissões de acesso para usuários sob sua subordinação à área executora que detenha o controle de acesso ao respectivo recurso computacional;
X .solicitar, com a devida justificativa, para área de TIC a instalação de softwares.

Art 53 Compete à área responsável pela Segurança da Informação:
I .elaborar a Política de Segurança da Informação;
II .verificar o cumprimento desta Resolução e recomendar as ações preventivas e ou corretivas necessárias;
III .administrar, controlar e dar tratamento aos incidentes de segurança da informação;
IV .analisar e autorizar solicitação para conexão na rede corporativa de mídias ou dispositivo móvel particular nas dependências do órgão ou entidade;
V .autorizar, quando necessário, a criação de regras no firewall, considerando a análise de risco realizada;
VI .analisar e emitir parecer sobre as informações de incidentes de segurança ou inconformidades;
VII .aprovar controle de segurança;
VIII .avaliar e apresentar pareceres a respeito das exceções requeridas pelos responsáveis de unidades administrativas do órgão ou entidade;
IX .avaliar, periodicamente, a Segurança da Informação, por meio de análise de indicadores e recomendar ações corretivas e preventivas;
X .definir e padronizar os critérios das senhas de acesso à rede;
XI .elaborar campanhas e programas de treinamento e de conscientização em Segurança da Informação;
XII .elaborar relatórios gerenciais sobre o acesso à Internet;
XIII .elaborar, propor e coordenar projetos, ações e soluções de segurança da informação;
XIV .emitir relatório de alerta e incidente de segurança quando detectado acesso indevido à Internet;
XV .especificar padrão de configuração de segurança destinada a acesso remoto à rede corporativa;
XVI .garantir a implementação dos projetos e soluções de segurança da informação aprovados, atuando permanentemente em busca de parcerias com os diversos responsáveis pelos processos, visando à redução do índice de riscos do órgão ou entidade;
XVII .homologar junto à área de TIC os procedimentos de backup e restore;
XVIII .homologar padrões definidos pela área de redes;
XIX .homologar parâmetros de configuração dos IDS/IPS;
XX .homologar, autorizar e validar o uso de equipamentos e programas de computador nas estações de trabalho quando não existir licença de uso ou o software solicitado for desconhecido ou passível de risco de segurança;
XXI .priorizar as ações de segurança;
XXII .prover apoio técnico consultivo para as unidades administrativas do órgão ou entidade nas questões relativas à segurança da informação;
XXIII .recomendar a adoção de soluções emergenciais sobre segurança da informação;
XXIV .recomendar soluções, ferramentas ou recursos que viabilizem o monitoramento e o registro dos acessos à internet;
XXV .realizar análise de riscos em equipamentos, infraestrutura e pessoas;
XXVI .avaliar o nível de segurança alcançado, emitindo relatórios periódicos de Análise de Riscos à Diretoria e ao Comitê Gestor;
XXVII .definir e acompanhar a execução do Plano Estratégico para implantação da Política de Segurança da Informação;
XXVIII .definir e aprovar junto à alta gestão, os procedimentos e penalidades para se fazer cumprir a Política de Segurança;
XXIX .definir e solicitar os recursos necessários para implantação da Política de Segurança;
XXX .efetuar mudanças na Política de Segurança da Informação sempre que houver alteração no ambiente computacional ou atualizações tecnológicas, visando à manutenção e melhora do nível de segurança;
XXXI .realizar análise de risco para criação de regras no firewall e gerar laudo técnico;
XXXII .dar tratamento aos casos de exceção e aqueles não previstos nas normas relativas à segurança da informação.
XXXIII .aprovar, quando devido, as solicitações de acessos à rede corporativa com privilégios de administrador;
XXXIV .analisar os incidentes de segurança da informação e recomendar ações corretivas e preventivas;
XXXV .realizar, no mínimo anualmente, uma análise crítica dos direitos de acesso dos usuários sob sua coordenação e solicitar as alterações necessárias;
XXXVI .monitorar a utilização de mídias particulares para armazenamento de informações do órgão ou entidade;
XXXVII .tomar as providências cabíveis em caso de descumprimento da Política de Segurança da Informação por seus subordinados;
XXXVIII .analisar permanentemente os acessos remotos realizados por seus subordinados, através de relatório disponibilizado pela área de TIC;

XXXIX .receber, analisar e encaminhar a solicitação de permissão e revogação de acesso para o empregado ou prestador de serviço sob sua subordinação à área de TIC;
XL .informar, em caso de solicitações temporárias, o período em que a utilização da conexão permanecerá liberada, para visitantes e demais usuários;
XLI .avaliar as solicitações para o uso de dispositivo móvel de propriedade ou alugado pelo órgão ou entidade e requerer à área de TIC;
XLII .autorizar, quando necessário, a liberação de portas de diagnóstico remotas;
XLIII .autorizar acessos à rede;
XLIV .informar à Companhia de Tecnologia da Informação do Estado de Minas Gerais – Prodemge, pelo menos 2 gestores de segurança, que terão a função de tratar qualquer assunto relacionado a segurança da informação.
XLV .manter e publicar anualmente um programa de conscientização sobre a segurança da informação;
XLVI .informar anualmente à Superintendência Central de Governança Eletrônica - SCGE da Secretaria de Estado de Planejamento e Gestão - SEPLAG quais as ferramentas de segurança possuem, descrevendo pelo menos, a função, o fabricante, a versão utilizada e a indicação da existência de contrato de manutenção.

CAPÍTULO XIII – PENALIDADES

Art 54 O usuário que não cumprir as normas estabelecidas nessa Resolução estará sujeito às penalidades previstas em Lei.

CAPÍTULO XIV – DISPOSIÇÕES FINAIS

Art 55 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 56 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 57 Caberá à Secretaria de Estado de Planejamento e Gestão, por meio da Subsecretaria de Gestão, esclarecer os casos omissos a esta Resolução.

Art 58 Este Decreto entra em vigor na data de sua publicação, revogada a Resolução SEPLAG nº 73 de 21 de setembro de 2009.

Belo Horizonte, aos 26 de dezembro de 2018.

HELVÉCIO MIRANDA MAGALHÃES JUNIOR
Secretário de Estado de Planejamento e Gestão

Documento assinado eletronicamente por **Helvécio Miranda Magalhães Júnior**, **Secretário(a) de Estado**, em 26/12/2018, às 15:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2755233** e o código CRC **C13692F9**.
