6.2 - RESOLUÇÃO

6.2.1 - Resolução nº 003/2021/GCG-CG

João Pessoa-PB, 27 Abr 2021.

Aprova o REGULAMENTO INTERNO DE SEGURANÇA CIBERNÉTICA e dá outras providências.

O COMANDANTE-GERAL DA POLÍCIA MILITAR, no uso das atribuições que lhe são conferidas pelo inciso XII do Art. 12 da LC nº 87/2008, RESOLVE:

Art. 1º Aprovar o REGULAMENTO INTERNO DE SEGURANÇA CIBERNÉTICA, conforme anexo.

Art. 2º Instituir a Comissão Permanente de Segurança Cibernética (CPCiber), subordinada ao Estado-Maior Estratégico, com a responsabilidade pela gestão do Sistema de Segurança Cibernética (SiSCiber) da Polícia Militar, conforme disposto no regulamento anexo.

Art. 3º Autorizar a Comissão Permanente de Segurança Cibernética à elaboração e publicação de Normas Técnicas de Segurança Cibernética.

Art. 4º Os casos omissos serão apreciados pela Comissão Permanente de Segurança Cibernética, respeitadas as instâncias administrativas subsequentes.

Art. 5º Esta Resolução entra em vigor na data da sua publicação, revogando-se as disposições em contrário.

EULLER DE ASSIS CHAVES - CEL QOC
Comandante-Geral

REGULAMENTO INTERNO DE SEGURANÇA CIBERNÉTICA

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

Finalidade, Aplicabilidade e Interpretação

Art. 1º O presente instrumento tem por finalidade regulamentar o Sistema de Segurança Cibernética da Polícia Militar do Estado da Paraíba (SiSCiber/PMPB), bem como a Política de Segurança Cibernética Institucional.

Art. 2º O presente Regulamento aplicar-se-á a toda Polícia Militar do Estado da Paraíba, incluindo seus colaboradores e usuários externos, ainda que eventuais.

Art. 3º Na interpretação deste Regulamento, aplicar-se-ão os termos previsto no Glossário apenso.

CAPÍTULO II

SISTEMA DE SEGURANÇA CIBERNÉTICA

Seção I

Definição e Princípios

Art. 4º O Sistema de Segurança Cibernética da Polícia Militar do Estado da Paraíba (SiSCiber/PMPB) consiste no conjunto de órgãos, autoridades, sistemas, infraestruturas, processos, pessoas, equipamentos e normas, com a finalidade de planejar, organizar, coordenar e controlar a Política de Segurança Cibernética Institucional; tendo como Órgão Central a Comissão Permanente de Segurança Cibernética (CPCiber).

Art. 5º O SiSCiber/PMPB orientar-se-á pelos seguintes princípios:

- I. Legalidade;
- II. Confidencialidade;
- III. Integridade;
- IV. Disponibilidade.

Seção II

Comissão Permanente Segurança Cibernética (CPCiber).

Art. 6º A Comissão Permanente de Segurança Cibernética (CPCiber), designada pelo Comandante-Geral, é responsável pelo planejamento, coordenação e supervisão da segurança da cibernética institucional, em especial as seguintes atribuições:

- I. assessorar o Comandante-Geral na formulação de políticas e diretrizes;
- II. realizar a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;
- III. acompanhar assuntos pertinentes às infraestruturas críticas, com prioridade aos relacionados à avaliação de riscos e, em especial:
 - a) manter em contínuo aperfeiçoamento a identificação e a classificação das infraestruturas críticas;
 - b) identificar as possíveis ameaças e vulnerabilidades dessas infraestruturas críticas;
 - c) propor medidas de controle para redução dos riscos às infraestruturas críticas correspondentes à área prioritária considerada.
- IV. elaborar a Diretriz-Geral de Segurança Cibernética (DGC) e a Diretriz-Geral de Acesso à Informação (DGAI);
- V. publicar normas técnicas de Segurança Cibernética e procedimentos para contingência e redução de danos, nos casos de incidentes cibernéticos, mediante aprovação da maioria dos seus membros;
- VI. realizar apuração técnica dos incidentes cibernéticos;
- VII. designar agentes de controle para o cumprimento das medidas de segurança cibernética;
- VIII. supervisionar o cumprimento das normas de segurança

cibernética, em particular fiscalizando, por meio dos seus agentes de controle, as conexões à rede interna, o acesso aos sistemas informatizados e o uso dos dispositivos eletrônicos;

IX. regulamentar os padrões de segurança dos dispositivos, das redes e dos sistemas institucionais;

X. realizar análise de riscos cibernéticos bem como estudos, análises e pareceres sobre segurança cibernética;

XI. elaborar e fomentar instruções, treinamentos, seminários e outros eventos educacionais sobre segurança cibernética;

XII. definir os requisitos essenciais para acesso, conexão e uso dos recursos tecnológicos institucionais, por meio de norma técnica;

XIII. emitir parecer sobre os pedidos de acesso à informação e classificar e desclassificar os dados em harmonia com a Política de Acesso à Informação;

XIV. autorizar a realização de testes de segurança cibernética;

XV. estabelecer estratégias para a preservação de longo prazo, o acesso e o uso contínuo dos documentos digitais, com proteção contra deterioração e a implementação de mecanismos para garantir a autenticidade, a integridade e a legibilidade dos documentos digitais.

Parágrafo Único - Caberá ao Presidente da CPCiber o encargo de Data Protection Officer (DPO).

Art. 7º A CPCiber terá a seguinte estrutura:

- I. Presidente;
- II. Secretário;
- III. Membros;
- IV. Auxiliares administrativos;
- V. Agentes de Controle designados.

Parágrafo Único - Na composição dos membros deverá haver, no mínimo, um representante da Coordenadoria de Planejamento Estratégico e Elaboração de Projetos, da Coordenadoria de Tecnologia da Informação e da Coordenadoria de Inteligência.

Seção III

Agentes de Controle

Art. 8º Cada OPM deverá possuir um Agente de Controle designado pela CPCiber, mediante indicação do respectivo Comandante, responsável pelo cumprimento das normas de segurança cibernética vigentes.

Parágrafo Único - Ao Agente de Controle caberá a representação e a execução das atribuições da CPCiber no âmbito de uma ou mais OPM; resguardado o poder de avocação ou revogação pela CPCiber.

Seção IV

Diretriz-Geral e Normas Técnicas

Art. 9º Deverá ser publicada periodicamente, conforme as demandas institucionais, após homologação do Comandante-Geral, a

Diretriz-Geral de Segurança Cibernética (DGC), estabelecendo a(o):

I. normas gerais para segurança cibernética;

II. normas gerais para resposta a incidentes cibernéticos;

III. procedimentos e modelos para elaboração dos planos de segurança cibernética;

IV. segurança de Infraestrutura Crítica;

V. normas para padronização dos termos de uso dos recursos tecnológicos;

VI. Política de Privacidade Institucional;

VII. relação de softwares autorizados;

VIII. outras questões de interesse estratégico para segurança cibernética.

Art. 10 A CPCiber poderá, mediante aprovação da maioria dos seus membros, publicar Normas Técnicas de Segurança Cibernética.

CAPÍTULO III

DADOS E ARQUIVOS DIGITAIS

Seção I

Acesso aos dados institucionais

Art. 11 O acesso aos dados institucionais será realizado exclusivamente por meio dos Sistemas Informatizados definidos pela CPCiber.

Parágrafo Único - Os dados somente poderão ser disponibilizados a usuários devidamente autorizados e identificados, que tenham realizado o aceite dos termos de uso do respectivo sistema.

Seção II

Organização dos Arquivos Digitais

Art. 12 Os arquivos digitais referentes às atividades institucionais deverão ser armazenados e organizados em sistemas homologados pela CPCiber.

Art. 13 É vedado o armazenamento de arquivos digitais privados em Sistemas de Dados Online institucional, bem como o armazenamento de arquivos digitais institucionais em Sistema de Dados Online não homologados pela CPCiber.

Art. 14 A guarda dos dados de valor permanente deverá estar de acordo com as normas previstas pela arquivística pública responsável por sua custódia.

Art. 15 Os órgãos e as autoridades da instituição deverão realizar periodicamente a cópia de segurança (backup) dos seus arquivos digitais, preferencialmente por meio de mecanismos automatizados.

§ 1 Os Backups poderão ser realizados por meio de Sistema de Dados

Online ou Dispositivos de Armazenamento (HD, SSD, pendrive ou similar), devidamente homologados pela CPCiber.

§ 2 A CPCiber, por meio dos seus agentes de controle, deverá periodicamente fiscalizar os sistemas de backup para evitar cópias não autorizadas.

Seção III

Dados Sigilosos

Art. 16 O acesso, a divulgação e o tratamento dos dados classificados como sigilosos (dados sigilosos) ficarão restritos às pessoas devidamente credenciadas, sem prejuízo das atribuições dos agentes públicos autorizados por lei.

§ 1 Os procedimentos de classificação dos dados quanto ao grau de sigilo e de controle do acesso observarão os termos da Lei nº 12.527, de 18 de novembro de 2011, e das demais normas aplicáveis.

§ 2 O acesso aos dados sigilosos constitui para o usuário que teve acesso, a obrigação de resguardar o sigilo dos dados, sob pena de responsabilização nos termos da legislação vigente.

Art. 17 Os Comandantes de OPM deverão adotar as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de dados sigilosos.

Parágrafo único - A pessoa física ou jurídica que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de dados sigilosos adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta norma.

Art. 18 Caberá ao Sistema de Inteligência da Polícia Militar (SIPOM) elaborar as normas para o trâmite e o processamento dos dados de inteligência.

CAPÍTULO IV

RECURSOS TECNOLÓGICOS INSTITUCIONAIS

Seção I

Recursos tecnológicos institucionais

Art. 19 O acesso, a conexão e o uso dos recursos tecnológicos institucionais de hardware (dispositivos eletrônicos), softwares (sistemas informatizados), infraestrutura (rede interna), dentre outros, na modalidade presencial ou remota, somente poderão ser realizados mediante prévia autorização da CPCiber.

§ 1 Caberá ao usuário que pretenda acessar, conectar ou fazer uso de qualquer dos recursos tecnológicos institucionais (dispositivos eletrônicos, sistemas informatizados e infraestrutura de rede), requerer a sua autorização à CPCiber, por meio do seu Agente de Controle.

§ 2 A solicitação deverá ser encaminhada ao Agente de Controle, por meio digital disponibilizado (E-mail, mensageiro eletrônico, etc.), a quem caberá analisar e decidir pelo pedido de autorização; sendo

admitido recurso à CPCiber em caso de indeferimento.

§ 3 Nos casos previstos na DGC, a autorização poderá ser concedida de ofício, por meio da verificação digital do usuário e do aceite eletrônico dos termos de uso e da Política de Privacidade Institucional.

§ 4 Em qualquer hipótese a autorização somente poderá ser concedida com a identificação do usuário e do seu dispositivo, e após o aceite do termo de uso do recurso e da Política de Privacidade Institucional.

Art. 20 O acesso, a conexão e o uso dos recursos tecnológicos institucionais (dispositivos eletrônicos, sistemas informatizados e rede interna) serão monitorados pela CPCiber, por meio dos seus Agentes de Controle, sem prejuízo aos termos da Política de Privacidade Institucional.

§ 1 Os roteadores, switches, pontos de acesso, dentre outros dispositivos utilizados para distribuição e/ou compartilhamento de rede nos órgãos e setores deverão ser periodicamente vistoriados pela CPCiber, por meio dos seus Agentes de Controle.

§ 2 É vedado o uso da infraestrutura de rede institucional para fins pessoais ou em desacordo com o interesse público.

§ 3 A CPCiber poderá vetar o acesso a determinados sítios virtuais através da infraestrutura de rede institucional e ainda a busca por meio de determinadas expressões.

Art. 21 É vedado qualquer espécie de acesso, conexão ou uso dos recursos tecnológicos institucionais (dispositivos eletrônicos, sistemas informatizados e rede interna), por usuários ou dispositivos não autorizados pela CPCiber.

Art. 22 Caberá a CPCiber apurar qualquer espécie de acesso, conexão ou uso de recurso tecnológico institucional por usuário ou dispositivos não autorizados, bem como o descumprimento de qualquer das cláusulas do termo de uso, para fins de responsabilização dos envolvidos.

Seção II

Softwares Autorizados

Art. 23 Os dispositivos eletrônicos institucionais somente poderão conter os softwares autorizados pela CPCiber ou previstos na DGC.

Parágrafo Único - A autorização para instalação de software não autorizado deverá ser solicitada pelo usuário à CPCiber, a quem caberá decidir após análise dos riscos à segurança cibernética.

Art. 24 Quando identificado, o software não autorizado deverá ser imediatamente removido do dispositivo eletrônico institucional, juntamente com todos os dados vinculados.

§ 1 Antes de remover o software, deverá ser realizada uma análise de risco para orientar as intervenções técnicas necessárias e o resguardo dos elementos probatórios para responsabilização dos envolvidos.

§ 2 O usuário responsável pelo dispositivo eletrônico deverá ser

notificado da identificação do software irregular bem como da sua remoção.

Seção III

Comodato de dispositivos eletrônicos

Art. 25 Os dispositivos eletrônicos institucionais poderão ser disponibilizados aos usuários mediante regime de comodato.

§ 1 No regime de comodato o usuário comodatário receberá a posse permanente do equipamento após a assinatura do respectivo termo de responsabilidade no qual assumirá o compromisso de guardar, conservar e manter o equipamento nas mesmas condições recebidas.

§ 2 O usuário comodatário é livre para configurar o dispositivo da forma que melhor se adequar às suas atividades, podendo instalar os softwares que julgar necessários, sendo responsável pelos eventuais riscos e prejuízos à infraestrutura informatizada.

Art. 26 O usuário que descumprir com seus deveres terá o seu comodato revogado imediatamente, sem prejuízo de eventual responsabilização administrativa e/ou judicial.

Seção IV

Manutenção dos dispositivos eletrônicos

Art. 27 A manutenção dos dispositivos eletrônicos institucionais será realizada exclusivamente pelo pessoal técnico previamente autorizado pela CPCiber.

Parágrafo Único - O Agente de Controle deverá encaminhar periodicamente para CPCiber relação contendo o pessoal técnico autorizado a realizar a manutenção dos dispositivos eletrônicos.

Art. 28 É vedada a manutenção dos dispositivos eletrônicos institucionais por pessoal não autorizado, sob pena de responsabilização em decorrência dos eventuais riscos ou prejuízos à infraestrutura tecnológica institucional.

Seção V

Desenvolvimento de softwares

Art. 29 Serão considerados softwares institucionais somente aqueles desenvolvidos ou homologados pela CPCiber.

Parágrafo Única - As OPM com equipes de desenvolvimento próprias deverão informar periodicamente à CPCiber a relação do efetivo empregado nessa atividade.

Art. 30 É vedado o uso de aplicações desenvolvidas por equipes não autorizadas pela CPCiber.

Art. 31 A equipe responsável pelo desenvolvimento ficará encarregada pela segurança dos dados.

Art. 32 Toda solução desenvolvida por equipes independentes deverá ser analisada pela CPCiber.

CAPÍTULO V

INCIDENTES CIBERNÉTICOS

Seção I

Procedimentos em casos de incidentes cibernéticos

Art. 33 Quando for verificado qualquer espécie de incidente cibernético, a CPCiber deverá:

I. adotar imediatamente as medidas de contenção de dano que forem necessárias;

II. providenciar a análise dos eventuais prejuízos à infraestrutura de dados e aos sistemas informáticos;

III. proceder com a apuração das causas e dos responsáveis.

§ 1º O Agente de Controle que tomar ciência de qualquer espécie de incidente cibernético deverá comunicar imediatamente a CPCiber, sem prejuízo da adoção das medidas previstas no caput que se mostrarem inadiáveis.

§ 2º Os procedimentos decorrentes de incidentes cibernéticos deverão ser detalhados na DGC e nos Planos de Segurança Cibernética.

Seção II

Planos de Segurança Cibernética

Art. 34 O Agente de Controle de cada OPM deverá elaborar um plano de segurança cibernética para o órgão a que se vincula, o qual será submetido à CPCiber para aprovação e publicação.

Seção III

Testes de segurança

Art. 35 A CPCiber poderá promover periodicamente testes de segurança cibernética, realizados por agentes públicos, civil ou militar, pessoal conveniado ou ainda equipes externas devidamente autorizadas, em ambientes controlados.

CAPÍTULO VI

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Seção I

Disposições transitórias

Art. 36 Enquanto não for publicada a DGC, fica liminarmente autorizada a instalação dos softwares previsto em relação apensa.

Seção II

Disposições finais

Art. 37 Deverá ser responsabilizado todo agente público ou particular, civil ou militar, que fizer o uso indevido dos dados institucionais ou de informações pessoais de terceiros, nos termos do artigo 42 da Lei nº 13.709/2018.

Art. 38 Os prejuízos decorrentes das eventuais falhas de segurança cibernética serão atribuídos solidariamente às pessoas físicas e jurídicas, controladoras e operadoras dos dados.

Art. 39 Os casos omissos serão apreciados pelo Estado-Maior Estratégico, respeitadas as instâncias administrativas subsequentes.

Art. 40 Este Regulamento entra em vigor na data da sua publicação, revogando as disposições em contrário.

Cel QOC HÉLIO DE ARAÚJO FIRMINO
Presidente da Comissão

TC QOC ARNALDO SOBRINHO MORAIS NETO
Vice-presidente

Cap QOC ALESSANDRO HENRIQUE DE ANDRADE
Membro

Cap QOC HANDERSON G. DE LIMA CAVALCANTI
Relator

1º Ten QOC DIOGENES DA SILVA SOUSA
Membro

Sd PM LEOJOAN MOURA CAVALCANTE JUNIOR
Membro

Sd PM JIMMY FELIPE GOMES DOS SANTOS
Colaborador

JOSENILDO B. DA SILVA
Colaborador

APÊNDICE 1

GLOSSÁRIO

1) comodato: compreende a concessão gratuita de coisa móvel, por um certo período de tempo, com a condição de devolver nas mesmas condições ao fim do prazo

2) dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

3) dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

4) dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

5) banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

6) titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

7) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

8) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

9) encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

10) agentes de tratamento: o controlador e o operador;

11) tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

12) anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

13) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

14) bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

15) eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

16) Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

17) uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

18) relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

19) órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

20) autoridade nacional: órgão da administração pública responsável

por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;

21) dispositivos eletrônicos: os desktops, notebooks, tablets e smartphones, dentre outros, pertencentes a carga da instituição.

22) Política de Proteção de Dados - corresponde a um conjunto de normas para coleta, armazenagem, transmissão e processamento de dados determinados ou determináveis, efetuados por pessoas físicas ou jurídicas.

23) Infraestrutura de Rede Interna/Rede Interna/ Intranet: rede de computadores interna que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local, que só pode ser acessada pelos seus utilizadores ou colaboradores internos. compreende todos os tipos de conexões e tecnologias, seja ela cabeada, sem fio, dentre outras.

24) Infraestrutura Crítica: termo usado para descrever ativos e serviços , públicos ou privados, que são essenciais para o funcionamento da corporação.

25) Sistemas Informatizados Institucionais compreendem a qualquer sistema ou software oficialmente desenvolvido ou disponibilizado pela instituição, através do seu respectivo Setor de Tecnologia da Informação

26) segurança cibernética corresponde a um conjunto de medidas de proteção de sistemas informáticos, incluindo hardware, software, peopleware e dados, contra incidentes cibernéticos.

APÊNDICE 2

RELAÇÃO PRELIMINAR DE SOFTWARES AUTORIZADOS

1) Sistema operacional - MS Windows, Linux, Android, IOs, OS X, conforme hardware ou versão OEM;

2) Pacote Office (editor de texto, apresentador, etc.) - MS Office 365, WP Office, Libre Office, Open Office, Google Docs, OnlyOffice conforme hardware ou versão OEM;

3) Sistema de Dados Online (nuvem) - Google Drive;

4) Leitor de arquivos PDF - Adobe Acrobat versão Free;

5) Gestor de Bibliografia - Mendeley;

6) Gerenciador de Streaming - OBS Studio;

7) Mensageiro eletrônico - Whatsapp, Viber, Telegram, Signal e Rede Sinesp;

8) Vídeo Conferência - Google Meet;

9) Edição de Imagens Vetoriais - InkScape;

10) Edição de Fotos - GIMP;

11) Edição de Áudio- Audacity;

12) Edição de Vídeo - Openshot;

13) Navegador Web - Chrome, Firefox e Microsoft Edge. (Nota nº 0122/2021-ACG, de 28/04/2021).

-

(Nota nº 152299 de 28 Abr 2021 - GAB COMANDANTE GERAL)

6.2.2 - Resolução nº 004/2021/GCG-CG

João Pessoa-PB, 27 Abr 2021.

Aprova o Regulamento Interno de ACESSO À INFORMAÇÃO e dá outras providências.

O COMANDANTE-GERAL DA POLÍCIA MILITAR, no uso das atribuições que lhe são conferidas pelo inciso XII do Art. 12 da LC nº 87/2008, RESOLVE:

Art. 1º Aprovar o REGULAMENTO INTERNO DE ACESSO À INFORMAÇÃO, conforme anexo.

Art. 2º As consultas aos dados da Polícia Militar e de seus integrantes deverão ser realizadas estritamente por meio dos Sistemas Informatizados aprovados pela força.

Art. 3º É vedado o uso dos dados das consultas para fins comerciais, empresariais ou político-partidários.

Art. 4º É dever de todo integrante da Polícia Militar controlar o acesso e a divulgação dos dados produzidos por seus órgãos e setores, assegurando a sua proteção.

Art. 5º Os casos omissos serão apreciados pelo Estado-Maior Estratégico, respeitadas as instâncias administrativas subsequentes.

Art. 6º Fica delegado ao Estado-Maior Estratégico a publicação de Instruções Complementares, mediante homologação do Comandante-Geral.

Art. 7º Esta Resolução entra em vigor na data da sua publicação, revogando-se as disposições em contrário.

EULLER DE ASSIS CHAVES - CEL QOC
Comandante Geral

REGULAMENTO INTERNO DE ACESSO À INFORMAÇÃO

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

Finalidade Aplicabilidade e Conceitos

Art. 1º O presente instrumento tem por finalidade regular a Política de Acesso à Informação, no âmbito da Polícia Militar do Estado da Paraíba.