INDÍCE

1. CONCEITOS E DEFINIÇÕES

- **Algoritmo:** função matemática utilizada na cifração e na decifração de informações restritas.
- **Algoritmo Assimétrico:** função matemática que utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.
- **Algoritmo Simétrico:** função matemática que utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações restritas.
- **Certificado Digital:** funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas por um gestor, associa uma entidade (pessoa ou sistema informatizado) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.
- **Cifração:** ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la.
- **Chave ou chave criptográfica:** valor que trabalha com um algoritmo criptográfico para cifração ou decifração.

- **Controle criptográfico:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.
- **Credenciamento:** processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.
- **Decifração:** ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.
- **ICP-Brasil:** Instituído pela Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual de pessoas físicas, pessoas jurídicas ou sistemas informatizados associados a pessoas físicas ou jurídicas.
- **VPN:** Virtual Private Network. Rede privada construída sobre uma infraestrutura de rede pública, com recursos para proteção dos dados transmitidos contra interceptações e capturas.

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 controles criptográficos 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 sobre o uso efetivo e adequado de criptografia na proteção da informação.

4. DIRETRIZES GERAIS

- Os controles criptográficos serão usados para assegurar, dentre outros:
    - A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;
    - O não-repúdio: provar a ocorrência de um evento ou ação alegados e suas entidades originárias, de forma a resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e do envolvimento das entidades no evento.
    - A autenticação: confirmar a identidade de usuários ou de sistemas automatizados.
- A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação
- É proibida a implantação de controles criptográficos não homologados pelo setor de TI da EMAP ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade.
- O tráfego de login/senha de rede, durante a autenticação de usuários, e de informações classificadas como restritas entre as camadas envolvidas nos sistemas ou serviços disponibilizados pela EMAP deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.
- Quando permitido por norma de tratamento da informação, documentos restritos que forem armazenados em dispositivos móveis (notebook, tablet, smartphone etc.) ou em mídias removíveis (cd, dvd, pen drive etc.) devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

4.1. Certificados Digitais de Uso Interno

- Além dos certificados digitais válidos na ICP-BRASIL, poderão ser utilizados certificados digitais assinados por autoridade certificadora raiz criada pelo setor de TI da EMAP, desde que para identificar servidor/aplicação (computador ou

software) de uso interno ou para substituir credenciais de usuários baseadas em login e senha e utilizadas apenas nos sistemas internos da EMAP.

- Respeitados os limites da lei, poderá ser aprovado o uso de certificados digitais em dispositivos de rede visando interceptar com o objetivo de filtragem conteúdo previamente cifrado e que possa ser considerado inadequado, impróprio ou malicioso.

4.2. Responsabilidades

- Compete ao setor de TI da EMAP:
    - Criar e manter procedimentos de certificação e fazer o controle da Infraestrutura de Chaves Públicas da EMAP e dos certificados digitais de uso interno;
    - Homologar os recursos criptográficos para uso na EMAP;
    - Gerenciar o credenciamento de usuários de recursos criptográficos;
    - Criar, distribuir, recuperar e destruir chaves de uso em recursos criptográficos;
    - Elaborar e divulgar procedimentos para recuperação de informações cifradas, no caso de chaves criptográficas perdidas, comprometidas ou danificadas;
- Compete aos proprietários e custodiantes de ativos de informação:
    - Aplicar adequadamente os recursos criptográficos identificados para a proteção da informação sobre sua custódia, em conformidade com as determinações dessa política;

4.3. Disposições Finais

- Os casos não previstos nesta política técnica deverão ser encaminhados para o setor de TI.
- Os casos omissos serão resolvidos pelo setor de TI.

5. REVISÕES

Não se aplica.