



POLÍCIA MILITAR DO ESTADO DE SÃO PAULO



INSTRUÇÃO POLICIAL MILITAR

**INSTRUÇÕES PARA UTILIZAÇÃO DA REDE MUNDIAL DE COMPUTADORES
(INTERNET) E REDE INTERNA (INTRANET) PELA PMESP**

I-30-PM

**INSTRUÇÕES PARA UTILIZAÇÃO DA REDE MUNDIAL DE COMPUTADORES
(INTERNET) E REDE INTERNA (INTRANET) PELA PMESP**

4^a edição

Publicada anexo ao Bol G PM Nº 138, de 25JUL14.

(NR dada pelo Bol G PM 114/17)



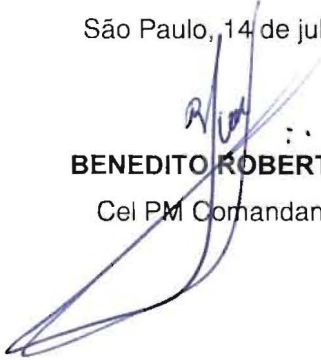
ESTADO DE SÃO PAULO
SECRETARIA DE ESTADO DOS NEGÓCIOS DA SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO ESTADO DE SÃO PAULO
COMANDO GERAL

PORTARIA Nº PM1-002/04/14

1. O Comandante Geral da Polícia Militar do Estado de São Paulo, nos termos do artigo 19, I, do Regulamento Geral da Polícia Militar, aprovado pelo Decreto nº 7.290, de 15 de dezembro de 1975, aprova as I-30-PM - Instruções para Utilização da Rede Mundial de Computadores (Internet) e Rede Interna (Intranet) pela PMESP, 4ª edição, autoriza sua publicação anexo ao Boletim Geral PM e sua divulgação pela intranet da Instituição.

2. Estas Instruções entrarão em vigor na data de sua publicação, revogando-se as disposições em contrário, em especial as I-30-PM - 3ª edição, publicadas em anexo ao Bol G PM 79, de 27 de abril de 2006.

São Paulo, 14 de julho de 2014.


BENEDITO ROBERTO MEIRA

Cel PM Comandante Geral

SUMÁRIO

CAPÍTULO I - DAS FINALIDADES	5
CAPÍTULO II - DOS ACESSOS À REDE INTERNET E INTRANET	5
Seção I - Das permissões de acesso às páginas eletrônicas na internet	5
Seção II - Do acesso à rede interna de computadores da PMESP	5
CAPÍTULO III - DAS NORMAS DE SEGURANÇA	6
CAPÍTULO IV - DA ELABORAÇÃO DE PÁGINAS ELETRÔNICAS	8
Seção I - Das páginas da Intranet	8
Seção II - Das páginas da Internet	8
CAPÍTULO V - DAS REDES SOCIAIS E BLOGS	8
CAPÍTULO VI - DO ACOMPANHAMENTO DO CONTEÚDO DAS PÁGINAS ELETRÔNICAS	9
CAPÍTULO VII - DO GERENCIAMENTO DE SITE NA INTERNET	9
CAPÍTULO VIII - DAS PRESCRIÇÕES DIVERSAS	10
GLOSSÁRIO	11
ANEXO - TERMO DE COMPROMISSO DE ACESSO POR MEIO DA REDE VIRTUAL PRIVADA (VPN) AOS RECURSOS COMPUTACIONAIS DA POLÍCIA MILITAR	13
OPM RESPONSÁVEL	14
ÍNDICE REMISSIVO	15

CAPÍTULO I DAS FINALIDADES

Artigo 1º - Estas Instruções têm por finalidade regular as condições de acesso e utilização dos recursos da Internet e Intranet em proveito da Polícia Militar do Estado de São Paulo (PMESP) no que diz respeito à correção dos procedimentos do Policial Militar, funcionário civil ou terceiros contratados, doravante denominados usuário, no desempenho de suas funções, em particular ao utilizar recursos de Tecnologia da Informação e Comunicação (TIC), de propriedade da PMESP, colocados sob a responsabilidade desses servidores.

Artigo 2º - São objetivos destas Instruções:

- I - estabelecer normas sobre gerenciamento de sites na Internet e Intranet;
- II - estabelecer normas para utilização da Internet e Intranet pelos usuários;
- III - coibir o acesso e/ou a inserção de assunto ou matéria considerada ilícita, contrária à disciplina, à moral e aos bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros, buscando acima de tudo a utilização mais adequada dos dispositivos.

CAPÍTULO II DOS ACESSOS À REDE INTERNET E INTRANET

Seção I

Das permissões de acesso às páginas eletrônicas na internet

Artigo 3º - A liberação de acesso à internet permite que o usuário, por meio de autenticação, navegue fora dos domínios Governamentais, respeitando as políticas de acesso institucionais.

§ 1º - O acesso à Internet aos Policiais Militares, em regra, será mediante “login” e “senha”, ambos fornecidos nos órgãos de ensino da Polícia Militar, quando do ingresso na Instituição.

§ 2º - Os demais usuários deverão solicitar o acesso ao Cmt da OPM a qual estiverem servindo.

Artigo 4º - A política de acesso institucional aos sites será definida pela Diretoria de Telemática (DTel) em norma específica.

Seção II

Do acesso à rede interna de computadores da PMESP

~~Artigo 5º - O acesso à rede interna de computadores da PMESP, denominada Intranet/PM é realizado por meio dos seguintes canais:~~

~~I - Link dedicado (Intragov) - o acesso por meio do link dedicado tem por objeto integrar as redes já instaladas nas Secretarias de Estado e no ambiente de Internet Central do Palácio do Governo, constituindo-se assim uma rede de âmbito estadual, em sistema de roteamento, para obter de imediato os benefícios do compartilhamento dos recursos tecnológicos já disponíveis e possibilitar a imediata implementação do ambiente do Governo do Estado e, em particular, no âmbito da PMESP;~~

Artigo 5º - O acesso à rede interna de computadores da PMESP, denominada Rede Intranet PM, será realizado por meio dos seguintes canais:

I - Link Intragov - é o principal canal de comunicação das OPM e tem por objetivo:

- a) fornecer conectividade aos serviços prestados pela Instituição, hospedados no Datacenter PM;
- b) permitir a interligação com os demais órgãos do Estado de São Paulo e entidades correlatas;
- c) fornecer acesso à Rede Internet. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

II - Rede Privada Virtual (*Virtual Private Network* - VPN) - o acesso por meio da Rede Privada Virtual caracteriza-se pela utilização da infraestrutura de uma rede pública, para acesso ao conteúdo da Intranet/PM, constituindo uma via virtual por onde os dados trafegam de modo seguro, por criptografia, conforme o protocolo utilizado.

~~Artigo 6º - A utilização da VPN está restrita ao uso individual, não compartilhado, para o acesso à Intranet e poderá ser realizada somente quando:~~

- ~~I - ocorrer impedimentos técnicos de instalação de link dedicado na OPM;~~
- ~~II - ocorrer mudança de endereço da OPM, até que o link dedicado seja instalado;~~
- ~~III - for constatada a interrupção da disponibilidade do acesso por link dedicado;~~
- ~~IV - a sua utilização decorrer da necessidade de obter informações disponibilizadas na rede interna, estando o usuário de microcomputador portátil em ambiente estranho à Administração PM;~~
- ~~V - necessidade do serviço policial militar.~~

Artigo 6º - A utilização da Rede VPN destina-se ao acesso excepcional e temporário à Rede Intranet PM, direcionado exclusivamente ao policial militar do serviço ativo, de modo individual e não compartilhado, diante de comprovada necessidade do serviço e quando houver a constatação de:

- I - impedimentos técnicos de instalação do link Intragov na OPM;
- II - mudança de endereço da OPM, até que o link Intragov seja instalado;
- III - interrupção prolongada da disponibilidade do acesso por link Intragov;
- IV - comprovada necessidade de utilização do equipamento em ambiente estranho à Administração policial-militar, mediante prévia autorização.

§ 1º - Os casos omissos e excepcionais que versarem sobre acesso à Rede VPN deverão ser submetidos à aprovação do Subcomandante PM.

§ 2º - A Diretoria de Telemática, por meio do CTel, é o órgão técnico responsável por subsidiar o Subcomandante PM nos assuntos relativos às questões de rede e segurança de dados, além de estabelecer as políticas de acesso e aspectos correlatos. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

~~Artigo 7º - Caberá ao Cmt/Ch/Dir autorizar a solicitação de acesso via VPN a Intranet PM.~~

~~§ 1º - Os Oficiais não necessitam da autorização do Cmt/Ch/Dir para solicitar o acesso via VPN.~~

~~§ 2º - A solicitação dos demais usuários deverá ser feita através da Central de Serviços de TIC, por meio dos canais de acesso disponíveis na página inicial da Intranet.~~

~~§ 3º - O Policial Militar, Praça ou Oficial, para acessar a Intranet via VPN, deverá obrigatoriamente assinar o Termo de Compromisso (Anexo), o qual deverá permanecer arquivado na Agência de Inteligência no Setor de Telemática da OPM.~~

Artigo 7º - A solicitação de acesso à Rede VPN deverá ser feita por meio da Central de Serviços de TIC.

§ 1º - Compete ao Cmt/Ch/Dir da OPM autorizar, mediante decisão fundamentada, o acesso de Praças, funcionários civis e prestadores de serviços à Rede VPN.

§ 2º - O acesso do usuário à Rede VPN será obrigatoriamente precedido da assinatura do Termo de Compromisso de Sigilo e Confidencialidade emitido pelo CTel, o qual deverá permanecer arquivado eletronicamente na Central de Serviços de TIC, no Setor de Telemática e na Agência de Área da respectiva OPM.

§ 3º - O CTel estabelecerá procedimentos técnicos internos para solucionar os casos extraordinários, bem como as rotinas de criação, manutenção, suspensão e cancelamento de usuários e senhas, além das rotinas de controle. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

§ 4º - O CSM/MTel estabelecerá os procedimentos técnicos internos para a criação/manutenção dos usuários e senhas, da instalação e controle da distribuição do aplicativo de acesso, denominado de Cliente VPN, bem como tratar eventuais exceções relacionadas ao acesso.

CAPÍTULO III DAS NORMAS DE SEGURANÇA

Artigo 8º - Quanto às normas de segurança para a utilização da Internet pelas OPM, deverá ser observado:

I - visando conscientizar o público interno quanto ao contido nestas Instruções, devem ser realizadas palestras ou outras atividades afins pelos Oficiais de Telemática, ressaltando-se a necessidade de comprometimento de todos os integrantes da OPM quanto à segurança na utilização da Internet;

II - em havendo suspeição da ocorrência de violação da segurança, por motivos direta ou indiretamente ligados à Internet, os serviços baseados naquela rede devem ser imediatamente suspensos e o fato comunicado ao escalão superior e à DTel para as providências cabíveis;

III - mediante planejamento da DTel, por meio do CPD, devem ocorrer, a atualização de versões e a eventual correção de sistemas operacionais e aplicativos, respeitadas as restrições impostas pela legislação em vigor quanto à necessidade de licenças de uso de programas (softwares);

IV - qualquer obtenção de arquivos da Internet limitar-se-á aos casos de interesse da Instituição;

V - todo usuário é responsável pela segurança da informação que manipular, bem como pelos recursos de informática ou de comunicação que utilizar;

~~VI - é vedado o uso de recursos de criptografia (hardwares e/ou softwares) não homologados pela PMESP, sendo que a regulamentação desses sistemas, assim como a definição dos parâmetros, deve ser de responsabilidade da DTel, cabendo ao CPD e ao CSM/MTel, a aquisição, implantação e treinamento;~~

~~VII - sistemas de proteção e controle de fluxo de dados e detecção de intrusão, denominado firewall, além de outros similares, quando utilizados, devem ser projetados, adquiridos, implementados e~~

VI - é vedado o uso de recursos de criptografia (hardwares e/ou softwares) não homologados pela PMESP, sendo que a regulamentação desses sistemas, assim como a definição dos parâmetros, deve ser de responsabilidade da DTel, cabendo ao CPD e ao CTel, a aquisição, implantação e treinamento;

VII - sistemas de proteção e controle de fluxo de dados e detecção de intrusão, denominado firewall, além de outros similares, quando utilizados, devem ser projetados, adquiridos, implementados e mantidos segundo requisitos mínimos definidos pelo CTel; (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

VIII - as informações eletrônicas disponíveis ao público interno e externo e deles recebidas devem ser submetidas a processos de detecção e remoção de códigos maléficos, tais como vírus de computador, por meio de programas, homologados pelo CPD e constantemente atualizados;

~~IX - o CSM/MTel executará os procedimentos voltados para a interação entre a Intranet corporativa e a Internet, em particular no tocante às estruturas físicas e lógicas utilizadas para interconexão e controle de acesso, de forma a preservar a segurança das informações.~~

IX - o CTel executará os procedimentos voltados para a interação entre a Intranet corporativa e a Internet, em particular no tocante às estruturas físicas e lógicas utilizadas para interconexão e controle de acesso, de forma a preservar a segurança das informações. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

Artigo 9º - Não são permitidas ligações remotas aos equipamentos da rede interna da OPM, oriundas de pontos externos à rede corporativa da PMESP, mesmo que para fins de administração por parte do responsável pela gerência da rede, exceto nos casos de acesso por meio VPN e/ou nos demais casos devidamente autorizados pela D Tel.

Artigo 10 - A fim de controlar a utilização do sistema informatizado da PMESP, todos os usuários devem possuir senha de acesso individual corporativa.

Artigo 11 - Compete ao usuário:

I - observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade da sua senha, a qual é pessoal e intransferível, através da qual pode efetuar operações a ele designadas nos recursos computacionais que acesse;

II - não divulgar a sua senha a outras pessoas, mantendo-a em segurança;

III - de maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outros usuários;

IV - somente utilizar o seu acesso para os fins relacionados com o serviço policial militar e para os quais estiver devidamente autorizado, em razão de suas funções;

V - responder em todas as instâncias, pelas consequências das ações ou omissões de sua parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações que tenha acesso;

VI - utilizar as informações as quais tenha acesso somente em razão do serviço;

VII - reportar imediatamente à sua Chefia ou ao Oficial de Telemática, em caso de violação, acidental ou não, da sua senha, e providenciar a sua substituição;

VIII - solicitar o cancelamento de sua senha quando cessar a necessidade de sua utilização.

CAPÍTULO IV DA ELABORAÇÃO DE PÁGINAS ELETRÔNICAS

Seção I Das páginas da Intranet

Artigo 12 - Cada OPM poderá dispor de apenas 01 (um) endereço eletrônico na Intranet, para divulgar ao público interno, informações e serviços.

Parágrafo único – Se o Cmt da OPM julgar conveniente e oportuna a criação da página na Intranet, deverá respeitar a padronização provida pelo C Com Soc e as demais normas vigentes no âmbito da PMESP.

Artigo 13 - O Cmt da OPM é responsável pela elaboração da página eletrônica solidariamente com o Oficial de Telemática e o Oficial P/5, devendo zelar pela coerência, exatidão e pertinência das informações divulgadas.

§ 1º - Em nenhuma hipótese devem ser disponibilizadas, por meio de páginas eletrônicas na Internet e Intranet, dados ou informações que possam expor e/ou comprometer a segurança da Instituição, bem como informações ou imagens que possam caracterizar promoção pessoal.

§ 2º - Fica proibido incluir, sob qualquer forma de divulgação, assuntos que não sejam de interesse Institucional.

Artigo 14 - Para elaboração das páginas eletrônicas e sua publicação deverão ser utilizados apenas programas aplicativos (*softwares*) adquiridos ou desenvolvidos pela PMESP, licenciados de acordo com a legislação vigente ou de domínio público (*freeware*).

Artigo 15 - Não deverão existir páginas sem conteúdo, com a mensagem "em construção" ou outra análoga, a fim de evitar o tráfego desnecessário de dados, causando frustração por parte do visitante, sendo permitida apenas a indicação de "site em manutenção", quando as páginas eletrônicas estiverem indisponíveis.

Parágrafo único - Caso seja necessário incluir botões, nas páginas que serão desenvolvidas, estes não deverão estar ativos, ou seja, configurados como hiperlinks.

Seção II Das páginas da Internet

Artigo 16 - A página eletrônica da Polícia Militar na Internet é o único canal de comunicação disponível com o público externo, sendo vedada a criação de páginas individuais pelas OPM.

CAPÍTULO V DAS REDES SOCIAIS E BLOGS

Artigo 17 – A criação, padronização e fiscalização de tais ferramentas de comunicação serão normatizadas pelo C Com Soc.

Parágrafo único – Caberá à DTel, por meio dos Centros subordinados, a disponibilização e a manutenção técnica das ferramentas.

CAPÍTULO VI.

DO ACOMPANHAMENTO DO CONTEÚDO DAS PÁGINAS ELETRÔNICAS

Artigo 18 - Compete ao CIPM observar as páginas eletrônicas quanto aos aspectos de segurança da informação e ao C Com Soc os aspectos institucionais, comunicando ao CPD a irregularidade, para que este possa indisponibilizar imediatamente o acesso ao site.

Artigo 19 - Compete a qualquer policial militar informar, via canal de Comando, a inobservância destas Instruções.

CAPÍTULO VII.

DO GERENCIAMENTO DE SITE NA INTERNET

~~Artigo 20 - A PMESP possui o domínio "www.policiamilitar.sp.gov.br", de primeiro nível, para o acesso às informações disponibilizadas na Internet.~~

Artigo 20 - A PMESP possui o domínio "policiamilitar.sp.gov.br", de primeiro nível, para o acesso às informações disponibilizadas na Internet. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

~~Artigo 21 - O domínio "www.policiamilitar.sp.gov.br" destina-se a hospedar as páginas eletrônicas criadas e mantidas pelo Centro de Processamento de Dados (CPD), o qual é responsável pela gerência e manutenção do site oficial da PMESP na Internet.~~

Artigo 21 - O domínio "policiamilitar.sp.gov.br", administrado e mantido pelo CTel, destina-se a hospedar as páginas eletrônicas criadas e mantidas pelo Centro de Processamento de Dados (CPD), Unidade responsável pela gerência e manutenção do site oficial da PMESP na Intranet e Internet. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

Parágrafo único – O CPD também é o responsável pela gestão de domínios correlatos ao principal.

~~Artigo 22 - Cabe ao CPD:~~

Artigo 22 - Cabe ao CTel: (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

I - manter o cadastro da PMESP atualizado junto ao órgão oficial incumbido do registro de nomes de domínio e endereços de Internet no Brasil;

II - cumprir as prescrições emanadas do Comitê Gestor da Internet no Brasil (CGI);

III - manter os recursos necessários ao funcionamento e gerenciamento do domínio;

IV - supervisionar e coordenar o funcionamento dos subdomínios estabelecidos sob o nome do domínio do qual é titular, podendo, quando julgar necessário, criar subdomínios adicionais aos explicitados nestas Instruções;

V - responder, perante os órgãos oficiais competentes, pelo funcionamento do respectivo domínio e pela criação de subdomínios;

VI - prover orientação técnica no âmbito do domínio sob sua responsabilidade;

VII - identificar e sanar possíveis irregularidades constatadas na utilização do domínio, bem como seus possíveis causadores;

~~VIII - realizar o cadastro em sistemas de busca, a fim de facilitar a busca por parte de usuários da Internet.~~

VIII - regular a utilização dos domínios públicos e privados de interesse e sob administração da Polícia Militar. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

~~Artigo 23 - As páginas eletrônicas das OPM deverão estar hospedadas exclusivamente nos subdomínios disponibilizados pelo CPD.~~

Artigo 23 - As páginas eletrônicas das OPM serão hospedadas exclusivamente nos domínios disponibilizados pelo CTel, tanto na Intranet quanto na Internet. (NR dada pela Portaria nº PM1-14/02/17, de 08JUN17)

CAPÍTULO VIII DAS PRESCRIÇÕES DIVERSAS

Artigo 24 - O Comandante da OPM é responsável pela interação da OPM, por meio eletrônico, com o público externo, devendo as mensagens eletrônicas recebidas pelas OPM serem tratadas e respondidas, conforme normas contidas nas I-31-PM, podendo esta função ser delegada para o Oficial P/5.

Artigo 25 - Aspectos técnicos de segurança da informação tais como assinaturas digitais, sistemas criptográficos, bem como outros que sejam necessários de acordo com a realidade corrente, serão detalhados em documento normativo específico, elaborado pela D Tel.

Artigo 26 - As inspeções presenciais ou remotas a serem realizadas nas OPM, por parte da D Tel, sob delegação do Subcmt PM, deverão ocorrer de forma sistemática e periódica, com o intuito de verificar se as normas, constantes destas Instruções e de documentos normativos complementares, estão sendo executados corretamente.

Artigo 27 - As sugestões e propostas de alterações do estabelecido nestas Instruções deverão ser encaminhadas, via cadeia de comando para apreciação da D Tel.

Artigo 28 - Todas as referências aos Comandantes feitas nestas Instruções aplicam-se também a Chefes e/ou Diretores.

Artigo 29 - Fica estabelecido, a partir da data da publicação destas Instruções, o prazo de 60 (sessenta) dias para que os Cmt das OPM providenciem a adequação a presente norma.

Artigo 30 – Todo conteúdo publicado nas ferramentas Institucionais descritas nesta Instrução não poderá:

- I – ferir a legislação pátria em vigor, em qualquer de suas esferas;
- II – ser caluniosa, injuriosa ou difamatória;
- III – ser contrária à moral, à ética e aos bons costumes;
- IV – ser desrespeitosa ou ofensiva a Instituição;
- V – conter linguagem “chula” ou termos de baixo calão;
- VI – depreciar a Instituição;
- VII – ser contrário ao tema em discussão ou conter frases, palavras ou expressões que não se coadunem com o contexto;
- VIII – possuir *banners* ou referências publicitárias;
- IX – possuir e/ou redirecionar o usuário à páginas, arquivos criptografados e/ou protegidos por senha;
- X – conter e/ou redirecionar o usuário a programas e/ou arquivos que contenham vírus ou qualquer outro código que apresente risco;
- XI – conter qualquer tipo de assunto de caráter político ou partidário;
- XII – conter qualquer tipo de matéria ilícita, sendo considerado para tal, qualquer tipo de pornografia (adulto e/ou infantil), o erotismo, ou qualquer forma de discriminação, seja, étnica, religiosa, racial, ideológica, política ou de gênero humano.

Parágrafo único – fica proibida a publicação de assunto sensível e/ou classificado sem o devido controle de acesso, nos termos da Lei Federal 12.527 de 18 de dezembro de 2011 e do Decreto Estadual 58.052 de 16 de maio de 2012.

GLOSSÁRIO

Administrador de rede: profissional que administra um website. São suas atribuições a criação e atualização das páginas, supervisão dos programas e equipamentos, respostas às mensagens de correio eletrônico dos usuários, etc.

Aplicativos: são programas desenvolvidos para atender a necessidades e requisitos específicos do usuário.

Browser: é um aplicativo que possibilita o acesso a qualquer serviço ou recurso disponível na Internet.

Chat: forma de comunicação através de rede de computadores similar a uma conversação, na qual se trocam em tempo real mensagens escritas e/ou imagens

Criptografia: conjunto de técnicas que permitem bloquear o livre acesso às informações (como mensagens escritas, dados armazenados ou transmitidos por computador, etc.).

Download: o processo de se transferir uma cópia de um arquivo em um computador remoto para outro computador através da rede de comunicação.

Domínio: seu nome corresponde à localização (um endereço) de uma entidade na Internet. Por exemplo, o nome de domínio www.policiamilitar.sp.gov.br localiza o endereço Internet da entidade Polícia Militar; a parte "sp" representa que é do Estado de São Paulo (não obrigatório) a parte "gov" do nome do domínio reflete o propósito (governamental) da entidade e a parte "br" o país em que se situa a mesma.

E-mail: correio eletrônico.

Frame: também conhecidas como molduras, os frames (ou quadros) permitem a divisão da área de visualização dos navegadores em diversas partes diferentes. Em cada uma dessas áreas será possível exibir uma página em linguagem de programação diferente.

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Firewall: é uma solução de hardware e/ou software destinada a proteger redes e equipamentos conectados à Internet, por meio do controle de tráfego de pacotes que chegam e deixam essas redes.

Hacker: indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, geralmente a partir de uma conexão remota em uma rede de computadores.

Hardware: unidades físicas: circuitos integrados, discos e mecanismos que compõem um computador e seus periféricos.

Hiperlinks: são ponteiros ou palavras chaves destacadas em um texto, que quando "clikadas" nos levam para o assunto desejado, mesmo que esteja em outro arquivo ou servidor.

Homepage: página inicial de um site da Web. Referenciado por um endereço eletrônico ou hiperlinks. É a página de apresentação da empresa ou Instituição. Escrita em HTML, pode conter textos, imagens, sons, ponteiros ou links para outras páginas ou outros servidores da Internet, etc.

Hospedagem: refere-se ao servidor Web que hospeda pagina inicial.

Intranet: é uma rede de computadores interna de uma organização, que provê serviços e recursos da Internet.

Layout: plano ou desenho global de um documento. Na programação, a ordem e a sequência da entrada e da saída. No projeto de computadores, a disposição de circuitos e outros componentes do sistema.

Link: conexão, ou seja, elementos físicos e lógicos que interligam os computadores da rede.

News group: grupo de Notícias. Como se dividem os grupos de discussão, segundo sua área de interesse.

Protocolo: conjunto de regras que regula a interação entre dois ou mais participantes de uma comunicação.

Servidor: é uma estação que provê facilidades para outras estações de dados, tais como, servidor de arquivos, servidor de impressão, servidor de correio eletrônico, servidor Web, etc.

Servidor Web: é um tipo de servidor que provê facilidades para hospedagem e acesso às páginas eletrônicas.

Sistema Operacional: programa que permite controlar o acesso aos recursos de um sistema computacional, buscando assegurar aos usuários a realização de todas as funções básicas e essenciais daquele sistema.

Site: coleção de arquivos inter-relacionados que inclui um arquivo inicial chamado homepage (página eletrônica); uma organização ou indivíduo informa a respeito de como acessar seu site fornecendo o endereço de sua homepage.

Software: qualquer programa ou grupo de rotinas que instruem o hardware sobre a maneira como ele deve executar uma tarefa, incluem-se nesta definição, sistemas operacionais, processadores de texto, programas de aplicativos etc.

Subdomínio: é uma subdivisão de um domínio, também conhecida como domínio de segundo nível; podem existir também níveis de subdomínios; um nome de subdomínio é mapeado em um endereço eletrônico, do qual constitui, assim, uma versão legível.

Web: recurso ou serviço oferecido na Internet (Rede Mundial de Computadores) e que consiste em um sistema distribuído de acesso a informações, as quais são apresentadas na forma de hipertexto, com elos entre documentos e outros objetos (menus, índices), localizados em pontos diversos da rede.

ANEXO.
TERMO DE COMPROMISSO DE ACESSO POR MEIO DA REDE VIRTUAL PRIVADA (VPN) AOS
RECURSOS COMPUTACIONAIS DA POLÍCIA MILITAR

NOME COMPLETO DO USUÁRIO:

RE/RG:

OPM:

SEÇÃO:

O presente termo visa dar ciência ao usuário sobre as suas obrigações ao receber um login (código de identificação) e senha que lhe possibilitará acesso aos recursos computacionais da Corporação, por meio da rede virtual privada (VPN).

1. O usuário reconhece que seu acesso aos recursos computacionais da Corporação, por meio da rede virtual privada (VPN), será efetuado com a utilização da identificação de login (*código de identificação*) e senha, os quais são de uso pessoal e intransferível e cuja responsabilidade é exclusiva do seu detentor.

2. O usuário reconhece que este acesso está lhe sendo concedido em razão das suas atividades no Serviço Policial-Militar e que somente deverá ser utilizado para este fim.

3. O usuário reconhece que o acesso por meio da rede virtual privada (VPN), pode agregar riscos de quebra de confidencialidade, disponibilidade e/ou integridade das informações e/ou serviços pertencentes à Polícia Militar e que exige, portanto, maior atenção quanto às questões relacionadas com a segurança, sendo que cuidados adicionais devem ser tomados, de forma a minimizar a possibilidade de ocorrência desses riscos.

4. O usuário reconhece que os dados disponibilizados pelos sistemas de informações existentes na Corporação não podem ser divulgados a pessoas que não estejam relacionadas com a sua atividade profissional.

5. O usuário reconhece que ao utilizar equipamentos estranhos à Corporação, para efetuar acesso por meio da rede virtual privada (VPN) aos recursos computacionais da Polícia Militar, deve se certificar que este possua software antivírus instalado e atualizado, bem como, que esteja livre de programas "maliciosos", como Worms, Cavalos de Tróia ou, até mesmo, programas capazes de capturar caracteres de teclado, etc.

6. O usuário reconhece que ao cessarem os motivos que levaram a necessidade de se utilizar o acesso ao ambiente computacional da Corporação, por meio da rede virtual privada (VPN), para a execução das suas atividades, deverá solicitar a seu comandante o imediato cancelamento.

7. O usuário obriga-se a informar, imediatamente, ao seu comandante imediato acerca de qualquer violação das regras de sigilo da Polícia Militar, bem como de qualquer dos itens deste termo, por parte dele ou de quaisquer outras pessoas, inclusive nos casos de violação não intencional ou culposa de sigilo da Polícia Militar e de informações a ela inerentes.

8. O usuário reconhece e aceita o fato de que seus acessos, feitos por meio da rede virtual privada (VPN), estarão sujeitos ao monitoramento e auditoria, sem que exista a necessidade de prévio aviso.

9. O não cumprimento de quaisquer dos itens deste termo implicará na responsabilidade disciplinar, civil e criminal, no que couber, dos que estiverem envolvidos na violação.

(Cidade), _____ de _____ de _____.

(Assinatura)

(Policial Militar, funcionário civil ou terceiro contratado)
Posto/Grad, Cargo/Função, RE ou RG e CPF, OPM ou Empresa contratada

(Assinatura)

Cmt/Ch/Dir

OPM RESPONSÁVEL

DIRETORIA DE TELEMÁTICA – DTel

Avenida Cruzeiro do Sul, 260

Canindé - - São Paulo/SP

CEP – 03033-020

ÍNDICE REMISSIVO

A

acesso5

C

Comitê Gestor da Internet no Brasil.....9

D

domínio8

F

finalidade.....5

freeware8

L

Link5

O

objetivos.....5

P

páginas eletrônicas.....8

política de acesso institucional.....5

publicação8

R

Rede Privada Virtual5

S

softwares.....7

T

Termo de Compromisso6

U

usuário.....6