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

Aprova a norma Proteção da Informação Classificada – NO09, a qual dispõe sobre controles administrativos e tecnológicos para proteção da informação classificada quanto ao aspecto da confidencialidade, em cada grau de sigilo definido 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,

R E S O L V E:

Art. 1º Aprovar a norma Proteção da Informação Classificada – NO09, a qual dispõe sobre controles administrativos e tecnológicos para proteção da informação classificada quanto ao aspecto da confidencialidade, em cada grau de sigilo definido nos termos da Resolução Administrativa TRT 18ª Região nº 129/2016, conforme Anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

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

PLATON TEIXEIRA DE AZEVEDO FILHO
Desembargador-Presidente

ANEXO

	Tribunal Regional do Trabalho da 18ª Região Comissão de Segurança da Informação Governança Corporativa de TIC	Código: **NO09**
		Revisão: **0.0**
		Vigência: **(DATA DE PUBLICAÇÃO)**
		Classificação: **PÚBLICO**
		Ato normativo: **Portaria TRT 18ª GP/NGTIC Nº ____2018**

PROTEÇÃO DA INFORMAÇÃO CLASSIFICADA

1 OBJETIVO

Dispõe sobre controles administrativos e tecnológicos para proteção da informação classificada quanto ao aspecto da confidencialidade, em cada grau de sigilo definido 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 Diretrizes da 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 classificada.

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.

5 DISPOSIÇÕES PRELIMINARES

5.1 Quanto à confidencialidade, as informações produzidas ou custodiadas pelo Tribunal classificam-se nos graus de confidencialidade público, reservado, secreto, ultrassecreto, pessoal e restrito.

5.2 A cada grau de confidencialidade corresponde um conjunto de controles administrativos e tecnológicos, listados no item 8 deste normativo, compatíveis com os danos potenciais à imagem ou ao negócio do Tribunal, ou a intimidade, vida privada, honra e imagem das pessoas, que o uso ou o acesso não autorizado à informação acarretariam.

5.3 É obrigatória a aplicação dos controles administrativos e tecnológicos descritos no item 8 deste normativo, a menos que seja tecnicamente inviável.

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

5.5 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 no item 8, desde que compatíveis com o grau de confidencialidade.

5.6 Qualquer duplicação de informações armazenadas em bases de dados – a exemplo daquelas necessárias aos ambientes de aceite, teste e desenvolvimento – 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 o grau de confidencialidade a ela atribuído.

6.2 Cabe ao gestor da informação sugerir à autoridade classificadora 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 o grau de confidencialidade 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 DISPOSIÇÕES GERAIS

7.1 Esta norma deverá ser revisada periodicamente, em intervalos de até dois anos.

8 CONTROLES ADMINISTRATIVOS E TECNOLÓGICOS

Informação Ultrassecreta	
Aspectos Gerais	
Descrição	Informação imprescindível à segurança da sociedade ou do Estado, nos termos do art. 23 da Resolução Administrativa nº 129/2016.
Prazo máximo de restrição de acesso	25 anos, em consonância com a Resolução Administrativa nº 129/2016.
Competência para a classificação	Presidente do Tribunal. É vedada a delegação da competência de classificação. (em consonância com a Resolução Administrativa nº 129/2016)
Controles administrativos e tecnológicos	
Produção	(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; (c5) Obrigatoriamente nas instalações do TRT18; (c6) Obrigatoriamente com equipamento corporativo; (c7) Obrigatoriamente em ambiente não compartilhado com pessoas estranhas ao grupo de acesso; (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;

	(c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação;
Recebimento	(c41) Verificar o grau de confidencialidade 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;
Armazenamento	(c22) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em cofre; (c23) O armazenamento de documentos/arquivos eletrônicos deve ser criptografado e observar as regras definidas no grupo de acesso habilitado;
Acesso	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora; (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; (c18) Permitido apenas a partir da rede interna; (c6) Obrigatoriamente com equipamento corporativo; (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação;
Cópia	(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 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	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia; (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;
Descarte	(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;

Informação Secreta	
Aspectos Gerais	
Descrição	Informação imprescindível à segurança da sociedade ou do Estado, nos termos do art. 23 da Resolução Administrativa nº 129/2016.
Prazo máximo de restrição de acesso	15 anos, em consonância com a Resolução Administrativa nº 129/2016.
Competência para a classificação*	Presidente do Tribunal, Membros do Tribunal Pleno. É vedada a delegação da competência de classificação. (em consonância com a Resolução Administrativa nº 129/2016)
Controles administrativos e tecnológicos	
Produção	(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;

	(c8) Preferencialmente nas instalações do TRT18; (c6) Obrigatoriamente com equipamento corporativo; (c9) Preferencialmente em ambiente não compartilhado com pessoas estranhas ao grupo de acesso; (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; (c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação;
Recebimento	(c41) Verificar o grau de confidencialidade 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;
Armazenamento	(c24) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em armário ou gaveta com chave; (c23) O armazenamento de documentos/arquivos eletrônicos deve ser criptografado e observar as regras definidas no grupo de acesso habilitado;
Acesso	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora; (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; (c19) Permitido apenas a partir da rede interna ou desktop virtual, no caso de acesso a documentos eletrônicos; (c6) Obrigatoriamente com equipamento corporativo; (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação;
Cópia	(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 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	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia; (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;
Descarte	(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;

Informação Reservada	
Aspectos Gerais	
Descrição	Informação imprescindível à segurança da sociedade ou do Estado, nos termos do art. 23 da Resolução Administrativa nº 129/2016.
Prazo máximo de restrição de acesso	5 anos, em consonância com a Resolução Administrativa nº 129/2016.

Competência para a classificação	Presidente do Tribunal, Membros do Tribunal Pleno, Juízes no exercício da titularidade de Vara do Trabalho, Secretário-Geral da Presidência, Diretor-Geral do Tribunal, Secretário-Geral Judiciário. (em consonância com a Resolução Administrativa nº 129/2016)
Controles administrativos e tecnológicos	
Produção	(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; (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, assegurar que o antivírus esteja atualizado e que estejam aplicadas as atualizações de segurança no sistema operacional e aplicativos utilizados; (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; (c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação;
Recebimento	(c41) Verificar o grau de confidencialidade 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;
Armazenamento	(c24) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em armário ou gaveta com chave; (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, computadores pessoais, etc) deve ser criptografado;
Acesso	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora; (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; (c11) Permitido o uso de equipamento corporativo ou particular; (c12) No caso de uso de equipamento particular, assegurar que o antivírus esteja atualizado e que estejam aplicadas as atualizações de segurança no sistema operacional e aplicativos utilizados; (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação;
Cópia	(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 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	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia; (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;
Descarte	(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;

Informação Pessoal	
Aspectos Gerais	
Descrição	Informação que diz respeito à intimidade, vida privada, honra e imagem da pessoa, bem como às liberdades e garantias individuais.
Prazo máximo de restrição de acesso	100 anos, em consonância com a Resolução Administrativa nº 129/2016.
Competência para a classificação	Presidente do Tribunal, Membros do Tribunal Pleno, Juízes no exercício da titularidade de Vara do Trabalho, Secretário-Geral da Presidência, Diretor-Geral do Tribunal, Secretário-Geral Judiciário, Diretores de Unidades Administrativas. (em consonância com a Resolução Administrativa nº 129/2016)
Controles administrativos e tecnológicos	
Produção	(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; (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, assegurar que o antivírus esteja atualizado e que estejam aplicadas as atualizações de segurança no sistema operacional e aplicativos utilizados; (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; (c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação;
Recebimento	(c41) Verificar o grau de confidencialidade 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;
Armazenamento	(c24) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em armário ou gaveta com chave; (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, computadores pessoais, etc) deve ser criptografado;
Acesso	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora; (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; (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; (c11) Permitido o uso de equipamento corporativo ou particular; (c12) No caso de uso de equipamento particular, assegurar que o antivírus esteja atualizado e que estejam aplicadas as atualizações de segurança no sistema operacional e aplicativos utilizados; (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação;
Cópia	(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 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	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia; (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;
Descarte	(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;

Informação Restrita	
Aspectos Gerais	
Descrição	Informação enquadrada nas hipóteses legais de sigilo, tais como as de natureza fiscal, bancária, a relacionada a operações e serviços no mercado de capitais, a protegida por sigilo comercial, profissional, aquela protegida por segredo de justiça, bem como os documentos preparatórios.
Prazo máximo de restrição de acesso	Obedece ao prazo estabelecido na legislação específica instituidora do sigilo.
Competência para a classificação	Presidente do Tribunal, Membros do Tribunal Pleno, Juízes no exercício da titularidade de Vara do Trabalho, Secretário-Geral da Presidência, Diretor-Geral do Tribunal, Secretário-Geral Judiciário, Diretores de Unidades Administrativas, ressalvados os processos judiciais, os quais serão classificados pela autoridade judicial competente. (em consonância com a Resolução Administrativa nº 129/2016)
Controles administrativos e tecnológicos	
Produção	(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; (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, assegurar que o antivírus esteja atualizado e que estejam aplicadas as atualizações de segurança no sistema operacional e aplicativos utilizados; (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; (c44) Deve ser incluída advertência sobre restrição de acesso, exceto quando seja tecnicamente inviável para o meio de armazenamento da informação;
Recebimento	(c41) Verificar o grau de confidencialidade 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;
Armazenamento	(c24) Documentos em papel ou mídias recebidas de terceiros não criptografadas devem ser armazenados em armário ou gaveta com chave; (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, computadores pessoais, etc) deve ser criptografado;
Acesso	(c13) Permitido ao grupo de acesso definido pela autoridade classificadora; (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; (c11) Permitido o uso de equipamento corporativo ou particular; (c12) No caso de uso de equipamento particular, assegurar que o antivírus esteja atualizado e que estejam aplicadas as

	atualizações de segurança no sistema operacional e aplicativos utilizados; (c17) Necessária manutenção de histórico de acesso (log), independente do meio em que esteja a informação; (c27) RA 129 Art. 1º, § 3º O acesso aos processos judiciais em segredo de justiça se dará consoante a legislação processual vigente;
Cópia	(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 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	(c1) O transporte externo ou interno, exceto quando inviável tecnicamente, deve ser feito em meio eletrônico e obrigatoriamente adotando criptografia; (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;
Descarte	(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, 23 de janeiro de 2018.
[assinado eletronicamente]

PLATON TEIXEIRA DE AZEVEDO FILHO
DES. FEDERAL DO TRABALHO