ÍNDICE

1. CONCEITOS E DEFINIÇÕES

- **Ativos de informação:** os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal;
- **Usuários de TI:** Todos os empregados, prestadores de serviço, estagiários ou pessoas que no exercício de suas atividades na empresa tenham acesso as informações e aos ativos de informação.
- **Dispositivos móveis:** equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets.
- **Trabalho remoto:** Possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc da infraestrutura interna, sem estar fisicamente na EMAP, utilizando-se de sistema de informação do tipo VPN.

Observar demais definições na Política de Segurança da Informação da EMAP.

2. REFERÊNCIAS LEGAIS E NORMATIVAS

Observar referências legais e normativas na Política de Segurança da Informação da EMAP.

3. OBJETIVO

A política técnica de computação móvel e trabalho remoto faz parte de um

conjunto de documentos que compõem a Política de Segurança da Informação da EMAP. Os detalhes de determinados assuntos contidos nessa política técnica estão regulados em outras políticas técnicas.

- Esta política deve ser lida por todos empregados e prestadores de serviços que atuem com as atividades descritas nela.

Esta política técnica institui regras de segurança a serem seguidas quanto à utilização de dispositivos móveis da EMAP e a execução de trabalhos remotos à infraestrutura interna da EMAP.

4. DIRETRIZES GERAIS

Os dispositivos móveis tratados nessa política técnica são limitados àqueles de propriedade da EMAP ou fornecidos por empresas contratadas pela EMAP.

As utilizações dos dispositivos móveis pelos empregados da EMAP devem ser realizadas somente quando for de estrito interesse da empresa.

A EMAP consente na utilização cuidadosa dos dispositivos móveis para interesses particulares, desde que não exceda os limites da razoabilidade, ética e bom senso.

- É vetado o uso dos dispositivos móveis da EMAP para acesso a conteúdos de jogos, crimes, rádios, TVs, apostas, eróticos, pornográficos e blogs.

Todos os dispositivos móveis da EMAP devem ser inventariados.

O trabalho remoto à infraestrutura da EMAP deve ser realizado somente quando for de estrito interesse da empresa.

- O acesso remoto a infraestrutura interna da EMAP, uma vez concedido, será controlado e monitorado.

4.1. Dispositivos móveis

Os dispositivos móveis da EMAP devem ser configurados de modo a garantir a proteção e segurança adequadas as informações que estão armazenadas neles.

- Deve ser realizada configurações que garantam a proteção e sigilo dos dados armazenados nos dispositivos móveis em casos de extravio.

A concessão aos empregados da EMAP para portar os dispositivos móveis está condicionada a autorização formal do superior imediato do setor.

- A distribuição somente será concedida pela GETIN caso haja disponibilidade do dispositivo móvel.
- A GETIN deve informar ao empregado as responsabilidades e os cuidados de uso com o dispositivo concedido no momento da retirada do dispositivo móvel.

A entrada e a saída dos dispositivos móveis das instalações da EMAP devem ser identificadas de acordo com os procedimentos operacionais do setor de segurança patrimonial.

Nos dispositivos móveis da EMAP devem conter instalações apenas de sistemas de informações homologados pela GETIN.

- Usuários de TI que não possuem perfil de administração, devem ser impedidos de instalar sistemas de informação nos dispositivos móveis.
- A necessidade de utilização de sistemas de informações diferente dos fornecidos no dispositivo móvel deve ser encaminhado para a GETIN para análise, avaliação e instalação no dispositivo.

Os dispositivos móveis devem ter suas sessões bloqueadas quando o empregado se afastar do equipamento.

Os dispositivos móveis devem ser desligados e acondicionados corretamente em local onde somente o empregado tenha acesso, quando não estiver em uso.

Os dispositivos móveis deverão ser configurados para executar automaticamente uma varredura com antivírus quando do uso de mídias de armazenamento removíveis.

O empregado deve providenciar a transferência das informações da EMAP manipuladas no dispositivo móvel para os servidores da infraestrutura interna, quando necessário.

- Quando da devolução do dispositivo móvel à GETIN, as informações da EMAP devem ser transferidas definitivamente para os servidores da infraestrutura interna.
- O empregado deve apagar todas as informações pessoais que tenha sido armazenada no dispositivo móvel. Em caso de dúvidas, deve solicitar auxílio aa GETIN.

A GETIN da EMAP não se responsabiliza por nenhuma informação pessoal do usuário contida/deixada nos dispositivos móveis.

4.2. Trabalho remoto

O trabalho remoto à infraestrutura interna da EMAP deve ser realizado por meio de canal criptografado.

- Quando possível, a GETIN deve observar as recomendações de criptografia descritas pela ICP-Brasil para realização do acesso.

A GETIN deve orientar os empregados que realizam trabalho remoto quanto aos requisitos de segurança da informação para realização de tal atividade.

O trabalho remoto à infraestrutura interna deve ser realizado somente a partir de ativos de informações e dispositivos móveis habilitados para tal atividade.

- Os ativos de informações e dispositivos móveis utilizados em residências para o trabalho remoto devem conter mecanismos de proteção contra vírus e sistemas de informações maliciosos bem como controle de acesso.

O trabalho remoto à infraestrutura interna deve ser solicitado, formalizado e justificado pelo superior imediato do empregado aa GETIN.

- O setor solicitante deve informar o prazo de validade para a realização do trabalho remoto e as permissões, ativos de informação e sistemas de informação que deverá ter acesso remotamente.
- A liberação de acesso remoto deve será precedida de análise quanto a sua viabilidade pela GETIN que poderá ou não autorizar o acesso.

Todos os acessos de trabalhos remotos devem ser monitorados com seus respectivos logs.

- Os logs devem ter no mínimo data e hora, serviço utilizado, usuário de acesso e informações específicas que facilitem o rastreamento e a auditoria posterior.
- A GETIN poderá realizar auditoria nos logs e permissões de trabalho remoto a qualquer tempo ou conforme necessidade.

A GETIN deverá orientar os empregados autorizados a respeito da operação de trabalho remoto.

A GETIN deve providenciar a instalação dos sistemas de informações necessários para o trabalho remoto.

4.3. Disposições Finais

- Os casos não previstos nesta política técnica deverão ser encaminhados para a GETIN.
- Os casos omissos serão resolvidos pela GETIN.

5. REVISÕES

Não se aplica