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

Aprova a revisão 1.0 da norma NO09, que dispõe sobre controles administrativos e tecnológicos para a proteção da informação sigilosa e da informação pessoal, definidas nos termos da Resolução Administrativa TRT 18ª Região Nº 129/2016.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais e tendo em vista o que consta do Processo Administrativo Nº 908/2018;

Considerando o Parágrafo Único do Art. 38 da Resolução Administrativa TRT 18ª Nº 129/2016;

Considerando a conclusão das atividades do Grupo de Trabalho de Classificação da Informação, instituído pela PORTARIA TRT 18ª GP/SGJ Nº 942, documentadas no Processo Administrativo Nº 6492/2018;

Considerando as diretrizes da Política de Segurança da Informação e Comunicação do TRT18, constantes do documento PO01,

R E S O L V E:

Art. 1º Aprovar a revisão 1.0 da norma Proteção da Informação Sigilosa e da Informação Pessoal – NO09, conforme Anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria TRT 18ª GP/NGTIC Nº 90/2018.

Art. 3º Publique-se no Diário Eletrônico da Justiça do Trabalho.

PAULO PIMENTA
Desembargador-Presidente
TRT da 18ª Região

PROTEÇÃO DA INFORMAÇÃO SIGILOSA E DA INFORMAÇÃO PESSOAL

1 OBJETIVO

Dispõe sobre controles administrativos e tecnológicos para proteção da informação sigilosa e da informação pessoal, definidas nos termos da Resolução Administrativa TRT 18ª Região nº 129/2016.

2 APLICAÇÃO

Este documento aplica-se no âmbito do TRT 18ª Região (TRT18).

3 REFERÊNCIA NORMATIVA

3.1 Política de Segurança da Informação do TRT18, constantes do documento PO01.

3.2 Resolução Administrativa TRT18 nº 129/2016 (RA129), que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, no âmbito do Tribunal Regional do Trabalho da 18ª Região.

4 DEFINIÇÕES

Para efeito desta norma, são adotadas as definições descritas nesta seção e nos documentos PO01 e RA129.

4.1 **Princípio do menor privilégio**: visa permitir o acesso à informação no nível mínimo necessário para a necessidade de conhecer.

4.2 **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.

4.3 **Custodiante da informação**: qualquer pessoa que detém a posse, mesmo

que transitória, de informação produzida ou recebida pelo Tribunal.

4.4 **Grupo de Acesso**: pessoas autorizadas pela autoridade classificadora (ou pela autoridade superior) para obtenção de acesso à informação sigilosa ou informação pessoal.

4.5 **Gestor da informação**: Unidade do TRT que, no exercício de suas competências, produz informações ou obtém, de fonte externa ao Tribunal, informações de propriedade de pessoa física ou jurídica.

4.6 **Computação em Nuvem**: modelo computacional que, independentemente da localização, permite acesso por demanda a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

5 DISPOSIÇÕES PRELIMINARES

5.1 Às informações classificadas em grau de sigilo (reservado, secreto e ultrassecreto), informações abrangidas por demais hipóteses legais de sigilo e informações pessoais, nos termos da RA129, é obrigatória a aplicação dos controles administrativos e tecnológicos descritos nos itens 7 e 9 deste normativo, a menos que seja tecnicamente inviável.

5.2 Aplicam-se aos documentos preparatórios, nos termos da RA129, os mesmos controles de proteção aplicáveis ao documento sigiloso que deles possa originar

5.3 A decisão de não aplicação dos controles de que trata o item 5.1 deve ser justificada e documentada, sendo registrada a concordância do gestor da informação.

5.4 O gestor da informação pode decidir, no caso concreto, com base no risco de acesso ou uso indevido da informação e devidamente motivado, que os controles administrativos e tecnológicos aplicados a uma dada informação sejam mais restritivos do que os descritos nos itens 7 e 9, desde que compatíveis com a natureza sigilosa ou pessoal.

5.5 Qualquer duplicação de informações armazenadas em bases de dados – a exemplo daquelas necessárias aos ambientes de desenvolvimento, teste e homologação – é considerada cópia da informação e deve respeitar o disposto neste normativo.

6 RESPONSABILIDADES

6.1 É responsabilidade do custodiante da informação aplicar-lhe controles administrativos e tecnológicos compatíveis com a natureza sigilosa ou pessoal.

6.2 Cabe ao gestor da informação sugerir à autoridade classificadora (ou autoridade superior) a composição dos grupos de acesso às informações sob sua gestão, respeitando o princípio do menor privilégio e a necessidade de conhecer.

6.3 Compete à unidade gestora de solução de TI, ouvidos os gestores da informação, definir funcionalidades que permitam implementar os controles administrativos e tecnológicos descritos neste normativo para as informações recebidas, produzidas ou tratadas pela solução de TI sob sua gestão.

6.4 A ausência ou a insuficiência injustificada de controles administrativos e tecnológicos compatíveis com a natureza sigilosa ou pessoal da informação configura incidente de segurança da informação, a ser reportado à Comissão de Segurança da Informação – CSegInfo – por quem dele tiver conhecimento.

6.5 Divulgar ou permitir a divulgação, bem como acessar ou permitir acesso indevido à informação protegida por sigilo, constitui conduta ilícita que enseja responsabilização nas esferas administrativa, civil e penal, nos termos da legislação em vigor, a exemplo do disposto nos §§ 1º e 2º do art. 32 da Lei nº 12.527, de 2011.

7 TRATAMENTO DE INFORMAÇÕES EM NUVEM

7.1 A informação classificada como secreta ou ultrassecreta não poderá ser tratada em ambiente de computação em nuvem.

7.2 As demais informações sigilosas e pessoais somente poderão ser tratadas em ambiente de computação em nuvem homologado pela STI.

8 DISPOSIÇÕES GERAIS

8.1 Esta norma deverá ser revisada em intervalos de até dois anos.

9 CONTROLES ADMINISTRATIVOS E TECNOLÓGICOS

Fase	Informação	Controles
Produção	Ultrassecreta Secreta Reservada	*(c3) Classificar a informação ou propor classificação à autoridade competente para a informação que não tenha sido previamente classificada. (c4) Rotular a informação de maneira apropriada ao meio em que é apresentada. (c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação.
	Ultrassecreta	(c5) Obrigatoriamente nas instalações do TRT18. (c7) Obrigatoriamente em ambiente não compartilhado com pessoas estranhas ao grupo de acesso.
	Secreta	(c8) Preferencialmente nas instalações do TRT18. (c9) Preferencialmente em ambiente não compartilhado com pessoas estranhas ao grupo de acesso.
	Ultrassecreta Secreta	(c6) Obrigatoriamente com equipamento corporativo.
	Reservada Pessoal **Outras	(c10) Nas instalações do TRT18 ou fora de suas dependências. (c11) Permitido o uso de equipamento corporativo ou particular. (c12) No caso de uso de equipamento particular, atender ao disposto no documento "requisitos mínimos de segurança para equipamentos pessoais" definidos pela STI.
	Ultrassecreta Secreta Reservada Pessoal Outras	(c34) RA129 Art. 43 – O responsável pela preparação ou reprodução de documentos sigilosos deverá providenciar a eliminação de provas ou de qualquer outro recurso que possam dar origem a cópia não autorizada do todo ou de parte.
Recebimento	Ultrassecreta Secreta Reservada	(c41) Verificar o grau de sigilo da informação. (c42) Respeitar a classificação atribuída na origem. Caso a classificação da informação não seja aderente à LAI, a autoridade competente pela classificação da informação deve realizar a conversão para a classificação correspondente no TRT. (c4) Rotular a informação de maneira apropriada ao meio em que é apresentada.
	Pessoal Outras	(c46) Verificar se a informação é pessoal ou se é abrangida por outra hipótese legal de sigilo.
Armazenamento	Ultrassecreta Secreta Reservada Pessoal Outras	(c22) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em local/recipiente protegido por chave e observar as regras definidas no grupo de acesso habilitado.
	Ultrassecreta Secreta	(c23) O armazenamento de documentos/arquivos eletrônicos deve ser criptografado e observar as regras definidas no grupo de acesso habilitado.
	Reservada Pessoal Outras	(c25) O armazenamento de documentos/arquivos eletrônicos em servidor ou solução corporativos de TIC do Tribunal deve observar as regras definidas no grupo de acesso habilitado. (c26) O armazenamento de documentos/arquivos eletrônicos em qualquer outro meio ou local (ex.: pendrive, nuvem homologada pelo TRT, computadores pessoais, etc) deve ser criptografado.

*(cxx): código do controle, associado ao processo de gestão de riscos que o derivou. **Outras: informações abrangidas por outras hipóteses legais de sigilo.

Fase	Informação	Controles
Acesso	Ultrassecreta Secreta Reservada Pessoal Outras	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora (ou autoridade superior). (c14) Permitido a pessoa com necessidade de conhecer a informação. (c15) Permitido a pessoa legalmente autorizada. (c16) Para acessar a informação é preciso identificação e autenticação. (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação.
	Ultrassecreta Secreta	(c6) Obrigatoriamente com equipamento corporativo.
	Reservada Pessoal Outras	(c11) Permitido o uso de equipamento corporativo ou particular. (c12) No caso de uso de equipamento particular, atender ao disposto no documento “requisitos mínimos de segurança para equipamentos pessoais” definidos pela STI.
	Ultrassecreta	(c18) Permitido apenas a partir da rede interna.
	Secreta	(c19) Permitido apenas a partir da rede interna ou desktop virtual, no caso de acesso a documentos eletrônicos.
	Pessoal	(c30) RA129 Art. 35 § 1º Permitido a agentes públicos e à pessoa a que se referir as informações. (c31) RA129 Art. 35 § 2º Permitido a terceiros mediante consentimento expresso da pessoa a que se referir a informação, observado § 5º. (c32) RA129 Art. 35 § 3º O acesso às informações pessoais por terceiros será condicionado à assinatura do termo de compromisso anexo à Resolução. (c33) RA129 Art. 35 § 7º As informações e documentos identificados como pessoais somente poderão ser fornecidos pessoalmente, com a identificação do requerente.
	Outras	(c27) RA 129 Art. 1º, § 3º O acesso aos processos judiciais em segredo de justiça se dará consoante a legislação processual vigente.
Cópia	Ultrassecreta Secreta Reservada Pessoal Outras	(c34) RA129 Art. 43 – O responsável pela preparação ou reprodução de documentos sigilosos deverá providenciar a eliminação de provas ou de qualquer outro recurso que possam dar origem a cópia não autorizada do todo ou de parte. (c43) Manter o mesmo rótulo, ser for o caso, e aplicar os mesmos controles da informação original no caso de cópia ou impressão. (c35) RA129 Art. 44 – Sempre que a preparação, a impressão ou, se for o caso, a reprodução de informações e de documentos sigilosos, forem efetuadas em tipografias, impressoras, oficinas gráficas ou similares, essas operações deverão ser acompanhadas por agente público credenciado, que será responsável pela garantia do sigilo durante a confecção do documento.
Transporte	Ultrassecreta Secreta Reservada Pessoal Outras	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia.
	Ultrassecreta Secreta Reservada	(c2) No caso de transporte externo ou interno de papel ou de mídias não criptografáveis, deve-se utilizar envelope interno lacrado cuja violação seja detectável, e envelope externo sem nenhuma indicação do grau de sigilo ou teor do documento. O envelope interno será expedido mediante relação de remessa, que indicará, necessariamente, remetente, destinatário, número de registro e grau de sigilo do documento.
	Pessoal Outras	(c28) No caso de transporte externo ou interno de papel ou de mídias não criptografáveis, deve-se utilizar envelope.
Descarte	Ultrassecreta Secreta Reservada Pessoal Outras	(c20) Nos casos de substituição de mídia de armazenamento (ex.: HDD/SSD) ou descarte de cópias, documentos/arquivos eletrônicos devem ser excluídos de maneira a impossibilitar sua recuperação, por meio de software para remoção segura. (c21) Nos casos de descarte de cópias, documentos em papel ou armazenados em CD/DVD/BD devem ser destruídos por meio de fragmentadora. (c45) Nos casos de descarte de mídias magnéticas (ex.: cartuchos LTO), as mídias devem ser destruídas ou, alternativamente, os documentos/arquivos eletrônicos devem ser excluídos de maneira a impossibilitar sua recuperação, por meio de software para remoção segura. (c40) RA129 Art. 42 – Decorridos os prazos previstos nas tabelas de temporalidade, as informações e documentos sigilosos de guarda temporária somente poderão ser eliminados após aprovação do Comitê ou Comissão de Gestão Documental.

Goiânia, 6 de setembro de 2019.
[assinado eletronicamente]

PAULO SÉRGIO PIMENTA

DESEMB. PRES. DE TRIBUNAL