PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO

Institui norma para uso de recursos criptográficos na proteção da informação, no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta do Processo Administrativo nº 14787/2015,

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO o controle "10.1.1 Política para o uso de controles criptográficos" da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação),

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui normas para uso efetivo e adequado de recursos criptográficos na proteção da informação.

Parágrafo único. Aplica-se o disposto nesta Portaria às informações sensíveis ou críticas e aos agentes envolvidos na disponibilização e no uso de recursos criptográficos, no âmbito do Tribunal Regional do Trabalho da 18ª Região (TRT18).

Art. 2º Para os fins desta Portaria, consideram-se as definições constantes do art. 2º da Resolução Administrativa TRT18 nº 145/2019 e as seguintes:

I – algoritmo assimétrico: função matemática que utiliza chaves

criptográficas distintas para cifração e decifração de informações;

II – algoritmo simétrico: função matemática que utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações;

III – 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 as pessoas que a eles têm acesso;

IV – certificado digital: documento virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos como a web. Trata-se de documento eletrônico, gerado e assinado por uma terceira parte confiável, denominada 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;

V – cifração: ato de cifrar com recurso criptográfico para substituir sinais claros de linguagem por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

VI – chave ou chave criptográfica: parâmetro utilizado com um algoritmo criptográfico para cifração ou decifração;

VII – credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a informação de autenticação e a definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

VIII – 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 gestores de ativos;

IX – decifração: ato de decifrar com recurso criptográfico para reverter processo de cifração original;

X – 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;

XI – informação sensível: toda a informação que possa causar dano a pessoas ou organizações caso revelada fora do grupo autorizado de indivíduos que tenham necessidade de conhecê-la, conforme determinado por lei ou regulamentação, a exemplo da RA nº 129/2016, que regulamenta a Lei de Acesso à Informação no âmbito do TRT da 18ª Região;

XII – informação crítica: informação imprescindível para a continuidade das operações do Tribunal nos momentos de crise provocados por incidentes graves ou desastres, conforme identificada pelo processo de Gestão de Continuidade do Negócio;

XIII – 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;

XIV – recurso criptográfico: sistema, programa, processo ou equipamento que, isoladamente ou em rede, utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XV – senha de rede: informação secreta, de uso individual, utilizada para confirmar (autenticar) a identidade de um usuário da rede de computadores.

Art. 3º Os recursos criptográficos serão usados para assegurar, dentre outros:

I – o sigilo, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;

II – 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;

III – a autenticação: confirmar a identidade de usuários ou de sistemas automatizados.

Art. 4º A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de recurso 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.

Art. 5º Uma tabela relacionando os recursos criptográficos, seus parâmetros e sua aplicação na proteção de informações sensíveis ou críticas, conforme definidas pelas áreas de negócio, será mantida e comunicada aos

gestores e custodiantes de ativos de informação.

Art. 6º É proibida a implantação de recursos criptográficos não homologados pelo TRT18 ou utilizá-los de forma distinta aos procedimentos.

Art. 7º O tráfego de senha de rede durante a autenticação de usuários e de informações sensíveis entre as camadas envolvidas nos sistemas ou serviços disponibilizados pelo TRT18 deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

Art. 8º Quando permitido por norma de tratamento da informação, documentos sensíveis 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.

CAPÍTULO III
DOS CERTIFICADOS DIGITAIS DE USO INTERNO

Art. 9º. Poderão ser utilizados os seguintes tipos de certificados digitais:

I - válidos na ICP-BRASIL;

II - contratados de empresas reconhecidas e que não façam parte da cadeia da ICP-BRASIL para identificar servidor/aplicação (computador ou software);

III - assinados por autoridade certificadora raiz criada pelo TRT18, desde que se destinem a identificar usuários em sistemas internos do Tribunal ou a identificar servidor/aplicação também de uso interno.

Art. 10. Observados os limites da lei, poderá ser aprovado o uso de certificados digitais em dispositivos de rede visando à filtragem de conteúdo previamente cifrado e que possa ser considerado inadequado, impróprio ou malicioso.

CAPÍTULO IV
DAS COMPETÊNCIAS

Art. 11. Compete à Comissão de Segurança da Informação:

I – deliberar sobre os seguintes procedimentos elaborados e mantidos pela unidade de Tecnologia da Informação e Comunicação:

a) procedimentos de certificação digital da Infraestrutura de Chaves Públicas do TRT18;

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 art. 13, inciso II.

Art. 12. Compete à unidade de Tecnologia da Informação e Comunicação:

I – criar e manter procedimentos de certificação e fazer o controle da Infraestrutura de Chaves Públicas do TRT18 e dos certificados digitais de uso interno, quando optar pela disponibilização e uso desse recurso criptográfico;

II – homologar os recursos criptográficos para uso no TRT18;

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, quando geradas por ferramentas homologadas pelo TRT18 que comportem tais funcionalidades;

VI – manter e publicar na intranet a tabela indicada no art. 5º;

VII – prover os recursos técnicos e pessoal necessários para implementar a Infraestrutura de Chaves Públicas do TRT18 em conformidade com os procedimentos indicados no art. 11, inciso I.

Art. 13. Compete aos gestores e custodiantes de ativos de informação:

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

II – propor à Comissão de Segurança da Informação, quando detectada a necessidade e apresentada justificativa devidamente fundamentada, o uso de certificados digitais em dispositivos de rede visando à filtragem de conteúdo cifrado.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 14. Esta Portaria entra em vigor na data de sua publicação,

revogando-se a Portaria GP/NGTIC n° 006/2016.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
PAULO PIMENTA
Desembargador-Presidente
TRT da 18ª Região

Goiânia, 17 de julho de 2020.
[assinado eletronicamente]

PAULO SÉRGIO PIMENTA

DESEMB. PRES. DE TRIBUNAL