NSI-010 – Uso de Recursos Criptográficos

1. OBJETIVOS

1.1. Estabelecer regras para o uso efetivo e adequado da Criptografia na proteção da informação no âmbito do Tribunal Regional Eleitoral da Bahia.

2. APLICABILIDADE

2.1. Este documento aplica-se aos magistrados, membros do Ministério Público, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço e colaboradores do TRE/BA.

3. MOTIVAÇÕES

3.1. Necessidade de proteção com recurso criptográfico de toda informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente, por qualquer meio eletrônico.

3.2. Resguardar o sigilo das informações que o Tribunal produz e custodia no exercício de suas competências.

4. REFERÊNCIAS NORMATIVAS

4.1. Norma ABNT NBR ISO/IEC 27002:2013, no Objetivo de Controle 10.1.1, quanto à política para uso de controles criptográficos;

4.2. Norma Complementar nº 09/IN01/DSIC/GSIPR, revisão 02, de 14/07/2014, sobre o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

5. CONCEITOS E DEFINIÇÕES

5.1. Algoritmo: função matemática utilizada na proteção de informações restritas, podendo ser:

a) Assimétrico: quando utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.

b) Simétrico: quando utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações restritas.

5.2. Ativo de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também as pessoas que a eles têm acesso;

5.3. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

5.4. 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;

5.5. Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem compreensível, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

5.6. Chave ou chave criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

5.7. Controle criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

5.8. Credencial: permissões, concedidas por gestor competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

5.9. 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;

5.10. Custodiante de ativo de informação: refere-se a qualquer indivíduo ou unidade da organização que tenha a responsabilidade formal de proteger um ou mais ativos de informação. Ele é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelos proprietários dos ativos de informação;

5.11. Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

5.12. Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

5.13. ICP-Brasil: Instituido 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;

5.14. Informação restrita: toda a informação que deva ser mantida em sigilo por tempo determinado, com acesso restrito a um grupo credenciado de pessoas que tenham necessidade de conhecê-la, conforme determinado por Lei, norma de classificação da informação e procedimentos de tratamento da informação;

5.15. Login de rede: código utilizado para identificação de um usuário da rede de computadores;

5.16. Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

5.17. Proprietário de ativo de informação: refere-se à parte interessada da unidade da organização, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

5.18. Recurso criptográfico: mesmo que controle criptográfico;

5.19. Senha de rede: informação secreta, de uso individual, utilizada para confirmar (autenticar) a identidade de um usuário da rede de computadores;

5.20. Usuário: pessoa que obteve autorização para acesso a Ativos de Informação do TRE/BA mediante a assinatura de Termo de Responsabilidade;

5.21. VPN: *Virtual Private Network*. Rede privada construída sobre uma infraestrutura de rede pública (comumente Internet), com recursos para proteção dos dados transmitidos contra interceptações e capturas.

6. REGRAS GERAIS

6.1. Os controles criptográficos serão usados para assegurar, dentre outros:

a) 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;

b) 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.

c) a autenticação: confirmar a identidade de usuários ou de sistemas automatizados.

6.2. A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pela unidade gestora de riscos, ou pelo Comitê de Segurança da Informação, ou quando prevista em normativo específico.

6.3. 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.

6.4. Uma tabela relacionando os controles criptográficos, seus parâmetros e sua aplicação na proteção de informações classificadas, será mantida e comunicada aos proprietários e custodiantes de ativos de informação.

6.5. É proibida a implantação de controles criptográficos não homologados pelo TRE-BA ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade.

6.6. 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 pelo TRE-BA, deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

6.7. 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.

7. CERTIFICADOS DIGITAIS DE USO INTERNO

7.1. Além dos certificados digitais válidos na ICP-BRASIL, poderão ser utilizados certificados digitais assinados por autoridade certificadora raiz criada pelo TRE-BA, 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 do Tribunal.

7.2. Respeitados os limites da lei, poderá ser aprovado o uso de certificados digitais em dispositivos de rede visando a interceptar conteúdo previamente cifrado e considerado inadequado, impróprio ou malicioso.

8. RESPONSABILIDADES

8.1. Compete ao Comitê de Segurança da Informação:

I - Deliberar sobre os seguintes procedimentos elaborados e mantidos pela área de TIC do Tribunal:

a) procedimentos de certificação digital da Infraestrutura de Chaves Públicas do TREBA;

b) procedimentos de recuperação de informações cifradas, no caso de chaves criptográficas perdidas, comprometidas ou danificadas;

II - Aprovar e dar ampla publicidade sobre o uso de certificados digitais em dispositivos de rede visando à filtragem de conteúdo cifrado, conforme item 7.2;

8.2. Compete à área de TIC do Tribunal:

I - criar e manter procedimentos de certificação e fazer o controle da Infraestrutura de Chaves Públicas do TRE-BA e dos certificados digitais de uso interno;

II - homologar os recursos criptográficos para uso no TRE-BA;

III - gerenciar o credenciamento de usuários de recursos criptográficos;

IV - criar, distribuir, recuperar e destruir chaves de uso em recursos criptográficos;

V - elaborar e divulgar procedimentos para recuperação de informações cifradas, no caso de chaves criptográficas perdidas, comprometidas ou danificadas;

VI – manter e comunicar aos interessados a tabela indicada no item 6.4.

VII - prover os recursos técnicos e de pessoal necessários para implementar a Infraestrutura de Chaves Públicas do TRE-BA em conformidade com os procedimentos indicados nos itens. 8.1 e 8.2;

8.3. Compete aos proprietários e custodiantes de ativos de informação:

I - aplicar adequadamente os recursos criptográficos identificados para a proteção da informação sob sua custódia, em conformidade com as determinações desta norma;

II - propor ao Comitê de Segurança da Informação, com justificativa devidamente fundamentada, o uso de certificados digitais em dispositivos de rede visando à filtragem de conteúdo cifrado.

9. DISPOSIÇÕES FINAIS

9.1. A área de TIC terá o prazo de **180 (cento e oitenta) dias** para:

I - Elaborar os procedimentos descritos no inciso I do item 8.2;

II - Homologar os recursos criptográficos para uso no TRE-BA e elaborar a tabela descrita no item 6.4;

9.2. Esta norma deverá ser revisada anualmente ou em menor tempo, se necessário, motivadamente por qualquer interessado.