PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

PORTARIA PRESI Nº 757 DE 28 DE JULHO DE 2016

Estabelece a Política de Controle de Ativos de Tecnologia da Informação do Tribunal Regional do Trabalho da 8ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO a dependência crescente dos sistemas de informação nas atividades judiciais e administrativas da Justiça do Trabalho no Pará e Amapá;

CONSIDERANDO a necessidade de garantir a segurança das informações armazenadas nos servidores do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a necessidade de gerenciar os dados a fim de manter a completude, a precisão, a disponibilidade e a proteção das informações;

CONSIDERANDO que a perda de informações eletrônicas podem significar graves dificuldades administrativas e de prestação jurisdicional ocasionando a paralisação de atividades essenciais do Tribunal;

CONSIDERANDO a secção 11 da norma ABNT-NBR 27.002/2013, que estabelece diretrizes para definição de Controles de Acesso lógico e físico aos recursos computacionais, com o intuito de proteger o negócio contra perda de dados.

R E S O L V E,

Art. 1º Regulamentar a política de controle de ativos de Tecnologia da Informação, no âmbito do Tribunal Regional do Trabalho da 8ª Região (TRT8), com o objetivo de estabelecer controles de segurança, resguardando e gerenciando o acesso aos ativos de Tecnologia da Informação.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2º Esta Portaria aplica-se a toda Justiça do Trabalho da 8ª Região e faz parte de um conjunto de normas que atendem a Política de Segurança da Informação deste Tribunal.

Art. 3º Para o disposto nesse ato, considera-se:

I - Ativos da informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do Tribunal, assim como também os locais onde se encontram esses dispositivos, Gestão de Pessoas que a eles têm acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

II - Classificação: atribuição, pela autoridade competente, de grau de sigilo a dados, informações, documentos, materiais, áreas ou instalações da instituição;

III - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso às informações;

IV - Criticidade: é o nível de dependência da organização em relação ao ativo, caso ela precise dele durante uma crise. A criticidade está diretamente relacionada ao tempo máximo aceitável da paralisação de um serviço ou processo associado ao negócio e pontua o quanto essa paralisação será crítica para a organização;

V - Custodiante: aquele que, de alguma forma, zela pelo armazenamento e preservação de informações que estão sob sua custódia para organização e processamento. Deve proteger um ou mais ativos de informação do órgão e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo responsável do ativo de informação;

VI - Mídia de armazenamento: é um dispositivo que guarda informações para posterior utilização. Requer energia elétrica para armazenar e recuperar dados. Para efeitos dessa Portaria as mídias de armazenamento incluem todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, cartões inteligentes, fitas magnéticas, disco rígidos, CDs, DVDs, pen drive, cartões de memória e quaisquer outros meios de armazenamento de dados;

VII - Proprietário da informação: magistrado ou servidor do TRT8 que tenha a guarda das informações produzidas ou que esteja sob responsabilidade do setor onde estão lotados. São responsabilidades do Proprietário da Informação atribuir os níveis de classificação que uma informação requer, reclassificar esta informação quando necessário e autorizar o acesso à informação aos usuários do TRT8;

VIII - Quebra de segurança da informação: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

IX - Rede de telecomunicações: pode ser composta de várias sub-redes, dependendo do tipo de serviço que é provido ao usuário

final. As redes de telecomunicações estão sendo aperfeiçoadas para suportar a transmissão de informações com a introdução de novas tecnologias, tanto do lado dos equipamentos da rede (elementos de rede) quanto dos meios de transmissão (redes de transporte) e dos sistemas de operação para gerenciamento de Redes de Telecomunicações;

X - Relevância: nível de importância que o ativo tem para a organização levando em consideração o negócio. Normalmente o valor do ativo da informação não está nele mesmo, mas no processo de negócio que ele suporta;

XI - Responsável pelo ativo: indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XII - Sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não-autorizada;

XIII - Usuário: magistrado, servidor, prestador de serviço ou fornecedor do TRT8 que obteve autorização do Proprietário da Informação pela área interessada para acesso aos Ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade e/ou pedido de concessão de acesso.

CAPÍTULO II
DO INVENTÁRIO DE ATIVOS DE INFORMAÇÃO

Art. 4º A Secretaria de Tecnologia da Informação (SETIN) do TRT8 deve identificar, inventariar e classificar os ativos de informação.

Art. 5º O escopo do inventário de ativos deve ser restrito àqueles para os quais se pretende gerenciar riscos, não se tratando de um inventário patrimonial que engloba a totalidade dos ativos de Tecnologia de Informação do Tribunal.

§ 1º Os ativos devem ser definidos por meio de critérios que atendam a disponibilidade, integridade, confidencialidade e a autenticidade da informação.

§ 2º O inventário deve cobrir os ativos de valor, cuja indisponibilização, mesmo que parcial, pode afetar significativamente o cumprimento da missão da organização, incluindo ativos de rede, software, hardware, serviços, processos, instalações físicas e, inclusive, os recursos humanos.

Art. 6º O inventário dos ativos deve incluir todas as informações necessárias que permitam a recuperação de um ativo de informação após um incidente de segurança da informação grave ou um

desastre, incluindo os seguintes atributos:

I - tipo;

II - identificação;

III - responsável pelo ativo;

IV - relevância;

V - criticidade;

VI - descrição clara e objetiva;

VII - localização;

VIII - levantamento das interfaces e das interdependências internas e externas do ativo de informação.

CAPÍTULO III
DA CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO

Art. 7º Os ativos de Tecnologia da Informação devem ser classificados de acordo com a informação armazenada, processada, manuseada ou protegida pelo ativo, levando em consideração o seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento, para evitar modificação ou divulgação não autorizada.

§ 1º A classificação deve ficar a cargo do responsável pelo ativo.

§ 2º Deve ser informada a relevância de cada ativo, de acordo com o processo de negócio que o ativo está relacionado. O ativo deve ser enquadrado em uma das seguintes relevâncias:

I - muito baixa: quando o ativo pode afetar uma parte muito pequena e localizada da organização e as perdas serão mínimas;

II - baixa: quando o ativo pode afetar uma parte pequena e localizada da organização e as perdas serão baixas;

III - média: quando o ativo pode afetar parte dos negócios da organização e as perdas serão consideráveis;

IV - alta: quando o ativo pode afetar um ou mais negócios da organização e as perdas serão graves;

V - muito alta: quando o ativo pode afetar toda a organização e as perdas serão extremamente altas.

§ 3º O responsável pelo ativo deve manter atualizada a classificação de acordo com as mudanças de relevância do ativo ao longo do seu ciclo de vida.

Art. 8º Os ativos devem sofrer restrições de acesso para apoiar os requisitos de proteção para cada nível de classificação.

CAPÍTULO IV
DO TRATAMENTO DE ATIVOS DE INFORMAÇÃO E MÍDIAS DE ARMAZENAMENTO

Art. 9º Os ativos de informação e as mídias de armazenamento devem ser guardados e manuseados em um ambiente protegido e de forma segura, de acordo com as especificações do fabricante, seguindo os requisitos de confidencialidade e integridade aplicáveis.

Art. 10. Dados valiosos devem ser copiados em mídias e guardados em cofres separados fisicamente para reduzir riscos de perda ou dano que, por ventura, ocorram nessas mídias.

Art. 11. A SETIN deve garantir a identificação e a rotulação dos ativos de informação e das mídias com dados valiosos.

Art. 12. As mídias e ativos de informação de propriedade do Tribunal devem ter as suas saídas e retornos às dependências do TRT8 registradas e autorizadas formalmente pela Direção da SETIN.

§ 1º A SETIN deve registrar a identidade e a atribuição de qualquer pessoa, física ou jurídica, que seja responsável pela remoção e transporte do ativo ou mídia.

§ 2º O meio de transporte deve ser confiável. A embalagem deve ser suficiente para proteger o conteúdo contra qualquer dano físico, levando em consideração fatores ambientais que possam reduzir a possibilidade de restauração dos dados, como a exposição ao calor, umidade ou campos magnéticos.

§ 3º Mídias contendo informações devem ser protegidas contra o acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

§ 4º É recomendada a utilização de técnicas de criptografia para proteger os dados contidos na mídia quando a integridade ou confidencialidade dos dados forem consideradas importantes. Neste caso as seguintes premissas devem ser atendidas:

I - o processo de encriptação deve ser suficientemente robusto e cobrir o disco por completo;

II - as chaves criptográficas devem ser de um tamanho considerável para resistir a um ataque de força buta;

III - as chaves criptográficas devem ser guardadas em meio seguro, nunca armazenadas no mesmo disco.

§ 5º Quando a informação confidencial não for criptografada na mídia, deve ser garantida a proteção física adicional desta mídia.

Art. 13. No descarte de ativos e mídias, que possuam informações institucionais, devem ser observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação.

§ 1º Os equipamentos devem ser inspecionados para verificar se há dados armazenados nas mídias antes do descarte ou reutilização.

§ 2º Quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável deve ser destruído, caso venha a ser retirado da organização. Mídias com dados valiosos devem passar por um dos dois processos:

I - destruição física através de incineração ou trituração;

II - remoção dos dados ou sobre gravação por meio de técnicas que tornem as informações originais irrecuperáveis.

Art. 14. Equipamentos danificados contendo dados sensíveis devem ser avaliados pela SETIN para determinar se é recomendado que os itens sejam destruídos fisicamente em vez de serem enviados para conserto ou descartados.

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 15. São atribuições do responsável pelo ativo de informação:

I - descrever o ativo de informação;

II - identificar e classificar adequadamente e periodicamente o ativo;

III - ter responsabilidade sobre a manutenção, utilização e segurança do ativo;

IV - identificar e sanar vulnerabilidades que podem afetar o ativo de informação;

V - contribuir na identificação das exigências de segurança da informação e comunicação do ativo de informação;

VI - assegurar que os ativos sejam adequadamente protegidos;

VII - aplicar restrições ao acesso ao ativo, levando em conta a política de controle de acesso;

VIII - comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;

IX - assegurar que as exigências de segurança da informação e comunicações em relação ao ativo estejam sendo cumpridas por meio de monitoramento contínuo;

X - assegurar o armazenamento dos ativos de informação de acordo com as especificações dos fabricantes;

XI - assegurar um adequado tratamento quando o ativo é excluído ou destruído;

XII - garantir que a informações sobre procedimentos e conhecimentos adquiridos em relação ao ativo sejam documentadas e transferidas para a organização.

Art. 16. O responsável pelo ativo de informação pode delegar a um custodiante as tarefas de rotina de operação do ativo, entretanto continuará respondendo pelos incidentes relacionados ao ativo.

Art. 17. O gestor de Segurança da Informação, no âmbito de suas atribuições, é responsável pela coordenação do inventário e mapeamento de ativos de informação visando a Gestão de Riscos de Segurança da Informação. É responsável, também, pela análise quanto aos resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação e, consequentemente, pela proposição de ajustes e de medidas preventivas e proativas perante o Conselho Gestor de Segurança da Informação.

Art. 18. O Tribunal deve viabilizar recursos que proporcionem a proteção dos ativos de informação proporcionais ao seu grau de confidencialidade e de criticidade.

Art. 19. Compete a SETIN implementar as diretrizes estabelecidas e comunicar ao Comitê Gestor de Segurança da Informação as ocorrências de incidentes de segurança relacionados aos ativos de informação.

Art. 20. O custodiante que tiver acesso aos ativos de informação do Tribunal fica sujeito às diretrizes, às normas e aos procedimentos para garantir a segurança da informação, tratados por esta Portaria.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 21. Os casos de acessos indevidos serão tratados pelo Comitê Gestor de Segurança da Informação do TRT8.

Art. 22. Esta Portaria entra em vigor na data de sua publicação no Diário Eletrônico da Justiça do Trabalho.

Publique-se, dê-se ciência e cumpra-se

FRANCISCO SÉRGIO SILVA ROCHA
Presidente