PREFEITURA MUNICIPAL DE PARNAMIRIM

GABINETE CIVIL

GRUPO DE CIÊNCIA E TECNOLOGIA DA INFORMAÇÃO

NUSTI

Normas de Utilização dos Serviços de Tecnologia da Informação

"Confidencialidade, Integridade e Disponibilidade"

Versão 1.0
Dezembro 2011

DECRETO Nº 5.617, DE 16 DE DEZEMBRO DE 2011

Aprova as Normas de Utilização dos Serviços de Tecnologia da Informação e dá outras providencias.

O PREFEITO DA CIDADE DE PARNAMIRIM/RN, com fundamento no art. 73, inciso IV e XII, da Lei Orgânica do Município de Parnamirim,

DECRETA:

Art. 1º - Aprova as Normas de Utilização dos Serviços de Tecnologia da Informação, constante no Anexo Único deste Decreto, elaborada pela Assessoria de Ciência e Tecnologia da Informação deste Município.

Art. 2º - Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrario.

Parnamirim/RN, 16 de dezembro de 2011.

MAURÍCIO MARQUES DOS SANTOS
Prefeito

PUBLICADO NO DIÁRIO OFICIAL DO MUNICÍPIO Nº 326 DE 23 DE DEZEMBRO DE 2011

SUMÁRIO

GESTORES

Maurício Marques do Santos – Prefeito Municipal
Marcio Cesar – Secretário Chefe Gabinete Civil

EQUIPE TÉCNICA - GCTI

Dario Candido de Medeiros – Assessor Especial de C&TI
Douglas Barbalho – Coordenador de Redes

1 APRESENTAÇÃO

A informática sempre proporcionou benefícios à sociedade. Os sistemas de computação integrados tornaram-se cada vez mais imprescindíveis para a realização dos mais variados trabalhos.

Baseado neste pensamento e conscientes do valor da informação, é que precisamos nos atentar a um ponto de grande importância, a **Segurança da informação**. Muito tem se ouvido nos últimos tempos sobre este assunto, mas nem sempre damos a ele devida atenção.

Baseado nesta preocupação, a Prefeitura de Parnamirim, através do Gabinete Civil – Assessoria Especial de Ciência e Tecnologia da Informação, vem adotando uma série de medidas para proteger as informações de sua posse ou que possa a vir a ter contato, necessárias à execução de suas atividades.

Dentre as medidas mencionadas, definimos as **Normas de Utilização dos Serviços de Tecnologia da Informação - NUSTI**, concebida para definir de forma clara e evidente, responsabilidades, direitos e deveres que devem ser conhecidos e seguidos por todos os funcionários e/ou agentes públicos vinculados a Prefeitura de Parnamirim, com a meta da busca constante de sempre podermos prestar um serviço com qualidade e confiabilidade aos nossos munícipes.

Esta norma, aplica-se a todos os funcionários, prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Prefeitura, ou acesso a informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da Prefeitura tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A violação desta política de segurança é qualquer ato que:

1. Exponha a Prefeitura a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda da perda de equipamento.

2. Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

3. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

2 OBJETIVOS

2.1 Objetivo Geral

Normatizar todas as atividades e serviços de Ciência e Tecnologia da Informação (C&TI) da Prefeitura Municipal de Parnamirim, com a finalidade maior de aumentar a segurança das informações da Prefeitura, estabelecendo procedimentos para viabilização, tanto de acessos internos, como acessos externos, às informações de posse da Prefeitura Municipal de Parnamirim.

2.2 Objetivos Específicos

a) Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização das atividades da PMP.

b) Informar ao usuário, quais os procedimentos para a correta utilização dos serviços de acessos a rede, intranet e internet oferecidos pela Prefeitura Municipal de Parnamirim.

c) Informar ao usuário a correta utilização da sua conta de acesso aos computadores.

d) Definição dos tipos de perfis de acesso a conteúdos, interno e/ou externo.

3 MISSÃO DO GCTI

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação, necessária para a realização das atividades da Prefeitura Municipal de Parnamirim. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade com aprovação do Titular do Executivo Municipal em Exercício.

4 DEFINIÇÕES

Para os efeitos e aplicações deste documento, são adotadas as seguintes definições técnicas:

a) **Rede Local**: Conjunto de hardware e software que permite a computadores individuais estabelecerem comunicação entre si, trocando e compartilhando informações e recursos;

b) **Usuários**: É o conjunto de funcionários devidamente autorizados a fazer uso de recursos computacionais como por exemplo, o sistema de correio eletrônico (E-mail) ou obter acesso as informações contidas em planilhas ou documentos de projetos para o desempenho de suas atividades funcionais.

c) **Hardware**: Componente ou conjunto de componentes físicos de um computador ou de seus periféricos;

d) **Software**: Conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas, bem como os dados a eles associados, empregados durante a utilização do sistema;

e) **Internet**: Conjunto de computadores interligados em uma rede de abrangência mundial, que se comunicam utilizando o protocolo TCP/IP;

f) **Intranet**: Conjunto de computadores e outros equipamentos de uma instituição que formam uma rede utilizando o protocolo TCP/IP e são ligados à Internet usualmente através de um sistema de proteção (Firewal);

g) **Correio eletrônico**: Serviço que possibilita a troca de mensagens através de recursos da Internet;

h) **Sítio da Internet** também conhecido como **site**: Conjunto de documentos apresentados ou disponibilizados na rede mundial (web) por um indivíduo, empresa ou instituição, que pode ser acessado em um endereço específico da rede Internet (URL – Uniform Resource Locator), podendo ser subdividido em páginas com endereços específicos e próprios;

i) **Download**: Obtenção de cópia, em máquina local, de um arquivo originalmente armazenado em máquina remota ou em rede.

j) **Freeware**: Software distribuído gratuitamente e que permite ilimitado número de cópias, além de não exigir nenhum tipo de registro. Diferente do software de domínio público, o autor do freeware mantém os direitos autorais sobre o produto e pode impedir a sua modificação, comercialização ou inclusão em um pacote de programas.

k) **Shareware**: Software que pode ser experimentado antes da compra. Alguns programas shareware funcionam somente durante um período determinado de avaliação; outros apenas mostram mensagens periodicamente lembrando o usuário que não se trata de um produto gratuito. Os autores de shareware normalmente pedem pagamentos simbólicos pelo software. Alguns chegam a pedir apenas um cartão postal como prova da satisfação com o produto.

l) **Firewall**: Medida de segurança que é implementada para limitar o acesso de terceiros a uma determinada rede ligada à Internet. O Firewall pode proteger a rede local contra os Hackers e contra Vírus, pode ser em Software ou em Hardware.

m) **GCTI**: Assessoria Especial de Ciência e Tecnologia da Informação.

n) **PMP:** Prefeitura Municipal de Parnamirim.

5 SEGURANÇA DA INFORMAÇÃO

Segurança da informação é um conjunto de medidas com o objetivo de tornar seguras as informações de posse ou confiadas a uma instituição.

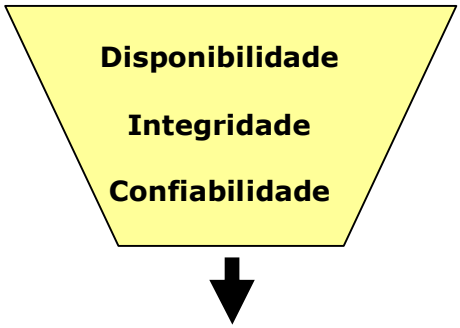
5.1 Informação Segura

Uma informação segura possui três características fundamentais:

Disponibilidade: Capacidade de estar, quando autorizado, sempre acessível e utilizável.

Integridade: Manter características de precisão e perfeição.

Confidencialidade: Estar disponível e ser divulgada apenas a indivíduos ou organizações autorizadas.



Segurança da Informação

A manutenção destes componentes e de outras propriedades, como a LEGALIDADE, a AUTENTICIDADE, a RESPONSABILIDADE e o não repúdio é uma tarefa essencial para a operação Prefeitura de Parnamirim.

5.2 Responsabilidade pela segurança da informação

Assim como a execução diária das atividades de cada um, atender as regras definidas neste documento é responsabilidade de todos, incluindo, funcionários efetivos, comissionados, estagiários, voluntários e terceiros autorizados, chamados Usuários Temporários.

A Prefeitura de Parnamirim, através do GCTI, adota uma série de processos, atividades e tecnologias para proteção das informações, mas o componente mais importante sem dúvida são os **usuários** – as pessoas que compõem a instituição. Sem elas não seria possível manter o bom funcionamento da estrutura computacional e a segurança da informação em níveis adequados.

> **ATENÇÃO**! É responsabilidade de qualquer usuário comunicar imediatamente ao GCTI quaisquer incidentes ou eventos que possam vir a por em risco as informações da Prefeitura de Parnamirim.

6 CLASSIFICAÇÃO DA INFORMAÇÃO

A Prefeitura de Parnamirim adota metodologia para classificar suas informações conforme o nível de sigilo que todos os usuários devem seguir atentamente.

A Prefeitura entende que durante seu ciclo de vida, a informação deve ser adequadamente manuseada, preservada e gerenciada. Os principais objetivos da informação são:

- Garatir seu uso racional;
- Prevenir que informações restritas sejam reveladas a pessoas ou organizações não autorizadas;
- Evitar danos ou perdas de conhecimentos e/ou projetos da instituição.

Os critérios para classificação da informação são:

6.1 Informação Pública

Oficialmente liberada para o público em geral como por exemplo Boletim Oficial, Avisos de Licitação, Pregão, Tomada de Preços, Material de Marketing, etc.

6.2 Informação de uso iterno

Restrita aos usuários da PMP, não podendo ser compartilhadas com o público em geral, tais como normas internas ou memorandos.

6.3 Informação confidencial

Possui caráter sigiloso, podendo ser comunicada apenas a usuários especialmente autorizados que necessitem conhecê-las para o desempenho de suas atividades. Caso divulgadas erroneamente, podem ocasionar danos pessoais, patrimoniais e/ou a imagem da Prefeitura de Parnamirim.

> **Obs**.: De acordo com a Constituição Federal toda e qualquer documentação gerada por ente público, pode ser requisitada por qualquer cidadão.

É de responsabilidade do responsável de cada área, Secretário, Coordenador, Gerente e/ou Supervisor, estabelecer critérios relativos ao nível de confidencialidade da informação (documentos, relatórios e/ou mídias) gerada por sua área de acordo com os critérios acima descritos.

7 MANUSEANDO INFORMAÇÕES CORRETAMENTE

Com o intuito de simplificar o processo, definimos uma tabela de Ação X Requisito que deve ser sempre levada em consideração.

7.1 Tabela de ação x Requisito

AÇÃO	REQUISITO		
	Pública	**Uso Interno**	**Confidencial**
Cópia/Exclusão	Sem restrição	Sem restrição	Aprovação formal do gestor da informação
Fax	Sem restrição	Sem restrição	Capa Padronizada
Transmissão em rede pública	Permitido	Permitido	Permitido
Descarte	Lixo comum	Lixo comum	Uso de fragmentadora ou lixo seletivo
Envio a terceiros	Sem restrição	Sem restrição	Aprovação formal do gestor da informação
Solicitação de direito acesso	Sem restrição	Aprovação do autor da informação	Aprovação formal do gestor da informação
Correio interno e externo	Envelope comum	Envelope comum	Envio apenas para destinatário específico em envelope selado
Marca indicando nível de classificação	Não necessário	Não necessário	Na capa e em todas as páginas
Registro de Acompanhamento	Não necessário	Não necessário	Não obrigatório
Contato telefônico interno e externo	Sem restrição	Sem restrição	Sem restrição

7.2 Acesso e guarda da informação

Para garantir uma boa gerência da informação, é importante definir regras claras. No tocante às suas informações, a PMP define que:

1. Toda informação deverá possuir um gestor e pelo menos um usuário;
2. O gestor é responsável por classificar a informação quanto ao grau de sigilo requerido, conforme níveis de proteção;
3. A classificação de uma informação deverá ser de conhecimento de todos os usuários autorizados.

7.3 Regras para proteger as informações

Algumas regras simples para ajudar os usuários a proteger a informação:

1. Nunca deixe documentos que não estão em uso espalhados sobre mesas ou bancadas de trabalho;
2. Informações classificadas como confidenciais devem sempre ser armazenadas de forma controlada. Mantenha documentos sempre em gavetas ou armários com chaves. Para e-mail e outros documentos eletrônicos, faça o armazenamento em pastas seguras.

> **Dica**: Se tem dúvidas, procure o **GCTI** para saber se a pasta onde armazena seus dados é segura.

7.4 Regras para descarte de informações

1. Esteja seguro que tem permissão para realizar o descarte;
2. Siga todas as recomendações da tabela de Ação x Requisito;
3. Utilize meios seguros como fragmentadoras especiais ou incineradores para o descarte de informações armazenadas em CD, DVD, disquete, fitas ou qualquer outro meio de armazenamento magnético;
4. Para informações classificadas como CONFIDENCIAL sempre registre a data, o método de descarte, a descrição dos itens descartados e colha a assinatura das pessoas que supervisionaram e testemunharam o ato.

> **Lembre-se**: É durante o descarte que ocorrem muitos incidentes de segurança. Indivíduos ou organizações mal intencionados podem tentar reconstituir informações através de material descartado incorretamente.

É importante lembrar que a informação também deve ser protegida durante comunicações verbais, sendo aplicáveis as mesmas regras.

Durante conversas, reuniões, ou mesmo festas e eventos similares, usuários devem tomar cuidados para não revelar informações a terceiros ou mesmo outros usuários que não estejam devidamente autorizados.

Nunca compartilhe informações com terceiros, incluindo repórteres, familiares e parceiros comerciais, a menos que esteja seguro que eles estejam inteiramente autorizados.

> **Lembre-se**: Ambientes públicos não são locais seguros para compartilhar informações CONFIDENCIAIS. Um estranho aparentemente sem más intenções pode estar discretamente acompanhando a sua conversa e fazer uso das informações colhidas para beneficio próprio.

7.5 Armazenamento e acesso à informação

Com o objetivo de guardar as informações eletrônicas de forma adequada e segura, a PMP dispõe de uma estrutura de armazenamento centralizada acessível a todos os usuários autorizados.

7.5.1 Acesso à informação

O acesso é concedido levando em conta as diferentes necessidades profissionais. Ou seja, se você é do departamento de contabilidade, terá acesso a todas as informações que permitam a execução do seu trabalho, mas não poderá acessar arquivos de outros setores, como recursos humanos ou compras, a menos, é claro, que isso faça parte da sua rotina de trabalho.

Para facilitar o acesso, todos os computadores são automaticamente conectados a unidades de rede específica para os dados do setor, conforme exemplo abaixo abaixo:

G:\PASTA DO SETOR
P:\PASTA PUBLICA
U:\PASTA DO USUARIO

IMPORTANTE! o armazenamento deve ser usado apenas para arquivos relacionados a atividades profissionais ou de interesse da PMP. O uso de material de caráter pessoal não é permitido.

7.5.2 Regras para armazenamento de dados.

As regras abaixo deverão ser cumpridas por todos os usuários da rede.

1. Não utilize o espaço para armazenar material que infrinja direitos autorais;
2. Não é permitido o armazenar jogos eletrônicos, material adulto ou de mau gosto, especialmente pornografia infantil (pedofilia);
3. Nunca armazene material audiovisual como músicas, vídeos, imagens, flash vídeo e qualquer outro similar, a menos, que se trate de informação autorizada pela PMP;
4. Nunca tente ou permita que outra pessoa obtenha acesso não autorizado a unidades de rede.
5. Infrações deverão ser sempre comunicadas ao GCTI.

Lembre-se: O espaço para armazenamento de arquivos é limitado portanto deve ser utilizado com cautela. Cada usuário tem uma cota até 300Mb (trezentos megabytes). Se tiver motivo aceitável, poderá solicitar mais espaço ao GCTI.

7.5.3 Cópias de segurança da informação

Cópias de segurança, também conhecidas como backups, garantem que a PMP poderá recuperar informações perdidas acidentalmente ou como resultado de algum evento que possa vir a danificar a sua estrutura computacional.

Importante: Arquivos eletrônicos não forem salvos nas unidades de armazenamento, não são incluídos na rotina de backup. Se deixar informações importantes apenas em seu computador, em caso de falha, as mesmas poderão ser irrecuperáveis. Caso necessite de mover dados para as pastas de armazenamento, contate o GCTI.

8 COMPUTADOR E LOCAL DE TRABALHO

Durante a execução de tarefas do dia-a-dia é comum recebermos na PMP prestadores de serviço, ou pessoas de outras organizações, assim como é normal que funcionários da Prefeitura transitem por outros setores além de onde estão alocados.

Desta forma, é importante evitarmos que esses indivíduos venham a ter contato com informações que não estão autorizados a conhecer.

É fundamental que se tenha sempre alguns cuidados básicos.

Para informações contidas em suporte físico (papéis e outros documentos) ou armazenadas em mídias removíveis (CDs, DVDs, cartões magnéticos, pen drives ou câmeras digitais), siga estas recomendações:

- Evite deixar **documentos** ou **mídias** expostas sobre mesas ou estações de trabalho;
- Quando se ausentar de sua estação de trabalho, verifique se seus documentos estão protegidos e armazenados em gavetas ou armários, preferencialmente trancados com chave.
- Adicionalmente, lembre-se de bloquear o seu computador quando for se ausentar por períodos prolongados.

> **Dica:** Nos sistemas operacionais utilizados pela PMP, o bloqueio do computador pode ser feito usando a combinação simultânea das teclas **Ctrl+Alt+Del** seguidas da operação **"Bloquear este computador"**.

Caso tenha dúvidas sobre como bloquear seu computador, fale com o GCTI.

8.1 Dados dos funcionários

A PMP se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução de suas atividades. Todos os Dados Pessoais de Funcionários que porventura sejam armazenados, serão considerados dados confidenciais, não poderão ser usados para fins diferentes daqueles para os quais foram coletados, não serão transferidos para terceiros, exceto quando exigido pelas suas atividades, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da PMP.

Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da PMP. Mesmo que seja autorizado o armazenamento destes dados, a PMP não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores da PMP, e jamais poderão fazer parte da rotina de backup.

8.2 Noções básicas de Segurança da Informação

8.2.1 Cuidados com credenciais e senhas de acesso

Quando alguém chega a nossas residências, antes de entrar, pedimos que se identifique. Quando é possível, usamos outros recursos, como um olho mágico ou até mesmo um sistema de câmeras.

As credenciais e senhas permitem ao sistema executar um processo similar, identificando os usuários e liberando ou não acesso à informação. Por isso, é tão importante que os usuários zelem pelas credenciais sob a sua guarda como protegem as chaves de suas residências.

Caso um indivíduo obtenha suas credenciais e senhas de acesso, ele poderá se passar por você em qualquer sistema, enviando um e-mail, copiando ou até mesmo excluindo informações importantes da PMP.

É importante que os usuários saibam que suas credenciais e senhas de acesso são pessoais e intransferíveis e que qualquer ação executada com as mesmas é de sua exclusiva responsabilidade.

Para prevenir qualquer problema, a PMP recomenda os seguintes cuidados:

- Nunca revele suas senhas a outros usuários ou terceiros;
- Não tente obter acesso a sistemas e a outros recursos com credenciais de outros usuários;
- Nunca se utilize de eventuais falhas em sistemas para obter acesso não autorizado.

8.3 Política de Senhas da PMP - Segurança

8.3.1 Permissões e senhas

Todo usuário para acessar os dados da rede da PMP, deverá possuir um login e senha previamente cadastrados pelo GCTI.

Quem deve fornecer os dados referente aos direitos do usuário é o responsável direto pela sua chefia, através da **FICHA DE CADASTRO**. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da PMP, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

O GCTI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, **a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login** e após isso a cada 45 (quarenta e cinco) dias. Por segurança, o GCTI recomenda que as senhas tenham sempre o critério mínimo de segurança estabelecidos neste documento (Item 8.3 Página 12.)

Todos os sistemas computacionais da PMP fornecem recursos necessários para proteger sua senha. Mesmo assim, é muito importante que os usuários tomem alguns cuidados na escolha e no manuseio de suas senhas:

- Nunca utilize parte de seus dados pessoais/cadastrais como base para sua senha;
- Nunca utilize nomes de familiares, amigos, colegas de trabalho ou datas importantes, como aniversários;
- Não utilize palavras existentes em qualquer dicionário, mesmo gírias ou jargões;
- Não use qualquer variação ou parte do nome Prefeitura de Parnamirim;
- Não utilize qualquer variação dos itens acima invertido ou seguido por um número.

8.3.1.1 A política de senhas da PMP obedece às seguintes normas:

- A senha deverá conter no mínimo 6 (seis) e no máximo 16 (dezesseis) caracteres;
- A senha não poderá conter nome ou sobrenome do usuário;
- A senha não poderá ser o CPF, data de nascimento, número da identidade do usuário;
- A senha deve conter obrigatoriamente números e letras;

- Na troca da senha o usuário não poderá utilizar nenhuma das últimas 10 senhas utilizadas;
- É obrigatória a alteração das senhas pelo menos uma vez a cada 180 (cento e oitenta) dias. O intervalo recomendado é a cada 30 (trinta) dias;
- Os sistemas poderão bloquear o acesso do usuário caso o mesmo tente acessar com uma senha inválida por mais de 5 (cinco) vezes;
- É obrigatório o uso de letras MAIÚSCULAS e minúsculas. Recomenda-se para uma melhor segurança de sua senha a utilização de números (**0 a 9**) e caracteres especiais, tais como: **!#$%&*O[]{}**;.

DICA: Nunca escreva ou anote sua senha. Caso prefira uma senha fácil de lembrar, utilize método de substituição de letras por similares ou caracteres especiais. Exemplo: Uma senha **Amor123!** pode ser escrita como **45or@123**!. Assim você vai conseguir lembrar sua senha com facilidade e manter um bom nível de complexidade.

IMPORTANTE: Nunca utilize senhas encontradas em exemplos. O fato da senha 45or@123! Constar aqui como exemplo, automaticamente a torna uma senha fraca.

Lembre-se, se por qualquer motivo você achar que sua senha foi comprometida ou está sendo utilizada por outra pessoa, contate imediatamente o GCTI. Dessa forma você não apenas está ajudando a identificar uma falha no sistema ou um uso indevido, mas também estará demonstrando que não está envolvido no incidente.

8.4 Contas de usuários (LOGIN)

Para facilitar a identificação, tanto de usuários como dos computadores interligado em rede, os mesmos deverão seguir os padrões abaixo especificados.

8.4.1 Usuários Administrativos

Os usuários que possuírem direitos de acesso à rede local (LAN) da Prefeitura Municipal de Parnamirim serão cadastrados obedecendo ao seguinte padrão de nomes de usuário (login):

Modelo: **primeiro nome.segundo nome**
primeironome+iniciais

Exemplo:
Nome do usuário: **Maria Helena de Sousa**
Login: **maria.helena** ou **maria.hs**

Para todos os usuários da Rede Prefeitura Municipal de Parnamirim, o e-mail será o seu login de rede seguido do domínio **"@parnamirim.rn.gov.br".**

Exemplo:
Login de usuário na rede local: **maria.hs**
Endereço de e-mail: **maria.hs@parnamirim.rn.gov.br**

8.4.1.1 Regras para cadastro

Todo usuário da rede poderá ter direito à utilização do serviço de rede local, intranet, internet e correio eletrônico, desde que haja disponibilidade de recursos de infra-estrutura de rede, através do preenchimento da **FICHA DE CADASTRO**, a qual deverá estar devidamente assinada pelo responsável do departamento onde o usuário está lotado.

Esta ficha estará disponível no site da Prefeitura Municipal de Parnamirim **www.parnamirim.rn.gov.br** e deverá ser entregue ao GCTI, Setor de Atendimento ao Usuário, que dará encaminhamento ao processo de criação e entrega ao solicitante no prazo máximo de 48h (dois dias úteis).

Ao assinar a ficha, o usuário estará aceitando todos os termos contidos neste, estando sujeito às penalidades que possam vir a ocorrer em decorrência do mau uso dos serviços disponibilizados.

Após o cadastramento, o usuário receberá um **login e uma senha provisória,** que deverá ser trocada por ele, que serão sua identificação junto aos serviços solicitados.

8.4.1.2 Admissão e demissão de funcionários: Efetivos, Temporários e Estagiários.

O setor de Recursos Humanos da PMP deverá informar ao GCTI, toda e qualquer movimentação de funcionários, temporários e/ou estagiários, e admissão/demissão que venham a utilizar sistemas, para que os mesmos possam ser cadastrados ou excluídos no sistema da PMP. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo GCTI.

Cabe ao setor que o novo funcionários será lotado comunicar ao GCTI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á PMP, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível ao GCTI, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da PMP. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

8.4.1.3 Transferência de funcionários: Efetivos, Temporários e Estagiários

Quando um funcionário for transferido de órgão ou função, o setor competente deverá comunicar o fato ao GCTI, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao(s) sistema(s) e dado(s) da PMP que tenha direito.

8.5 Regras de uso de recursos computacionais

Como parte do seu programa de proteção a segurança da informação, a PMP adota uma série de regras de uso de seus ativos computacionais, como computadores e impressoras.

Essas regras têm o intuito de proteger a informação da PMP e garantir que

quaisquer leis ou normas pertinentes sejam seguidas pelos seus usuários durante atividades profissionais desempenhadas com equipamentos da entidade.

8.5.1 Uso de Hardware

A PMP disponibiliza aos seus usuários todos os hardwares necessários para execução de suas atividades.

Para o uso correto deste recurso, é fundamentai que os usuários observem as seguintes regras:

- Não utilize equipamentos pessoais para executar atividades profissionais da PMP;
- Não utilize hardware da PMP para fins pessoais ou que não sejam de interesse da instituição;
- Não conecte dispositivos pessoais como notebooks, pen drives, cartões de memória, câmeras digitais, smartphones, dispositivos de digitalização, fax ou impressão à estrutura de rede PMP;
- Utilize o hardware dentro das recomendações do GCTI e instruções do fabricante, sempre zelando pelo bom funcionamento do equipamento;
- Desligue o equipamento, inclusive o estabilizador ou no-break, ao final do dia de trabalho ou durante ausências prolongadas. Desta forma, você estará economizando energia e ajudando a proteger o meio-ambiente.

8.5.1.1 Procedimentos em caso de falha de HARDWARE

A atribuição de manutenções, configurações e qualquer outra alteração de hardware é responsabilidade exclusiva do GCTI.

> **Dica**: Nunca tente você mesmo fazer manutenções.
> **Lembre-se**: Manutenções realizadas de forma incorreta podem ocasionar danos permanentes. Além disso, normalmente o equipamento estará energizado e o manuseio incorreto poderá ocasionar descargas elétricas (choques).

8.5.2 Uso de Softwares e Aplicativos

A PMP disponibiliza aos seus usuários todos os softwares e aplicativos necessários para execução de suas atividades.

Para o uso correto deste recurso, é essencial que os usuários observem as seguintes regras:

- A PMP respeita integralmente a lei de direitos autorais e trabalha somente com softwares licenciados, não permitindo o uso de programas não licenciados nos seus computadores;
- Não instale ou utilize de forma portátil softwares não homologados ou pessoais;
- Não use softwares que possam causar dano ou comprometer a segurança da PMP;
- Todas as instalações de software deverão ser feitas pelo GCTI. Nunca tente instalar ou utilizar um software não homologado.

- Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a PMP por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos as sansões previstas em Lei.

8.5.2.1 Softwares Homologados

Para obter uma lista dos softwares homologados, entre em contato com o GCTI ou consulte o **Anexo "A"** deste documento.

Todos os equipamentos da PMP dispõe de todos os softwares necessários para execução das atividades necessárias a cada setor.

8.5.2.2 Necessidade de novos sistemas, aplicativos e equipamentos

O GCTI é responsável pela aplicação da Política da PMP em relação a definição de compra e substituição de "software" e "hardware".

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser solicitada ao GCTI.

Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários e/ou setores, sem a prévia avaliação e/ou autorização do GCTI.

8.5.3 Dispositivos móveis

Os usuários que tiverem direito ao uso de dispositivos móveis como notebooks, smartphones e similares, de propriedade da PMP, devem estar cientes de que é muito importante que tomem alguns cuidados adicionais, principalmente quando trabalhando em ambientes externos a PMP, tais como:

- Tentar disfarçar o notebook, evitando utilizar uma bolsa portátil que desperte atenção e dê preferência a mochilas ou outra forma de transporte que não aparente estar armazenando um notebook;
- Em locais movimentados como aeroportos, shoppings e similares esteja sempre atento ao seu ambiente. A pressa pode facilitar a ação de ladrões ou mesmo o esquecimento do equipamento;
- Verifique o ambiente ao seu redor quando estiver acessando informações sigilosas. Lembre-se que em um ambiente público uma pessoa próxima pode observar furtivamente por cima do seu ombro enquanto você utiliza um arquivo ou digita uma senha;
- Antes de viagens ou ausências prolongadas, solicite ao GCTI que faça backup. Desta forma, você estará resguardado no evento de um furto.
- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades fins da PMP.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados adicionais que devem ser observados:
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível; e

- Em caso de furto registre a ocorrência em uma delegacia de polícia, comunique ao seu superior imediato e ao GCTI, na volta, envie uma cópia da ocorrência para os setores competentes.

8.5.4 Dispositivos de impressão

Dispositivos de impressão como copiadoras, impressoras e aparelhos de fax devem ser utilizados de forma racional, evitando desperdício e falhas de segurança:

- Utilize dispositivos de impressão apenas para fins de trabalho da PMP;
- Quando imprimindo, sempre leve em consideração as recomendações expostas na tabela de Ação x Requisito.

Lembre-se: Você também tem responsabilidades importantes com a preservação do meio-ambiente. A PMP recomenda que seus usuários façam impressão apenas de material estritamente necessário utilizando, onde possível, papel reciclado.

8.6 Protegendo-se de vírus e outros softwares de códigos maliciosos

Códigos maliciosos são softwares de computador desenvolvidos com o propósito especifico de executar ações maliciosas em computadores, muitas vezes ocasionando diminuição da qualidade ou paradas não programadas em serviços, como o sistema de correio, ou ocasionando a destruição de dados e até mesmo do sistema operacional do computador.

Existem diferentes tipos de códigos maliciosos destinados a executar tarefas específicas, dentre os quais temos:

Vírus: Software malicioso com alto poder de replicação que se propaga adicionando seu código a outros programas e arquivos no computador. Um vírus pode causar um impacto devastador chegando até a destruir programas e arquivos.

Cavalo de Tróia: Assim como na mitologia grega, o Cavalo de Tróia é um programa geralmente recebido como um "presente" como, por exemplo, cartão virtual, fotos, um protetor de tela ou jogo. Além das funções para as quais aparentemente foi projetado, o Cavalo de Tróia também executa, sem o conhecimento do usuário, ações maliciosas, como captura de informações sensíveis (senha, dados bancários, informações pessoais, dados de cartão de crédito) ou mesmo a instalação de um vírus ou backdoor ou keylogger.

Verme: Também conhecido como **worm**, são códigos maliciosos que se multiplicam através da rede explorando falhas e vulnerabilidades dos programas instalados no computador sem a necessidade de ser executado diretamente. Diferentemente dos vírus, normalmente não causam danos como a infecção de arquivos ou a destruição de informações, mas podem consumir recursos como a conexão com a rede ou internet e espaço no disco riqido.

Keylogger: É um programa capaz de capturar e armazenar as teclas digitadas pelo usuário do computador como, por exemplo, senhas e mensagens de correio eletrônico. Quando associadas a outras ameaças, como um *backdoor,* podem ser acessadas por um usuário remoto.

Backdoor: Um atacante normalmente busca garantir seu acesso a um sistema comprometido sem ter que utilizar o mesmo método que permitiu a

invasão inicial. Um *backdoor* viabiliza o retorno do invasor, sem ser notado, a um sistema previamente atacado, permitindo que novas ações sejam executadas como, por exemplo, coletar informações capturadas por um *keylogger* ou instalar novos tipos de vírus e demais softwares maliciosos.

Novas ameaças surgem diariamente e são rapidamente propagadas através de redes públicas como a internet, demandando controles para evitar que sistemas e serviços sejam comprometidos.

A PMP adota diversas ferramentas para prevenção e controle de códigos maliciosos em sua rede, serviços e demais recursos computacionais. Atualizações freqüentes são realizadas para corrigir vulnerabilidades de softwares e sistemas, assim como para obter as mais novas assinaturas contra vírus e softwares maliciosos.

8.6.1 Como um computador pode ser infectado

Nenhum sistema de antivírus é 100% eficaz. O constante surgimento de novas ameaças, assim como pessoas mal intencionadas buscando falhas e vulnerabilidades em sistemas, eventualmente permite que um novo código malicioso infecte um computador mesmo quando protegido.

Desta forma, é necessário que todos os usuários façam a sua parte. Para isso, a PMP recomenda as seguintes práticas de segurança:

- Nunca execute arquivos não solicitados recebidos por correio eletrônico ou outras fontes, mesmo que sejam de pessoas conhecidas. Caso seja necessário abrir o arquivo, esteja certo que o mesmo foi analisado pelo software de antivírus;
- Nunca utilize mídias de armazenamento removível como CDS, DVDS, cartões, pen drives e similares sem primeiro realizar uma varredura com o software de antivírus.
- Não utilize intencionalmente softwares ou aplicativos que possuam ou possam conter vírus e outros códigos maliciosos.
- Finalmente, caso você suspeite que seu computador esteja infectado, entre em contato com o GCTI.

8.6.2 Engenharia Social

O termo **Engenharia Social** é concebido como o ato de manipular pessoas para que executem tarefas ou forneçam informações que podem ser utilizadas para obter acesso não autorizado a outros recursos e informações.

A Engenharia Social abusa da ingenuidade e credulidade de usuários, evitando um processo longo para quebrar senhas ou explorar vulnerabilidades e falhas existentes em sistemas.

Existem diferentes técnicas de Engenharia Social nas quais o atacante pode "criar" um cenário falso, personificando, por exemplo, colegas de trabalho, autoridades, policiais ou qualquer outra personalidade que na concepção da vítima tenha autoridade e o "direito de conhecer" a informação solicitada.

Outros métodos, como o phishing, incluem o envio em massa de mensagens de correio eletrônico aparentemente originadas de instituições legitimas como bancos, operadoras de cartão de crédito ou órgãos de proteção ao crédito.

Essas mensagens solicitam ao usuário a confirmação de dados sigilosos como senhas, dados bancários, informações pessoais, dados de cartão de crédito e contém quase sempre um link para um site fraudulento que simula a aparência de um site legítimo, incluindo mesmo logomarca e conteúdo.

8.6.2.1 Como se proteger de ataques de Engenharia Social

Diferente de outras ameaças em geral, não é possível utilizar uma ferramenta para prevenir ou detectar ataques baseados em Engenharia Social. Neste caso, a sua melhor arma é o bom senso.

Os usuários devem conhecer bem as normas deste documento. Desta forma, estarão inteirados dos procedimentos da PMP e poderão reconhecer facilmente uma tentativa de uso de Engenharia Social.

Adicionalmente, algumas dicas de segurança podem ajudar a prevenir esse tipo de ataque:

- Esteja atento para abordagens via telefone ou qualquer outro meio de comunicação onde uma pessoa - geralmente falando em nome de uma instituição - solicita diversas informações, incluindo confidenciais;
- O GCTI da PMP não solicita informações sigilosas ou credenciais de acesso por telefone ou e-mail. Sob nenhuma hipótese forneça essas informações;
- Instituições legítimas evitam enviar mensagens de correio eletrônico não solicitadas. Desconfie de qualquer mensagem que solicite informações e para tirar a dúvida, procure entrar em contato com uma fonte confiável dentro da Prefeitura.

Finalmente, caso você suspeite que foi vítima ou que possa estar sendo abordado por indivíduos com intenções suspeitas, entre em contato com o GCTI.

8.6.3 SPAM - Envio de mensagens em massa

O termo SPAM é utilizado para definir o envio, geralmente em massa, de mensagens eletrônicas não solicitadas.

O envio de mensagens não solicitadas prejudica principalmente usuários do sistema de correio eletrônico que podem ter seu desempenho reduzido devido à quantidade de mensagens desnecessárias.

Adicionalmente, com o amplo uso do correio eletrônico como ferramenta de trabalho, o *SPAM* aumenta o tempo gasto pelo usuário para ler, separar e excluir mensagens desnecessárias, consequentemente diminuindo sua produtividade.

O SPAM pode ainda inviabilizar a entrega de mensagens válidas, pois provedores de serviço de internet, mesmo empresas, podem ser incluídas em listas de bloqueio caso seus usuários estejam envolvidos no envio de mensagens não solicitadas.

A PMP adota ferramentas para proteção contra mensagens eletrônicas não solicitadas.

Ainda assim, é necessário que seus usuários adotem alguns cuidados:

- Evite divulgar seu endereço de correio eletrônico (e-mail) em sites da internet como listas de discussão, blogs e redes sociais;
- Nunca responda a mensagens de SPAM. Esta é uma forma de garantir que seu endereço eletrônico é válido e ele certamente será utilizado durante o envio de novas mensagens;
- Nunca utilize a estrutura computacional da PMP para enviar mensagens não solicitadas, especialmente em massa;
- Reporte eventuais mensagens não solicitadas ao GCTI.

9 ACESSO A INTERNET E REDES EXTERNAS

A Internet é um recurso essencial para execução das atividades profissionais necessárias para o bom funcionamento da PMP. Desta forma, a organização provê aos seus usuários acesso a rede mundial de computadores e qualquer outra que seja necessária.

O acesso a internet também apresenta ameaças que devem ser adequadamente gerenciadas de forma a resguardar a segurança da informação da PMP e de seus usuários.

Desta forma, é importante que todos conheçam e sigam as seguintes regras para acesso a internet:

1. Sempre se autentique através de usuário e senha antes de obter acesso a internet;
2. O acesso a internet não é um benefício. Utilize-o exclusivamente para atividades profissionais ou aprovadas pela PMP;
3. Você não terá acesso a qualquer serviço público de mensagens instantâneas como MSN, Yahoo! Messenger, ICQ ou similares. Caso em sua atividade seja necessário o uso desses serviços, solicite formalmente para o GCTI, através de sua Chefia, que irá analisar e dar o devido deferimento;
4. Usuários não devem acessar sites com conteúdo pertencente às seguintes categorias:
    a) Material adulto ou de mau gosto;
    b) Pornografia infantil (pedofilia);
    c) Material que incite o uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim com qualquer outro que possa infringir a legislação vigente;
    d) Sites de relacionamento e redes sociais;
    e) Jogos e/ou qualquer tipo de recreação;
    f) Sites de streaming de áudio ou vídeo.
5. Não acesse sites ou serviços na internet que possam resultar em falhas de segurança na infraestrutura computacional da PMP.

A PMP resguarda-se o direito de monitorar e registrar o uso/acesso a internet dentro de sua rede. Este monitoramento tem como único objetivo validar o respeito às normas da organização, bem como produzir evidências durante eventuais violações de conduta e/ou a legislação em vigor.

> **Lembre-se:** De acordo com a lei nº 10.764, de 12 novembro de 2003 a pedofilia é considerada crime com pena de reclusão de 2 (dois) a 6 (seis) anos e multa.

9.1 Perfil Padrão de Acesso a Internet

Os sítios na Internet estarão agrupados por categorias.
O perfil de acesso padrão a Internet obedecerá às seguintes regras, organizadas por categoria:

9.1.1 Sítios com conteúdo apenas de pesquisa que estarão disponíveis a qualquer hora:

- Compras
- Crimes e terrorismo
- Drogas e álcool
- Finanças e Investimentos
- Notícias e portais
- Racismo/Preconceito
- Governo

9.1.2 Sítios que estarão disponíveis de 12:00h às 14:00h e após as 18:00hs:

- Astrologia e Misticismo
- Diversão e Entretenimento
- Esportes
- Hobbies
- Veículos e Motores
- Viagens
- Mídias sociais (MSN, Youtube, Orkut, Facebook, etc)

9.1.3 Sítios que estarão sempre indisponíveis:

- Bate-papo
- Erotismo e Nudez
- Hackers
- Jogos de Azar e Jogos eletrônicos
- Música e MP3
- Namoro e sexo explícito
- Violência
- Armazenamento de arquivos
- Rádio e TV
- Blogs/Fotolog
- Downloads de software
- Navegação anônima
- Ganhe navegando
- Relacionamento
- Procura de Emprego

O acesso a rede e a internet pode ser realizado por todos os usuários que obtiveram permissão através da **ficha de solicitação**, preferencialmente, utilizada para finalidades profissionais ou necessárias para o bom andamento do serviço público.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Chefia e/ou Direção de cada um, com base em recomendação do GCTI e destas normas. Não é permitido instalar programas provenientes da Internet nos computadores da PMP, sem expressa anuência do GCTI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Sites que não contenham informações que agreguem conhecimento profissional e/ou para as atividades da PMP não devem ser acessados.

> **ATENÇÃO**: O uso da Internet será monitorado pelo GCTI, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

9.2 Das proibições

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso por qualquer usuário a sítios (sites) cujos conteúdos não sejam úteis e indispensáveis à atividade laboral tais como os:

- que contenham material pornográfico, de pedofilia e assemelhados;
- que contenham propaganda de ideologias contrárias ao regime democrático, bem como façam a apologia do uso da violência;
- que contenham material que faça apologia a atividades criminosas assim previstas no nosso país ou no exterior, bem como venha ensinar ou facilitar a prática de crimes assim previstos nas legislações brasileiras ou no exterior;
- que contenham exibição de material inconveniente ao ambiente de trabalho e cujo conteúdo cause desconforto ao ser humano médio;
- que contenham conteúdo hacker ou similar.

> **ATENÇÃO**: É terminantemente proibido fazer download de arquivos de músicas, jogos, filmes e softwares aplicativos, entre outros, sob pena de advertência.

9.3 Acesso remoto

A PMP provê acesso remoto a seus usuários para que possam realizar atividades profissionais. Os acessos são realizados através da internet e são protegidos por ferramentas que garantem que a transferência de informação esteja sempre segura e contra terceiros não autorizados.

O acesso remoto é concedido apenas com base nas necessidades de trabalho. Se durante suas atividades você estiver constantemente fora das dependências da PMP e precisar de acesso a algum recurso ou serviço, você poderá entrar em contato com seu chefe para que ele solicite o acesso remoto. Entretanto, é importante compreender algumas regras:

- A concessão do acesso remoto é feita com base no principio do mínimo recurso necessário, ou seja, você normalmente não terá acesso a toda rede, mas apenas ao recurso que precisa para trabalhar;
- O usuário é o único responsável por toda ação executada com suas credenciais. Dessa forma, você é responsável por seguir todas as medidas de segurança que garantam que pessoas não autorizadas não obtenham acesso remoto;
- Caso esteja usando dispositivos de autenticação como tokens ou smatcards, zele pelo bom uso e segurança dos mesmos;
- Nunca tente obter acesso remoto a recursos aos quais não esteja autorizado.

9.4 Mensagens Instantâneas

A PMP**,** como regra não permite o acesso a ferramentas públicas de mensagem instantâneas. Entretanto, pode autorizar o uso ou disponibilizar uma ferramenta homologada para comunicação via mensagens instantâneas dentro da PMP.

Para o uso do sistema de mensagens instantâneas, os usuários devem observar as seguintes regras:

- Utilize o sistema unicamente para transmissão e recebimento de mensagens relacionadas com atividades profissionais;
- Seja cortês, utilize boas práticas de escrita e evite termos ou palavras de baixo calão;
- Nunca tente utilizar o sistema de mensagens instantâneas para forjar ou simular falsa identidade;
- Nunca faça disseminação de informações de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
- Quando estiver transmitindo informações sensíveis lembre-se de atender as recomendações da tabela de Ação x Requisito.

OBSERVAÇÃO: A PMP resguarda-se o direito de monitorar e registrar o uso do sistema de mensagens instantâneas. Este monitoramento tem como único objetivo validar o respeito às normas da organização, bem como produzir evidências durante eventuais violações de conduta e/ou a legislação em vigor.

9.5 Correio Eletrônico (E-Mail)

Todos os usuários devem compreender que o sistema de correio eletrônico é uma ferramenta institucional utilizada apenas durante atividades profissionais, não sendo permitido o seu uso para fins pessoais ou que não sejam de interesse da PMP.

A PMP estabelece o endereço de correio eletrônico de seus usuários a mesma identificação do login de rede, conforme o formato a seguir, :

nome.sobrenome@parnamirim.rn.gov.br

Sou conhecido por outro nome, posso mudar esta regra?

Caso você tenha uma boa justificativa ou existe uma coincidência no seu nome com o de outro colaborador, você pode se dirigir ao GCTI para solicitar um e-mail diferente do padrão especificado. Porém, esta solicitação será analisada e concedida apenas quando o GCTI julgar ser necessário.

A PMP utiliza um modelo padronizado para assinatura, que deverá estar presente em todas as mensagens de correio eletrônico apresentando os seguintes itens:

- Nome Completo;
- Setor;
- Prefeitura de Parnamirim-RN;
- Contatos

Exemplo:
CARLOS Jose da Silva
Secretaria de Habitação
Prefeitura de Parnamirim-RN
(84) 3644-9555 / (84) 9418-4433
E-mail: Carlos.jose@parnamirim.rn.gov.br

Após a assinatura padrão, deverá ser exibido o seguinte aviso de confidencialidade:

As informações contidas nesta mensagem são CONFIDENCIAIS, protegidas pelo sigilo legal e por direitos autorais. A divulgação, distribuição, reprodução ou qualquer forma de utilização do teor deste documento depende de autorização do emissor, sujeitando-se o infrator às sanções legais. O emissor desta mensagem utiliza o recurso somente no exercício do seu trabalho ou em razão dele, eximindo-se PREFEITURA MUNICIPAL DE PARNAMIRIM-RN de qualquer responsabilidade por utilização indevida ou pessoal. Caso esta comunicação tenha sido recebida por engano, favor avisar imediatamente, respondendo esta mensagem.

Antes de imprimir esse e-mail, pense em seu compromisso com o Meio Ambiente. Verifique se o equipamento possui recursos como impressão frente e verso, modo econômico, entre outros.

9.5.1 Regras de uso

Para o uso do sistema de correio eletrônico, os usuários devem observar as seguintes regras:

1. Utilize o sistema unicamente para transmissão e recebimento de mensagens relacionadas com atividades profissionais;
2. Seja cortês, utilize boas práticas de escrita e evite termos ou palavras de baixo calão;
3. Procure sempre enviar informação classificada como confidencial através de endereços eletrônicos institucionais;
4. Não inscreva seu endereço de correio eletrônico em listas de distribuição que não tenham relacionamento com atividades profissionais;
5. Nunca faça disseminação de informações de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
6. Nunca tente utilizar o sistema de correio eletrônico para forjar ou simular falsa identidade;
7. Não utilize o sistema de correio eletrônico para disseminar mensagens caracterizadas como SPAM ou que possam conter vírus e outros softwares maliciosos
8. Quando estiver transmitindo informações sensíveis lembre-se de atender as recomendações da tabela de Ação x Requisito.

9.5.2 Proibições

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. O usuário **NÃO** poderá utilizar o serviço de correio eletrônico para:

1. modificar arquivos ou assumir, sem autorização, a identidade de outro usuário;
2. prejudicar intencionalmente usuários da Internet, através do envio de programas e acesso não autorizado a computadores, ou de alterações de arquivos de programas;

3. utilizar-se do serviço de propriedade da Prefeitura, desvirtuando sua finalidade com o intuito de cometer fraude;
4. utilizar o serviço de Correio-Eletrônico de qualquer forma a participar em atividades de pesquisa comercial, concursos, correntes, lixo eletrônico ou quaisquer mensagens periódicas ou não-solicitadas (comerciais ou não) ou abusivas também conhecidas como SPAM;
5. utilizar a solução para participação em campanhas eleitorais, cívico-sociais e mesmo veicular informações de caráter eleitoral, seja dele próprio ou de terceiros;
6. difamar, ofender, perturbar a tranqüilidade alheia, perseguir, ameaçar ou, de qualquer outra forma, violar direitos de terceiros;
7. publicar, postar, carregar, distribuir ou divulgar quaisquer tópicos, nomes, materiais ou informações que incentivem a discriminação, ódio ou violência com relação a uma pessoa ou a um grupo devido à sua raça, religião ou nacionalidade;
8. usar quaisquer materiais ou informações, incluindo imagens ou fotografias disponíveis nos sítios de propriedade da Prefeitura, de modo a infringir quaisquer direitos autorais, marcas registradas, patentes, segredos comerciais ou outros direitos de propriedade de terceiros;
9. enviar arquivos que contenham vírus, cavalos de tróia, bombas-relógio, arquivos corrompidos ou quaisquer outros softwares ou programas semelhantes que possam danificar a operação de outros computadores ou a propriedade de terceiros;
10. violar, através da utilização do serviço, qualquer código de conduta ou outras diretrizes que possam ser aplicáveis a qualquer serviço de comunicação; e
11. veicular, incitar ou estimular a pedofilia e similares (pornografia);

> **OBSERVAÇÃO**: A PMP resguarda-se o direito de monitorar e registrar o uso do sistema de correio eletrônico. Este monitoramento tem como único objetivo validar o respeito às normas da organização, bem como produzir evidências durante eventuais violações de conduta e/ou a legislação em vigor.

9.5.3 Do Uso de Softwares para Envio e Recebimento de E-Mail

Para os usuários que fizerem uso do software de cliente de correio eletrônico tais como Microsoft Outlook, os mesmos deverão solicitar auxilio aos técnicos do apoio ao usuário, pois os mesmos necessitarão configurar o software para que os e-mails sejam baixados para o computador, mas não sejam apagados do servidor. Esta medida será adotada para evitar a perda dos e-mails em caso de pane no computador do usuário. Desta forma os e-mails estarão assegurados uma vez que será realizado backup diário do servidor de e-mail.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da PMP. O GCTI poderá, visando evitar a entrada de vírus na rede, bloquear o recebimento de e-mails provenientes de sites gratuitos.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o GCTI fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

9.5.4 Cuidados especiais com o E-Mail

1. O e-mail deverá ser verificado regularmente sempre que o usuário estiver trabalhando no microcomputador. Ao encerrar suas atividades no microcomputador o usuário deverá encerrar a sessão.
2. As mensagens do e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). Deve-se proibir a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela. Quaisquer leituras indevidas e injustificadas de mensagens de outros usuários serão tratadas conforme as normas da PMP. e
3. As mensagens já lidas ou sem utilidade devem ser apagadas regularmente, para que a caixa postal do usuário não exceda o tamanho limite de 150 MB, causando a impossibilidade de recebimento de novos e-mails que por ventura sejam encaminhados.

10 UTILIZAÇÃO DA REDE DE DADOS

Os recursos da rede de dados da Prefeitura deverão ser utilizados exclusivamente para fins de atividades laborais relativas à Prefeitura, conforme abaixo:

1. O Servidor de Arquivos (BUZIOS) deve ser utilizado **SOMENTE** para armazenamento dos arquivos de trabalho da Prefeitura Municipal de Parnamirim, tais como: ofícios, memorandos, pareceres, apostilas, apresentações de projetos e/ou programas da Prefeitura Municipal de Parnamirim ou de terceiros, arquivos com imagem ou som relativos à Prefeitura Municipal de Parnamirim.
2. **Não deve ser utilizado** para armazenar arquivos pessoais dos usuários, tais como: fotos, apresentações do tipo correntes, vídeos, programas, etc. Os arquivos pessoais deverão ser armazenados na estação de trabalho do usuário.
3. O usuário deverá efetuar *logoff* sempre que terminar o uso da estação de trabalho.
4. O usuário é o único responsável pelo uso da sua identificação (login) na rede e internet, quaisquer ações que possam vir a ocorrer que prejudiquem outros usuários serão de total responsabilidade do usuário.
5. O usuário não deverá compartilhar sua senha com outros usuários. Caso, o usuário perceba que outro usuário possa estar utilizando seu login de acesso, o mesmo deverá informar imediatamente ao CTI, para efetuar a troca da senha e auditoria das atividades executadas com este login.
6. Cabe ao chefe de departamento informar ao CTI, sempre que um usuário se desligar do setor, para que sejam aplicadas as devidas restrições de acessos a este usuário.

7. Com o intuito de aumentar a segurança da rede, o usuário deverá alterar sua senha a cada 45 dias.
8. O acesso especial a informações ou outros privilégios só pode ser usado para o exercício de tarefas oficiais. Informações obtidas por meio de direitos especiais e privilégios devem ser tratados como privativas e totalmente confidenciais pelos administradores, que responderão por qualquer uso indevido.

10.1 Responsabilidades das Chefias

Os Secretários, Coordenadores, Gerentes, Supervisores, etc, são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da PMP, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido neste documento.

O GCTI fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

10.2 Responsabilidades dos Usuários

10.2.1 Segurança

1. O usuário é responsável pela segurança e integridade das informações da PREFEITURA DE PARNAMIRIM armazenadas nos computadores sob sua responsabilidade. Tal responsabilidade inclui fazer regularmente cópias de segurança de seus dados (BACK-UP's).
2. Em se tratando de segurança no uso dos recursos computacionais da PREFEITURA DE PARNAMIRIM, os usuários **não** podem efetuar ou tentar efetuar os seguintes procedimentos:

    a) passar por outra pessoa ou camuflar sua identidade ao utilizar os recursos computacionais da PREFEITURA DE PARNAMIRIM;

    b) efetuar qualquer tipo de acesso não autorizado a dados ou tentar alterá-los, como por exemplo, ler mensagens pessoais de terceiros ou acessar arquivos confidenciais;

    c) violar ou tentar violar os sistemas de segurança, como quebrar ou tentar decodificar identificação ou senhas de terceiros;

    d) interceptar transmissão de dados não destinados ao seu próprio acesso, seja monitorando barramentos de dados, ou através da rede;

    e) efetuar interferência em serviços de outros usuários ou o seu bloqueio provocando, por exemplo, congestionamento da rede, inserindo *malware* ou tentando a apropriação de mais recursos do que os alocados à sua conta.

10.2.2 Das Proibições

1. Os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicação instalados na Prefeitura, de sua propriedade ou de qualquer outra instituição ou pessoa. Essas alterações incluem, mas não se limitam, às alterações de dados, reconfiguração de parâmetros de controle ou mudanças no firmware.
2. Nenhum usuário pode, em quaisquer circunstâncias, usar a rede da PREFEITURA DE PARNAMIRIM para difamar, caluniar ou molestar outras pessoas.
3. Qualquer ato neste sentido será passível de punição. Entende-se por molestamento o uso intencional da rede para perturbar, amedrontar, ameaçar e ofender pessoas, ou mesmo causar danos e/ou prejudicar as atividades da PREFEITURA DE PARNAMIRIM ou de outros órgãos ou empresas.
4. não é permitido ao usuário servir-se dos recursos de informática da Prefeitura para usar, examinar, copiar, armazenar ou instalar programas ou qualquer outro material protegido por direito autoral (*copyright*), sem que possua licença ou autorização específica para tal;
5. nenhum software pode ser instalado, copiado ou usado na PREFEITURA DE PARNAMIRIM sem a permissão do portador da licença de uso. Todo software deverá ser devidamente licenciado e todas as medidas necessárias (instalação, uso, cópia, número de usuários simultâneos, termos de licença, dentre outros) devem ser rigorosamente cumpridas, sob orientação do CTI.
6. não será permitido ao usuário instalar software adquirido através da Internet, mesmo sendo de licença gratuita, nem transferência dos mesmos por meios eletrônicos através de FTP, contas de e-mail ou similar;
7. fica proibido ao usuário copiar softwares que não possuam licença freeware ou shareware ou qualquer material, que não seja de domínio público, via Internet para contas de e-mail particulares, disquetes, discos virtuais ou similares;
8. fica proibido a utilização de técnicas ou programas para invasão, aquisição de senhas, ou qualquer operação que coloque em risco a segurança da Prefeitura e de terceiros;
9. É proibido o uso de computadores e redes da Prefeitura em campanhas políticas ou propagandas comerciais.
10. Computadores, redes e outros serviços não podem ser usados para trabalhos particulares ou em benefício de organizações que não tenham relação com a Prefeitura, exceto quando estes trabalhos se referirem a atividades acadêmicas. Esses e outros usos tais como (mensagens eletrônicas ou armazenamento de dados em computadores pessoais) não devem ser excessivos e não podem interferir no acesso de outros usuários a estes recursos.
11. Não é permitida a utilização dos recursos computacionais da PREFEITURA DE PARNAMIRIM para benefício financeiro direto ou indireto, próprio ou de terceiros fora da instituição, sujeitando-se o infrator à imediata suspensão

de sua conta, sem prejuízo da aplicação das demais penalidades cabíveis previstas no Serviço Público Municipal.

12. Sem uma autorização específica, os usuários não podem ligar ou desligar fisicamente os recursos computacionais da PREFEITURA DE PARNAMIRIM, especialmente as estações de trabalho e componentes externos, como cabos, impressoras, discos ou sistemas de vídeo e equipamentos de rede.
13. Não é permitido o uso de material de consumo de informática da Prefeitura para fins particulares.
14. A Prefeitura Municipal de Parnamirim não poderá ser responsabilizada por quaisquer roubos de senhas que possam vir a ocorrer por acesso à sítios de bancos e/ou outras instituições financeiras através da rede da Prefeitura Municipal de Parnamirim.

10.2.3 Outras Recomendações

1. Nenhum usuário pode acessar, copiar, alterar ou remover arquivos pessoais de terceiros sem autorização explícita.
2. O usuário é inteiramente responsável pelo uso de sua conta, senha e outros tipos de autorização, que são de uso individual e não podem ser compartilhados com outros.
3. O **usuário autorizado** não pode executar ou configurar *software* ou *hardware* com a intenção de permitir o acesso a usuários não autorizados.
4. Todos os usuários e unidades têm o dever de denunciar qualquer tentativa de acesso não autorizado ou qualquer outro uso indevido de computadores e redes da PREFEITURA DE PARNAMIRIM. Ao testemunhar ou tomar conhecimento (por quaisquer meios) de problemas relacionados à segurança ou ao uso abusivo de computadores e redes da Prefeitura, incluindo o desrespeito a este regulamento, o usuário deve tomar imediatamente as providências necessárias, que estiverem a seu alcance, para garantir a segurança e a conservação dos recursos de informação. Na ocorrência destes eventos, o usuário deverá avisar, imediatamente, ao CTI.
5. É de responsabilidade do usuário manter os CD's, DVD's, discos, fitas magnéticas e disquetes sempre nas suas respectivas embalagens protetoras quando não estiverem em uso, protegendo-os das grandes variações de temperatura e umidade.
6. O usuário não deve manipular líquidos ou substâncias que possam danificar os equipamentos/materiais de informática, segurando-os sempre de maneira a não tocar na sua superfície magnética ou ótica.
7. O usuário deve manter fora do alcance de equipamentos, peças que possuam campo magnético, tais como: tubos de imagem, motores, ventiladores, tesouras, ferramentas metálicas, entre outros.

10.3 Responsabilidades do GCTI

10.3.1 Segurança

Os responsáveis pela administração da rede têm autorização para utilizarem os sistemas de segurança que julgarem adequados à manutenção da normalidade dos trabalhos. Serão consideradas nocivas ao sistema, as seguintes atividades:

1. uso de qualquer dispositivo para interceptar ou decodificar senhas, ou acesso similar ao controle de informações;
2. criar ou propagar *malwares*, danificar serviços e arquivos;
3. destruir ou danificar intencionalmente equipamentos, *software* ou dados pertencentes à Prefeitura ou a outros usuários;
4. obter acesso a recursos não autorizados;
5. utilizar os recursos de computação para o monitoramento não autorizado de mensagens eletrônicas ou qualquer transmissão de dados.

Os agentes de administração dos recursos da rede são responsáveis pelas medidas de segurança necessárias para garantir o uso adequado e a integridade de informações relativas à Prefeitura e a cada usuário.

10.3.2 Outras Recomendações

1. Compete ao GCTI, a gestão dos sistemas de informação e dos recursos computacionais de processamento, armazenamento e de transmissão de dados da PREFEITURA DE PARNAMIRIM.
2. É de responsabilidade do GCTI manter um cadastro atualizado de todos os usuários dos recursos computacionais da Prefeitura, bem como a regulamentação da concessão de acessos, seja internamente ou a partir de pontos externos à Prefeitura.
3. Cuidar da administração dos recursos da rede de computadores da PREFEITURA DE PARNAMIRIM e designar colaboradores para tal função. Garantir a segurança de suas áreas e controlar o acesso físico aos equipamentos sob sua responsabilidade.
4. Adotar medidas apropriadas de segurança em relação aos recursos da rede e informações sob sua responsabilidade.
5. Preservar informações confidenciais como, por exemplo, arquivos de usuário e códigos de acesso ao sistema.
6. Administrar devidamente as permissões de acesso.
7. Monitorar os recursos da rede para controlar tentativas de violação das normas de uso e impedir acessos não autorizados de usuários externos à comunidade da PREFEITURA DE PARNAMIRIM.
8. Caberá ao GCTI auxiliar a na análise e aprovação do conteúdo de quaisquer publicações oficiais da PREFEITURA DE PARNAMIRIM, via Internet e/ou Intranet, tais como *home pages*, notícias, entre outras.
9. Sempre que julgar necessário à preservação da integridade dos recursos computacionais, dos serviços aos usuários ou dos dados, o GCTI poderá suspender, temporariamente, qualquer conta de uso restrito ou privilegiada, sendo ou não o responsável pela conta suspeito de alguma violação.

11 POLÍTICA DE BACKUP (CÓPIA DE SEGURANÇA)

11.1 Compartilhamento de dados

Não é permitido o compartilhamento de pastas nos computadores e desktops da PMP, pois cada setor ou usuário da máquina é responsável pelo armazenamento de informações em suas respectivas máquinas de trabalho.

11.2 BACKUP (Cópia de seguranças dos dasos)

Todos os bancos de dados da PMP deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do GCTI e deverão ser feitas diariamente.

O conjunto de backup armazenado externamente deverá sofrer rodízio semanal com um dos conjuntos de backup ativo. Validação do Backup – Mensalmente o backup devera ser testado pelo pessoal do GCTI, voltando-se parte ou todo o conteúdo do backup em um HD previamente definido para este fim. Esta operação devera ser acompanhada pelo responsável por supervisionar toda a área de TI da PMP.

11.3 Cópias de segurança de arquivos em desktops

Não é política da PMP o armazenamento de dados em desktops individuais, entretanto, se existirem alguns programas que não permitem o armazenamento em rede, o GCTI deverá ser comunicado para que alerte e instrua o usuário responsável para que ele faça backup dos dados dessa maquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos trabalhos da PMP.

11.4 Segurança e integridade dos dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do GCTI, assim como a manutenção, alteração e atualização de equipamentos e programas.

Serão executados diariamente procedimentos de salva-guarda das informações geradas e armazenadas pela Prefeitura Municipal de Parnamirim, nos servidores da rede, com vistas a garantir o bom andamento das atividades desenvolvidas pelos usuários em caso de pane de algum computador ou mesmo em caso de perda parcial ou total de informações seja por falha humana ou eletrônica.

11.5 Tipo de Backup

O tipo de backup a ser realizado será o **Backup Total**. Este backup consiste na total captura de todos os dados, incluindo arquivos de todas as unidades de disco rígido. Cada arquivo é marcado como tendo sido submetido a backup; ou seja, o atributo de arquivamento é desmarcado ou redefinido.

Uma fita atualizada de backup total pode ser usada para restaurar um servidor completamente em um determinado momento.

Algumas das vantagens deste tipo de backup é a cópia total dos dados que significa que você tem uma cópia completa de todos os dados, se for necessária uma recuperação do sistema é mais prático e ainda o rápido acesso aos dados de backup, uma vez que você não precisa pesquisar em várias fitas para localizar o arquivo que deseja restaurar, porque os backups totais incluem todos os dados contidos nos discos rígidos em um determinado momento.

Algumas das desvantagens são os dados redundantes, porque os dados alterados e não alterados são copiados para fitas sempre que um backup total é executado e ainda o tempo, uma vez que os backups totais levam mais tempo para serem executados e podem ser muito demorados.

***Obs.**:* Apesar de se utilizar este tipo de backup, serão identificadas para cada servidor, as áreas destinadas ao processo de backup, sendo anexadas posteriormente estas informações a este documento.

11.6 Modo de Backup

O modo de backup a ser utilizado para o backup de dados é o modo *Offline*. Este modo de backup é realizado quando ninguém estiver tentando acessar os dados. Uma das vantagens em se utilizar este modo de backup é que a operação de backup será mais rápida e também diminui o risco de que os dados possam vir a ser corrompidos durante este processo. A desvantagem é que ninguém poderá acessar as informações durante o processo de backup.

11.7 Mídia Digital de Armazenamento de Dados

O meio de gravação que será utilizado é o meio magnético.

A mídia digital para armazenamento de dados que será utilizada é a Fita DAT que utiliza a tecnologia DDS, por se tratar de uma unidade com grande capacidade de armazenamento de dados.

11.8 Periodicidade e Recover

O backup será executado diariamente, sendo utilizado uma fita para cada dia da semana (segunda a domingo).

A operação de backup será realizada durante a noite em horário ainda a ser definido por meio de agendamento de software.

11.8.1 A rotatividade das fitas será dada da seguinte forma:

Do dia 01 ao dia 15 de cada mês será utilizada uma fita para cada dia, no dia 15 de cada mês será realizado uma cópia total dos arquivos e colocado em uma fita a qual ficará fora das fitas selecionadas para rotatividade quinzenal. Onde a fita do dia 01 será novamente utilizada para gravação dos dados do dia 16, depois a fita do dia 02 para gravação do dia 17 e assim sucessivamente, até chegarmos ao dia 30 de cada mês onde novamente será realizada uma cópia total dos dados em uma outra fita que não faça parte das fitas de rotatividade de backup quinzenal. Desta forma, teremos duas fitas com backup total dos arquivos para cada mês, onde estas fitas só entrarão para rotatividade após 06 meses (rotatividade semestral), onde as fitas do mês de janeiro serão utilizadas para gravação do backup do mês de julho e assim sucessivamente.

- Rotatividade de fitas: são as fitas DAT que serão utilizadas no processo diário de backup as quais serão apagadas e regravadas a cada 15 dias, salvo as 02 fitas de backup total que serão feitas por mês, as quais terão rotatividade a cada 06 meses.

12 SANÇÕES

O não cumprimento das Políticas de Segurança da Informação contidas neste documento, implica em falta grave podendo a PREFEITURA DE PARNAMIRIM impor sanções e penas aos que violarem o aqui previsto relativo ao uso de computadores e redes, cabendo ao GCTI a análise das ocorrências. A determinação das sanções, será de acordo com o Estatuto do Servidor Público e/ou processo civil ou criminal.

13 ACESSO FÍSICO AS ÁREAS SEGURAS

Todos os equipamentos e demais ativos que compõem a infraestrutura computacional da PMP são armazenados em áreas seguras, acessíveis apenas por usuários autorizados.

A PMP adota uma série de controles para proteção, como paredes, portas, janelas, trancas, cadeados, sistemas de vigilância e alarme.

É importante que todos os usuários conheçam e sigam as seguintes regras de acesso a áreas seguras:

1. Nunca tente obter acesso a uma área segura a menos que esteja devidamente autorizado;
2. Sempre se identifique e registre o seu acesso a áreas seguras;
3. Caso esteja acompanhando um terceiro, nunca permita que este fique sozinho em uma área segura;
4. Não utilize dispositivos para registros audiovisuais como câmeras, webcams, câmera de celulares, gravadores e filmadoras sem estar devidamente autorizado.
5. Caso precise remover algum hardware ou outro ativo de uma área segura, sempre faça um registro incluindo data, horário e motivo da retirada.
6. Caso você identifique alguma irregularidade, comunique imediatamente ao GCTI.

14 CÂMERAS DE FILMAGEM

Em suas dependências, a PMP faz uso, quando necessário, de câmeras de filmagem com o objetivo de manter a proteção física dos usuários e ativos.

De forma a guardar a dignidade humana de seus funcionários, a PMP não permite a instalação de câmeras em áreas como lavabos ou banheiros.

Todas as imagens gravadas serão mantidas em áreas seguras, acessíveis apenas a usuários autorizados para fins institucionais da PMP. Desta forma, não constituem invasão a privacidade dos seus servidores.

15 ACESSO DE TERCEIROS

Durante a realização de atividades profissionais, pode ser necessário o apoio de terceiros, como prestadores de serviços, parceiros comerciais ou estagiários.

O acesso de terceiros a recursos da PMP deve ser realizado de forma controlada, garantindo que informações sensíveis não venham a ser expostas a pessoas ou organizações não autorizadas.

Neste caso, é importante que todos os usuários conheçam as seguintes regras:

1. Para que um terceiro possa obter acesso a recursos da PMP, é necessário a assinatura de termos de uso e de confidencialidade, onde o terceiro deverá concordar em seguir níveis de serviço e de segurança adotados pela organização;

2. Terceiros deverão estar sempre acompanhados por um colaborador encarregado de supervisionar o acesso as dependências e recursos computacionais da PMP;

3. O acesso de terceiros deverá ser imediatamente revogado após a conclusão do serviço contratado;

4. Nunca forneça credenciais ou permita que um terceiro obtenha acesso a serviços da PMP sem autorização apropriada.

16 HELP DESK

A PMP disponibiliza aos seus usuários um ponto único de contato para solicitação de serviços de suporte e esclarecimento de quaisquer dúvidas relacionadas aos recursos computacionais da organização.

O HELP DESK está disponível através do telefone (84) **3644-8333** ou pelo uso do E-mail **helpdesk@parnamiirm.rn.gov.br**

Lembre-se: O HELP DESK é a maneira mais rápida para obter suporte e solucionar qualquer dúvida relacionada ao uso de recursos computacionais da PMP. Evite outras fontes, tais como colegas de trabalho, terceiros ou familiares.

17 PROPRIEDADE INTELECTUAL

É de propriedade da PMP, todos os designs, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a PMP.

COLABORE COM O PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

A PMP compreende e estimula a participação de seus usuários na gestão da Segurança da Informação. Envie sugestões, dúvidas e opiniões para o GCTI através do endereço **normasdeti@parnamirim.rn.gov.br**

Caso o usuário não saiba como fazê-lo, deverá solicitar treinamento junto ao GCTI.

Em caso de dúvidas e/ou dificuldades em utilizar os recursos da rede de computadores da Prefeitura, o usuário deverá consultar o CTI.

Parnamirim/RN, 16 de dezembro de 2011

MAURÍCIO MARQUES DOS SANTOS
Prefeito