Tribunal Regional do Trabalho da 18ª Região Comitê de Segurança da Informação Secretaria de Tecnologia da Informação e Comunicações Núcleo de Segurança da Informação	Código: **NO05**
	Revisão: **00**
	Vigência: **Publicação no DEJT**
	Classificação: **PÚBLICO**
	Ato normativo: **Portaria GP/DG nº 318/2015**

USO DE CONTROLES CRIPTOGRÁFICOS

1 OBJETIVO

Estabelecer regras sobre o uso efetivo e adequado de criptografia na proteção da informação.

2 APLICAÇÃO

Esta norma de segurança da informação se aplica no âmbito do Tribunal Regional do Trabalho da 18ª Região (TRT18).

3 REFERÊNCIA NORMATIVA

3.1 Portaria TRT18 GP/DG nº 76/2014 e anexo "**PO01**", que aprova as diretrizes da Política de Segurança da Informação e Comunicações do TRT18.

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

3.3 Objetivo de Controle 10.1.1 da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação).

4 DEFINIÇÕES

Para efeito desta política, serão adotadas as definições descritas nesta seção e no documento PO01.

4.1 Algoritmo: função matemática utilizada na cifração e na decifração de informações restritas.

4.2 Algorítmo Assimétrico: função matemática que utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.

4.3 Algorítmo Simétrico: função matemática que utiliza a mesma chave

criptográfica tanto para a cifração quanto para a decifração de informações restritas.

4.4 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.

4.5 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.

4.6 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 contém os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

4.7 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.

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

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

4.10 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

4.11 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.

4.12 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.

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

4.14 Gestão de Riscos de Segurança da Informação e Comunicações: 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.

4.15 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.

4.16 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.

4.17 Login de rede: código utilizado para identificar de um usuário da rede de computadores.

4.18 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.

4.19 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.

4.20 Recurso criptográfico: mesmo que controle criptográfico.

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

4.22 Usuário: pessoa que obteve autorização para acesso a Ativos de Informação do TRT18 mediante a assinatura de Termo de Responsabilidade.

4.23 VPN: Virtual Private Network. Rede privada construída sobre uma infraestrutura de rede pública, com recursos para proteção dos dados transmitidos contra

interceptações e capturas.

5 REGRAS GERAIS

5.1 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.

5.2 A escolha dos tipos, da qualidade e da força de algorítimos, 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.

5.3 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;

5.4 É proibida a implantação de controles criptográficos não homologados pelo TRT18 ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade.

5.5 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 TRT18 deve ser protegido com o uso de mecanismos de criptografia como *HTTPS*, *SSL*, *TLS* e *VPN.*

5.6 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.

6 CERTIFICADOS DIGITAIS DE USO INTERNO

6.1 Além dos certificados digitais válidos na ICP-BRASIL, poderão ser utilizados

certificados digitais assinados por autoridade certificadora raiz criada pelo TRT18, 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.

6.2 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.

7 RESPONSABILIDADES

7.1 Compete ao Comitê de Segurança da Informação:

7.1.1 Deliberar sobre os seguintes procedimentos elaborados e mantidos pelo Núcleo de Segurança da Informação:

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;

7.1.2 Aprovar e dar ampla publicidade sobre o uso de certificados digitais em dispositivos de rede visando à filtragem de conteúdo cifrado, conforme item 6.2;

7.2 Compete ao Núcleo de Segurança da Informação:

a) criar e manter procedimentos de certificação e fazer o controle da Infraestrutura de Chaves Públicas do TRT18 e dos certificados digitais de uso interno;
b) homologar os recursos criptográficos para uso no TRT18;
c) gerenciar o credenciamento de usuários de recursos criptográficos;
d) criar, distribuir, recuperar e destruir chaves de uso em recursos criptográficos;
e) elaborar e divulgar procedimentos para recuperação de informações cifradas, no caso de chaves criptográficas perdidas, comprometidas ou danificadas;
f) Manter e comunicar aos interessados a tabela indicada no item 5.3.

7.3 Compete à Secretaria de Tecnologia da Informação e Comunicações

a) prover os recursos técnicos e de pessoal necessários para implementar a Infraestrutura de Chaves Públicas do TRT18 em conformidade com os procedimentos elaborados pelo Núcleo de Segurança da Informação;
b) apoiar o NSI na homologação de recursos criptográficos para uso no TRT18;

7.4 Compete aos proprietários e custodiantes de ativos de informação:

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

b) 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.

8 DISPOSIÇÕES GERAIS

8.1 O NSI terá o prazo de 180 dias para:

a) Elaborar os procedimentos descritos no item 7.1.1;

b) Homologar os recursos criptográficos para uso no TRT18 e elaborar a tabela descrita no item 5.3;

8.2 Esta norma deverá ser revisada a cada dois anos.

A S S I N A T U R A S

[Documento assinado eletronicamente por]

MARIA CÉLIA DE SENE BAVARESCO

CHEFE DE NUCLEO FC-6

LEANDRO CÂNDIDO OLIVEIRA

COORDENAD CJ-02

HUMBERTO MAGALHÃES AYRES

DIR DE SECRET-CJ-3

JOSÉ EVERSON NOGUEIRA REIS

COORDENAD CJ-02

CÉLVORA MARRA MOREIRA R. DE OLIVEIRA

ASSIST JUR FC-5

Goiânia, 14 de julho de 2015.