ANEXO IX
NORMA DE GESTÃO DE CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução nº 27/2013-GP	
PORTARIA nº 97/2019-GP	

Versionamento:

Versão:	1.0
Data:	02/05/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	24/07/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de gestão de criptografia e gerenciamento de chaves complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para garantir o acesso aos ativos Tecnologia da Informação e Comunicação (TIC) ou Sistemas de Informação do Poder Judiciário do Estado do Maranhão (PJMA) com níveis adequados de proteção.

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação, estabelecendo regras sobre o uso efetivo e adequado de criptografia na proteção da informação.

2. OBJETIVO

Assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade das informações de acordo com os requisitos de segurança da informação da organização, levando em consideração os requisitos legais, estatutários, regulamentares e contratuais relacionados à criptografia.

3. DIRETRIZES

É vedada a implantação de controles criptográficos não homologados pelo Poder Judiciário do Estado do Maranhão. Os controles criptográficos serão usados para assegurar:

I - a confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transmissão eletrônica;

II - o não-repúdio: provar a ocorrência de evento ou ação alegados e suas entidades participativas originárias, de forma a resolver disputas sobre a ocorrência ou não de evento ou ação e do envolvimento ou não destas entidades;

III - 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.

Os computadores de mesa e dispositivos móveis (notebooks) dos(as) desembargadores(as), juízes(as), diretores(as) e/ou presidente contendo dados confidenciais deverão ser criptografados por ferramenta disponibilizada ou autorizada pela DIA, podendo optar pela criptografia a nível de disco, pasta ou arquivo.

Os dispositivos de armazenamento removíveis (pendrives e discos rígidos externos, etc.), de uso exclusivamente corporativo, dos(as) usuários(as) contendo dados confidenciais deverão ser criptografados por ferramenta disponibilizada ou autorizada pela DIA, devendo optar pela criptografia a nível de dispositivo.

Os dados sensíveis disponíveis em servidores de rede, sistemas e bancos de dados poderão ser criptografados, após a devida avaliação da DIA.

A segurança dos dados que trafegam na rede corporativa ou na internet, como credenciais de acesso e informações sensíveis, deverão utilizar mecanismos de criptografia, tais como: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).

4. CERTIFICADOS DIGITAIS

Os certificados digitais utilizados no âmbito do Poder Judiciário do Estado do Maranhão serão adquiridos de autoridade certificadora credenciada pela ICP-Brasil, para identificar servidores de rede e sistemas de uso interno, para substituir credenciais de acesso de usuários(as) baseadas em login e senha utilizadas nos sistemas administrativos ou judiciais ou para assinar documentos eletrônicos, bem como documentos reproduzidos em meio eletrônico gerados no PJMA.

Os certificados digitais e os suportes criptográficos (tokens) serão cedidos aos(às) usuários(as) que necessitarem utilizar a assinatura digital em razão do exercício das atribuições do cargo ou função pública que ocuparem.

O certificado digital é de uso pessoal e intransferível, cabendo ao(à) usuário(a) zelar pela confidencialidade da senha, bem como pela guarda e pela conservação do suporte criptográfico (token), sob pena de responsabilidades cíveis, penais ou administrativas cabíveis, assegurado o contraditório e a ampla defesa.

Para emissão e uso do certificado digital, os(as) usuários(as) do PJMA deverão observar a PORTARIA-GP - 972019 ou posterior que a substitua e a Resolução nº 272013-GP ou posterior que a substitua.

5. GERENCIAMENTO DE CHAVES

O gerenciamento de chaves do PJMA deverá garantir a confidencialidade, integridade e disponibilidade das chaves criptográficas, além de proteger as chaves contra acesso não autorizado, perda, roubo ou comprometimento, garantindo a conformidade com as leis e regulamentações aplicáveis.

O PJMA deverá dispor de um gerador de chaves criptográficas seguro e confiável e designar uma equipe responsável pelo gerenciamento das chaves criptográficas, bem como controle de acesso adequado para restringir o acesso a estas chaves.

A realização de cópias de segurança (backup) das chaves criptográficas deverá ser realizada de forma regular e segura. Garantindo que as cópias de segurança estejam armazenadas em um local separado do armazenamento principal, devendo ser testado regularmente a restauração das chaves a partir das cópias de segurança para garantir a sua integridade. Para recuperação das chaves criptográficas, em caso de perda ou comprometimento, a DIA adotará procedimento específico.

O PJMA deverá manter um registro das chaves geradas e distribuídas para fins de auditoria e possível responsabilização dos(as) usuários(as) autorizados(as) pela DIA.

6. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

6.1 Usuários(as)

Além do disposto na Resolução GP nº 31/2015 ou posterior que a substitua, compete ao(à) usuário(a):

I - estar de posse do certificado digital para o desempenho de atividades profissionais que requeiram o uso deste;

II - solicitar à autoridade certificadora, de acordo com procedimentos definidos para esse fim, a imediata revogação do certificado em caso de inutilização, observando as situações dispostas na Resolução GP nº 27/2013 ou posterior que a substitua;

III - alterar imediatamente a senha de acesso do certificado digital em caso de suspeita de seu conhecimento por pessoa não autorizada;

IV - observar as diretrizes de complexidade e tamanho definidas para elaboração de senhas, dispostas na norma de controle de acesso e gestão de identidade, para criação de senha do certificado digital;

V - manter o suporte criptográfico (token) em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor e/ou umidade excessivos e outras condições ambientais que representem risco à integridade das mesmas;

VI - solicitar o fornecimento de novo suporte criptográfico (token) ou certificado digital nos casos de inutilização, revogação ou expiração da validade do certificado, observando as situações dispostas na Resolução GP nº 27/2013 ou posterior que a substitua;

VII - verificar periodicamente a data de validade do certificado digital e solicitar tempestivamente a emissão de um novo, conforme orientações expedidas para esse fim;

VIII - devolver em boas condições o suporte criptográfico (token) anteriormente cedido em caso de desligamento do quadro de pessoal do PJMA.

Em caso de perda, roubo ou furto do suporte criptográfico (token), o(a) usuário(a) deverá procurar a ajuda das autoridades policiais registrando boletim de ocorrência e em seguida comunicar, via DIGIDOC, a Diretoria de Informática e Automação para que possam ser tomadas as medidas cabíveis.

6.2 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - realizar a gestão dos certificados digitais e suportes criptográficos (tokens) utilizados no PJMA;

II - adequar a infraestrutura de TIC para uso dos certificados digitais;

III - elaborar e divulgar padrões de compatibilidade dos certificados digitais e dos respectivos suportes criptográficos utilizados no PJMA;

IV - desenvolver em sua área de atuação novas aplicações, ou atualizar as existentes, que requeiram a utilização de certificados digitais;

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

VI - tomar medidas administrativas a respeito dos suportes criptográficos (tokens) que tenham sido objetos de perda, roubo ou furto, reportando, no que couber, as Diretorias Administrativa e/ou a de Segurança Institucional e Gabinete Militar.

6.3 Diretoria Administrativa

Compete à Diretoria Administrativa:

I - realizar acompanhamento administrativo junto a DIA a respeito dos suportes criptográficos (tokens) que tenham sido objetos de perda, roubo ou furto.

6.4 Diretoria de Segurança Institucional e Gabinete Militar

Compete à Diretoria de Segurança Institucional e Gabinete Militar:

I - fornecer apoio técnico, por meio de sistema de segurança eletrônica e outros recursos disponíveis, para investigações em andamento de possíveis ilícitos relacionados aos suportes criptográficos (tokens) nas dependências do PJMA.

7. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

8. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

9. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.