DEFENSORIA PÚBLICA DO ESTADO DE RORAIMA
"Amazônia: Patrimônio dos brasileiros"

RESOLUÇÃO CSDPE Nº 97, DE 19 DE JUNHO DE 2023.

"Dispõe sobre a Política para Utilização de Ativos de Informática e Acesso à Rede da Defensoria Pública do Estado de Roraima."

O DEFENSOR PÚBLICO-GERAL do Estado de Roraima, conforme estabelecido no art. 18, XXI, da Lei Complementar nº 164/2010, e no uso de suas atribuições legais e regulamentares,

CONSIDERANDO, a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias ao funcionamento desta Defensoria Pública com integridade, confidencialidade, disponibilidade e confiabilidade;

CONSIDERANDO, que este documento foi elaborado pelo Departamento de Tecnologia da Informação e Comunicação (DTIC) e contém as normas para utilização da rede de comunicação, ativos de informática e acesso à Internet da Defensoria Pública do Estado de Roraima (DPE/RR);

CONSIDERANDO a necessidade de implementação de boas práticas quanto ao uso de ativos de informática de uso institucional e particular no âmbito da DPE;

RESOLVE:

Art. 1º Instituir a Política para utilização de ativos de informática e acesso à rede da defensoria pública do estado de roraima, obedecendo as regras e procedimentos estabelecidos nesta Resolução, tendo como objetivos principais: I - Apresentar normas para utilização dos recursos acima referidos, de forma a preservar o patrimônio e a informação, no que se refere aos setores computacionais de comunicação e a reputação da Defensoria Pública do Estado de Roraima; II - Garantir a correta e adequada utilização da Internet, Intranet, Extranet, Ativos de Informática e Recursos de Computação e Comunicação. Pode vir a ser substituída ou conviver com as demais políticas futuramente elaboradas e visa, de forma geral, a proteção do ambiente tecnológico da DPE/RR.

CAPÍTULO I

DA POLÍTICA PARA UTILIZAÇÃO DE ATIVOS DE INFORMÁTICA

Art. 2º A presente política destina-se aos membros e servidores, prestadores de serviços e demais colaboradores, doravante denominados apenas colaboradores e visa, em seus diversos aspectos, preservar o patrimônio e a informação. **Art. 3º** São princípios desta Política: I - confidencialidade; II - integridade; III - disponibilidade; IV - autenticidade; e, V - irretratabilidade ou não repúdio.

Art. 4º A DPE/RR se exime das responsabilidades decorrentes da violação de qualquer um dos itens deste documento. Fica o colaborador responsável pelos atos ilícitos ou danosos, praticados utilizando os recursos computacionais da Instituição, que venham a causar prejuízos ou ônus às informações, sistemas, imagem, equipamentos da Instituição ou terceiros. Os colaboradores devem estar cientes de que as informações geradas e manuseadas a partir dos sistemas da DPE/RR são de propriedade da instituição.

Art. 5º Ressalta-se que, primordialmente, todos os colaboradores que necessitem ter acesso aos recursos de rede, comunicação e informação a partir de ativos de TI pessoais deverão, como requisito básico, assinar o "Termo de Responsabilidade de uso de ativos de TI". Neste, o colaborador se compromete à estrita observância e obediência às condições e requisitos básicos para o acesso aos recursos computacionais da DPE/RR.

Art. 6º O descumprimento incorrerá nas penalidades cabíveis, de acordo com a infração cometida e com a legislação vigente. O referido "Termo de Responsabilidade" estará disponível em bloco de assinatura do SEI - Sistema Eletrônico de Informação.

CAPÍTULO II

DAS DIRETRIZES DA POLÍTICA

Art. 7º As normas para utilização dos ativos de informática constantes neste documento estão descritas no Capítulo IV e encontram-se divididas nas seguintes categorias:

I - Utilização dos Ativos de Informática;

II - Utilização da Rede;

III - Utilização da Internet, Intranet e Extranet;

IV - Utilização do e-mail Institucional;

V - Utilização de equipamentos particulares;

VI - Adição de Recursos;

VII - Utilização de Senhas;

VIII - Para empresas ou equipamentos terceirizados.

CAPÍTULO III

DEFINIÇÕES

Art. 8º Para os efeitos desta Resolução, entende-se por:

I - Ativos de informática são principalmente hardwares, softwares e insumos. Switches, roteadores e computadores são exemplos de hardware, sistemas e aplicativos são softwares, ao passo que insumos são os custos com energia elétrica, refrigeração, espaço físico, entre outros;

II - GLPI: é uma ferramenta livre de licença para gerenciamento de atendimentos, inventário de serviços entre outros na área de Tecnologia da Informação que contribui para um melhor gerenciamento dos ativos da empresa e atendimento ao cliente. Sua sigla (Gestionnaire Libre de Parc Informatique) é a uma sigla em Francês, que significa Gerenciamento Livre de Parque de Informática;

III - Wireless: espécie de conexão sem cabo que tem por finalidade troca de informações;

IV - Download: transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local. É um procedimento muito comum e necessário quando o objetivo é obter dados disponibilizados na internet. Os arquivos para download podem ser textos, imagens, vídeos, programas, entre outros;

V - Upload: se refere ao ato de "subir" arquivos presentes no seu computador ou celular para um servidor online, ao contrário do download, que é o ato de baixar algo para o seu dispositivo;

VI - Proxy: é uma ponte entre você e o resto da internet. Normalmente, ao usar o navegador na internet, você será conectado diretamente ao site acessado;

VII - BIOS: vem do acrônimo Basic Input/Output System ("Sistema básico de entrada e saída", em tradução livre);

VIII - Backup: Cópias de segurança de arquivos ou pastas;

IX - SSM: Seção de Suporte e Manutenção;

X - DTIC: Departamento de Tecnologia da Informação e Comunicação;

XI - SASR: Seção de Administração e Segurança de Rede;

XII - DHCP: Do inglês Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de Endereços de Rede), é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente;

XIII - IP: Endereço IP significa "endereço do Protocolo de Internet". O Protocolo de Internet é um conjunto de regras para comunicação pela internet para envio de e-mail, streaming de vídeo ou conexão a um site. Um endereço IP identifica uma rede ou dispositivo na internet;

XIV - NAT: Network Address Translation (Traduções de endereços de rede) é a capacidade de um roteador para traduzir para um endereço IP público para um endereço IP privado e vice-versa. Ele adiciona segurança à rede mantendo os endereços IP privados ocultos do mundo externo;

XV - Internet: conjunto de redes de computadores que, espalhados por todas as regiões do planeta, conseguem trocar dados e mensagens utilizando um protocolo comum;

XVI - Intranet: rede de computadores, mas diferentemente da internet – uma rede global, a intranet é restrita ao contexto de uma corporação e/ou instituição;

XVII - Extranet: extensão da intranet, ou seja, é a mesma rede usada na empresa que pode ser acessada pelas pessoas autorizadas de forma remota, a partir de outros locais;

XVIII - P2P: Peer-to-peer, na tradução para o português, significa ponto a ponto. Na informática, o termo se refere a um tipo de arquitetura de rede de computadores em que cada participante (ponto) é também um servidor, e ajuda a manter o sistema funcionando;

XIX - Streaming: são aqueles serviços que possibilitam a transmissão de conteúdos pela internet, sem a necessidade do usuário fazer download para ter acesso ao filme, música ou livro;

XX - Keyloggers: em inglês significa "registrador do teclado" e, como o próprio nome explica, captura todas as teclas digitadas pelos usuários;

XXI - Back Orifice: Orifício Traseiro, em inglês, é um programa de computador, mais especificamente uma ferramenta de administração remota, que permite a uma pessoa operar remotamente outro computador que esteja executando o sistema operacional Windows e que esteja conectado a uma rede de computadores;

XXII - Netbus: Ferramenta de administração remota com uma interface muito simples e muito fácil de utilizar que utiliza a porta 12345. Tem funções como abrir e fechar drive de cd, iniciar algum programa, controlar mouse entre outras. O indivíduo que controla a máquina infectada remotamente, pode fazer download, abrir programas, deletar arquivos e formatar partições. Um perigo se cair em mãos mal-intencionadas;

XXIII - Mail Bombing: bomba de email é uma forma de abuso da Internet que é perpetrada pelo envio de grandes volumes de email para um endereço de email específico com o objetivo de sobrecarregar a caixa de correio e sobrecarregar o servidor de email que hospeda o endereço, transformando-o em alguma forma de negação de serviço ataque;

XXIV - SPAM: é a prática que consiste em utilizar meios eletrônicos para enviar mensagens que não foram solicitadas. Em geral, o objetivo do SPAM é fazer propaganda de produtos e serviços, mas também aplicar golpes, disseminar boatos e espalhar softwares maliciosos;

XXV - Firewall: dispositivo de uma rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP. XXVI - Cracks: pequenos softwares usados para quebrar um sistema de segurança qualquer. Geralmente utilizados para instalação de softwares que precisam de licença.

CAPÍTULO IV

NORMAS DE UTILIZAÇÃO DOS ATIVOS DE INFORMÁTICA

Seção I

Utilização dos Ativos de Informática

Art. 9º Os colaboradores poderão acessar as redes lógica e sem fio (wi-fi), os Ativos de Informática (Computadores, Notebooks, Tablets, Celular e demais equipamentos Informática) desde que obedecendo todas as normas existentes neste documento, e após cadastro de acesso individual e intransferível.

Art. 10º A manutenção e backup diários/regulares de arquivos pessoais, como cursos em vídeo ou arquivos de texto, imagens fotográficas, dentre outros de natureza pessoal, é de responsabilidade exclusiva de cada colaborador, devendo a DTIC orientar/auxiliar como proceder a realização de backup, quando solicitado via GLPI.

Art. 11º É vedado ao colaborador:

I - Instalar ou remover softwares nos computadores da DPE/RR sem o prévio conhecimento e autorização do Departamento de Tecnologia da Informação e Comunicação - DTIC;

II - Abrir computadores ou outros ativos de informática para qualquer tipo de reparo. Cabe ao colaborador sob os quais os ativos encontram-se em posse abrir chamado via GLPI (http://glpi.rr.def.br/) quando qualquer problema for identificado;

III - Alterar as configurações de rede ou da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

IV - Retirar ou transportar qualquer equipamento da DPE/RR sem autorização prévia do DTIC e Divisão de Material e Patrimônio (DMP);

V - Instalar, desinstalar, desabilitar ou alterar qualquer software ou hardware a fim de tornar o mesmo total ou parcialmente inoperante;

VI - Retirar ou desconectar qualquer equipamento da rede sem um motivo aceitável;

VII - Comprometer, por mau uso ou de forma intencional, equipamento pertencente a DPE/RR;

VIII - Autorizar, sem devido conhecimento e liberação do DTIC, a utilização de equipamentos de informática por pessoas sem vínculo com a Instituição;

IX - Utilizar equipamentos e informações para outros fins, que não sejam atividades ligadas à Instituição;

X - Retirar/danificar licenças/placas identificadoras de patrimônio afixadas nos equipamentos de informática ou travas/lacres de segurança existentes;

XI - Conectar e/ou configurar equipamento à rede de dados cabeada ou wireless da DPE/RR, sem a prévia liberação da Seção de Administração e Segurança de Redes - SASR/DTIC e/ou Seção de Suporte e Manutenção - SSM;

XII - Alterar, excluir ou inutilizar informações ou meios de acesso a aplicativos/equipamentos de forma indevida ou sem prévia autorização;

XIII - Apropriar-se de segredos de pesquisa, indústria, comércio, informações de outros colaboradores ou pertencentes à Instituição através de qualquer meio, eletrônico ou não, sem prévia autorização do proprietário de tais informações; XIV - Tornar vulnerável a segurança dos ativos de informática portáteis (notebook, data show, pen drive, etc);

XV - Compartilhar arquivos ou diretórios sem prévia autorização da SASR/DTIC ou SSM/DTIC.

Seção II

Utilização da Rede

Art. 11 Nas redes cabeadas, o servidor poderá acessar pastas e movimentar arquivos dentro das suas atribuições que lhe são conferidas pela sua função.

Art. 12 É vedado ao colaborador:

I - Tentar ou obter acesso não autorizado a qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conexão a servidor ou conta, cujo acesso não seja expressamente autorizado ao usuário pelo DTIC;

II - Tentar colocar à prova a segurança da rede ou de equipamentos de informática, tanto da Instituição quanto de terceiros;

III - Conectar dispositivos não autorizados na rede local, equipamentos de rede sem fio, equipamentos que permitam a ligação da rede da Instituição a outra rede, que interfiram na frequência/trabalho de operação dos equipamentos da Instituição ou que forneçam serviços de rede, como DHCP, NAT ou outros;

IV - Realizar testes de rede ou estabelecer conexões ad hoc em local onde há o alcance da rede da DPE/RR;

V - Tentar interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo negação de serviço (DoS), congestionamento em redes, tentativas de sobrecarregar um servidor ou "quebrar" (invadir) um servidor;

VI - Infringir a privacidade de qualquer usuário;

VII - Monitorar, interceptar, interromper, modificar servidores, computadores, arquivos ou sistemas de computação instalados dentro da Instituição ou efetuar o mascaramento/falsificação/personificação de endereços/contas de login com objetivo de ocultar-se dos sistemas de segurança da Instituição;

VIII - Configurar manualmente o endereço IP de computadores particulares ou pertencentes à Instituição. A distribuição de endereços de rede é feita pelo serviço de DHCP, mantido e disponível na instituição pelo DTIC;

IX - Conectar computador particular na rede da Instituição sem a devida assinatura do “Termo de Responsabilidade” e autorização do DTIC;

X - Criar, obter ou divulgar imagens, vídeos, documentos ou arquivos com conteúdo abusivo, ofensivo, difamatório, discriminatório, pornográfico, obsceno, injurioso, vexatório, enganoso, calunioso, violento, vulgar, de propaganda não solicitada, de assédio, ameaça, de uso de falsa identidade, ou que seja contrário às normas éticas atuais;

XI Utilizar-se de outro sistema de proxy que não seja o determinado e configurado pela SASR e SSM.

Seção III

Utilização da Internet, Intranet e Extranet

Art. 13 Navegar nos sites e aplicativos institucional em todas as redes.

I - Nas redes cabeadas, o servidor poderá acessar, sites para pesquisas, e redes sociais, desde que não comprometa o desempenho de suas atividades junto a este órgão;

II - Nas redes wifi, o mesmo poderá acessar sites institucionais, acessar redes sociais, e sites de pesquisas.

Art. 14 É vedado ao colaborador:

I - Divulgar, acessar, reter ou disseminar material que não esteja de acordo com as normas, atividades ou políticas da Instituição por meio dos recursos computacionais disponibilizados na Instituição;

II - Utilizar recursos disponíveis para: armazenamento, distribuição ou execução de qualquer tipo de arquivo ou software não autorizado pelo DTIC;

III - Utilizar ferramentas de compartilhamento de arquivos tais como: Torrent, Morpheus, Kazaa, e-mule, Ares e similares;

IV - Utilizar a Internet ou Intranet para jogos individuais ou contra oponentes;

V - Utilizar programas P2P, ou qualquer outro similar, para efetuar download/upload;

VI - Acessar serviços de streaming de rádio utilizando os recursos computacionais disponíveis;

VII - Utilizar e/ou divulgar parâmetros/configurações/softwares, impedindo o bom funcionamento dos ativos de informática ou burlar os sistemas de segurança a fim de conseguir acesso ou privilégios indevidos;

VIII - Utilizar ou propagar softwares mal-intencionados, como vírus, vermes (worms), cavalos de tróia, keyloggers, ou programas que controlem outros computadores (Back Oriffice, Netbus ou similares) através dos recursos disponibilizados pela Instituição;

IX - Divulgar informações confidenciais da Instituição através meios eletrônicos ou não;

X - Apropriar-se de ou distribuir, por intermédio de qualquer meio físico ou virtual, softwares licenciados ou licenças de software de propriedade exclusiva da Instituição bem como qualquer informação, sem autorização por escrito;

XI - Utilizar os recursos disponibilizados pela Instituição para distribuir cópia de qualquer material protegido por direitos autorais, propriedades intelectuais, leis, regulamentações similares, patentes ou outras normas/políticas;

XII - Tentar ou obter acesso a recursos computacionais com o nome de usuário de outra pessoa;

XIII - Divulgar, por intermédio dos equipamentos de informática disponibilizados para uso, informações que possam causar alguma forma de dano físico ou moral a terceiros;

XIV - Utilizar procedimentos ou recursos com a finalidade de obter informações que trafegam pela rede da DTIC ou por redes externas;

XV - Causar falhas nos recursos computacionais da Instituição, ou por intermédio destes em outras redes, através da transmissão de arquivos ou outras informações;

XVI - Utilizar a personificação, mascarando endereços de computadores de rede, e-mail ou logins ocultando a própria identidade e/ou responsabilizar terceiros por qualquer tipo de ação;

XVII - Comprometer ou excluir informações ou arquivos, que não sejam de sua propriedade, armazenados nos recursos computacionais da Instituição sem autorização;

XVIII - Utilizar os recursos computacionais disponibilizados para realizar o envio de mensagens idênticas a grande quantidade de destinatários (SPAM) ou enviar grande quantidade de mensagens a um destinatário (Mail Bombing);

XIX - Efetuar o download (baixa) de programas de entretenimento, filmes, jogos ou quaisquer outros que não sejam estritamente para uso laboral na Instituição.

Seção IV

Utilização do e-mail Institucional

Art. 15 O e-mail institucional deve ser de uso restrito e exclusivo para as atividades relacionadas ao desempenho das funções do membro ou servidor.

Art. 16 São de responsabilidade do usuário todas as mensagens transmitidas sob seu nome de usuário.

Art. 17 Para manter o bom funcionamento do sistema de e-mail a Divisão de Modernização e Governança de TI - DMGT/DTIC poderá efetuar bloqueio de e-mails com arquivos de código executável como (.vbs, .hta, .src, .cpl, .reg, .dll, .inf, exe, .com, .bat, .pif, .js) ou outras extensões usualmente utilizadas por vírus, e-mails para domínios ou destinatários que afetem negativamente os ativos de informática ou exponha a Instituição a riscos de segurança.

Art. 18 A conta de e-mail dos ex-colaboradores da DPE/RR será desativada após 30 dias do desligamento da Instituição.

Art. 19 A manutenção e backup das mensagens é de responsabilidade exclusiva de cada colaborador responsável por seu e-mail institucional, podendo a DTIC auxiliar em tais operações, quando solicitado via GLPI.

Art. 20 É vedado ao colaborador:

I - Perturbar colaboradores ou outras pessoas através do envio frequente de mensagens ou envio de mensagens muito grandes;

II - Tentar ou obter acesso a conta de e-mail de outra pessoa;

III - Utilizar o e-mail institucional para enviar mensagens idênticas a grande quantidade de destinatários (SPAM) ou enviar grande quantidade de mensagens a um destinatário (Mail Bombing). Isso inclui, qualquer tipo de mala direta, como anúncios ou publicidades que não condizem com as atividades institucionais. Ressalta-se, neste caso, que fica preservado o direito de envio de e-mail para todos os colaboradores por parte da Instituição, quando se fizer necessário;

IV - Propagar mensagens em cadeia ou “pirâmides”, independentemente da vontade do destinatário de receber tais mensagens;

V - Sobrecarregar um servidor, usuário ou site com o envio de e-mails muito extensos ou compostos por múltiplas partes;

VI - Modificar qualquer informação do cabeçalho do remetente;

VII - Utilizar apelidos, nomes falsos ou ocultar-se a fim de enviar algum e-mail; VIII - Divulgar informações que possam causar danos físicos, materiais ou morais a terceiros.

Seção V

Utilização de equipamentos particulares

Art. 21 As informações, arquivos e softwares contidos no equipamento particular são de responsabilidade de seu portador/proprietário.

Art. 22 Cabe ao portador do equipamento manter um firewall pessoal ativo e um antivírus atualizado e em execução, não sendo possível ao portador responsabilizar a Instituição por qualquer problema causado por invasão ou pragas virtuais.

Art. 23 Ao utilizar a rede de dados e comunicação da Instituição, o portador deve seguir as mesmas regras de utilização da rede, Internet e Intranet.

Art. 24 O colaborador que desejar utilizar qualquer equipamento pessoal (ativo de TI como computador, notebook, tablet, celular, etc) deverá fazer solicitação prévia à DTIC mediante o Sistema GLPI, e deverá submeter o equipamento a inspeção prévia pela DTIC, conforme Seção VI.

§1º O equipamento após inspeção prévia que tiver identificado qualquer tipo de software, aplicativo ou configuração irregular, ausência de anti-vírus ou sistema operacional ilegal ou desatualizado, ou incompatível com os Sistemas em produção pela DPE/RR será impedido de se conectar à rede de dados cabeada ou wireless da DPE/RR desta Instituição.

Art. 25 A DPE/RR não se responsabiliza por extravio ou perda de qualquer arquivo, software, ou informações de equipamentos particulares que estejam em uso por colaboradores.

Art. 26 A manutenção e atualização de sistemas operacionais, softwares e aplicativos de equipamentos particulares restringe-se exclusivamente aos utilizados pelos equipamentos institucionais.

Art. 27 Nenhum técnico da DPE/RR poderá fazer instalações e manutenções em equipamentos particulares que não tenham sido autorizados e vistoriados previamente.

Art. 28 Mesmo após o equipamento particular ter sido fiscalizado e configurado para o acesso a rede da defensoria, não poderão ser instalados aplicativos que por ventura possam causar alguma fragilidade ou que comprometam a segurança da rede.

Art. 29 Os técnicos do Órgão não poderão fazer nenhuma manutenção no Hardware nem nos aplicativos do equipamento particular, exceto os que são de uso institucional. Seção VI Inspeção de ativos de TI pessoais

Art. 30 Todos os dados/informações do equipamento inspecionado, não poderão ser de forma alguma captados, divulgados, ou removidos sem a prévia autorização do proprietário, exceto os vírus e arquivos que por ventura possam causar, fragilidade, bem como corromper, a segurança da rede, desta Defensoria.

Art. 31 A DTIC realizará os seguintes procedimentos:

I - Verificação de todos os softwares instalados no computador ou tablet ou notebook, quanto a configurações legais (uso de licenças) dos softwares e aplicativos proprietários, inclusive Sistemas Operacionais;

II - Verificação quanto à existência de cracks, scripts de instalação ou similares, utilizados para instalações indevidas de softwares proprietários;

III - Verificação de existência de anti-vírus atualizado;

IV - Verificação quanto a atualizações de sistema operacional;

V - Verificação quanto a versão atualizada de sistema operacional.

Seção VII

Adição de Recursos

Art. 32 É vedado aos usuários da rede de dados cabeada ou wireless da DPE/RR a adição de quaisquer recursos, sejam eles microcomputadores, impressoras, ou outros equipamentos.

Art. 33 Toda e qualquer movimentação de ativos de TI só poderá ser feita pela Divisão de Material e Patrimônio ou Seção de Patrimônio.

Art. 34 A adição de novos equipamentos por parte do usuário deve ser solicitada por comunicação interna, preferencialmente GLPI, e deverá ser aprovada pelo DTIC.

Art. 35 Todos os equipamentos ligados à rede de dados cabeada ou wireless da DPE/RR devem obedecer a padrões de instalação, de designação de endereços e domínio, portanto, uma vez aprovada a solicitação, será realizada a adição do equipamento pelo DTIC.

Art. 36 A adição de recursos à revelia da DPE/RR compromete a administração e a segurança da rede, assim como a assistência aos equipamentos/dispositivos.

Art. 37 Quando for identificada qualquer utilização irregular (de ativos) a DTIC procederá com o bloqueio de acesso do equipamento e encaminhará à Administração Superior para providências cabíveis.

Seção IX

Uso de senhas.

Art. 38 É dever do colaborador manter o sigilo das suas senhas de acesso à rede e aos sistemas, bem como, seguir as recomendações de segurança de como se criar uma senha forte.

Art. 39 Toda ação efetuada com a utilização do usuário e senha do colaborador é de estrita responsabilidade do dono da mesma, não podendo este responsabilizar outras pessoas.

§1º A regra para criação de senhas fortes é utilizar no mínimo oito caracteres, onde a mesma deve ser composta por letras (maiúsculas e minúsculas), números e caracteres especiais (*,^,%,$,#, entre outros).

§2º Todos os servidores poderão alterar suas senhas em qualquer momento, caso suspeite de alguma violação de sigilo, mediante abertura de chamado de suporte via GLPI.

Seção X

Para empresas ou equipamentos terceirizados

Art. 40 Qualquer instalação de novo equipamento de informática ou comunicação deve obrigatoriamente ser acompanhada pelo SSM/DTIC.

§1º Se tal equipamento for um computador o mesmo deve ter um software de antivírus instalado, com atualizações automáticas ativadas e com um agendamento periódico para identificação de pragas que possam comprometer documentos ou o bom funcionamento dos ativos de Informática da Instituição, preferencialmente o mesmo que esteja em produção na DPE/RR.

§2º Se tal equipamento for um computador o mesmo deve ter um firewall pessoal ativado.

Art. 41 Todo software instalado em tais equipamentos devem ser softwares livres ou estarem licenciados e devidamente atualizados. Se licenciados, tais comprovações devem ser apresentadas ao DTIC.

Art. 42 Ao utilizar a rede de dados e comunicação da Instituição, a empresa terceirizada deve seguir as mesmas regras de utilização da rede, Internet, Intranet e Extranet inclusive assinando o “Termo de Responsabilidade”.

CAPÍTULO V

DISPOSIÇÕES GERAIS

Art. 43 Ao acessar a Rede de dados cabeada ou wireless da DPE/RR todos os usuários (Membros, servidores, colaboradores e convidados) concordam com a Política de Segurança da Defensoria Pública do Estado de Roraima. Uma vez acessada a rede da DPE/RR todos os atos realizados serão monitorados pelo SASR/DTIC, salvaguardando a privacidade de cada um, de acordo com a legislação vigente de proteção de dados.

Art. 44 Para garantir as regras acima mencionadas, a SASR/DTIC/DPE/RR vem utilizando os seguintes meios:

I - Sistemas que monitoram e geram relatórios do uso de Internet e acessos a serviços/ativos de informática através da rede, estações de trabalho da Instituição ou através de equipamentos particulares;

II - Sistemas de proteção da rede interna incluindo firewall com filtro de aplicações, proxy com filtro de sites/palavras não permitidos, sistema de detecção de intrusos entre outros;

III - Auditorias realizadas pelo SASR/DTIC sem prévio aviso nos sistemas de firewall ou ativos de informática objetivando o cumprimento das normas contidas nesta política.

Art. 45 Em virtude de ser a segurança da informação um processo contínuo, novas normas e possíveis alterações nesta política serão implementadas. Neste último caso, revoga-se automaticamente a política anterior.

Art. 46 Todos os colaboradores, que fazem uso dos recursos computacionais da DPE/RR devem manter-se atualizados e obedientes às normas em vigor. Este documento estará disponível no site da Instituição para consulta.

Documento assinado eletronicamente por **OLENO INÁCIO DE MATOS**, **Presidente do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 27/06/2023, às 11:40, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **FRANCISCO FRANCELINO DE SOUZA**, **Corregedor Geral**, em 27/06/2023, às 11:44, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **ELCIANNE VIANA DE SOUZA**, **Membro do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 27/06/2023, às 11:49, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **NATANAEL DE LIMA FERREIRA**, **Membro do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 27/06/2023, às 11:51, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **CHRISTIANNE GONZALEZ LEITE**, **Membro do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 27/06/2023, às 11:53, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **RONNIE GABRIEL GARCIA**, **Membro do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 28/06/2023, às 11:10, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **INAJA DE QUEIROZ MADURO**, **Membro do Conselho Superior da Defensoria Pública do Estado de Roraima**, em 28/06/2023, às 11:41, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.rr.def.br/autenticidade, informando o código verificador **0475503** e o código CRC **8552EBFE**.