TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS
Palácio da Justiça Rio Tocantins, Praça dos Girassóis, s/nº Centro - Palmas - CEP 77015-007 - Palmas - TO - http://wwa.tjto.jus.br

PORTARIA Nº 3433/2017 - PRESIDÊNCIA/ASPRE, de 26 de junho de 2017

Institui a Política de Segurança da Informação (PSI), no âmbito do Poder Judiciário do Estado do Tocantins e dá outras providências.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS, no uso de suas atribuições legais e regimentais,

CONSIDERANDO os termos da Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o contido na Resolução TJTO nº 22, de 16 de outubro de 2014, Institui Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI) no âmbito do Poder Judiciário do Estado do Tocantins e adota outras providências;

CONSIDERANDO que ao CGSI compete, entre outras atribuições, propor, aprovar e divulgar a Política de Segurança da Informação, bem como de ações que resultem na disseminação da cultura em matéria de segurança;

CONSIDERANDO que a Política de Segurança da Informação (PSI), balizada em disposições legais e princípios e diretrizes institucionais, consiste no conjunto de regras que visam à promoção da segurança da informação;

CONSIDERANDO o disposto no § 1º do art. 2º da Resolução TJTO nº 22, de 2014 e contido no processo SEI nº 16.0.000005260-8,

RESOLVE:

Título I

DISPOSIÇÕES GERAIS

Capítulo I

OBJETIVO E ABRANGÊNCIA

Art. 1º A Política de Segurança da Informação (PSI) do Poder Judiciário do Estado do Tocantins (PJTO), compreende princípios, diretrizes e requisitos com a finalidade de proteger seus ativos de informação e processamento, bem como direitos de propriedade intelectual, englobando aspectos de segurança pessoal, lógica e física, devendo ser observada por todos os usuários na forma desta Portaria e seus anexos.

Capítulo II

PRINCÍPIOS

Art. 2º A Política de Segurança da Informação tem como princípios a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações.

Capítulo III

TERMOS E DEFINIÇÕES

Art. 3º Para os fins da Política de Segurança da Informação entende-se como:

I – usuários: autoridades, servidores e estagiários do PJTO, fornecedores de produtos e serviços, seus prepostos e empregados, representantes de órgãos e entidades, jurisdicionados e visitantes que tenham acesso aos ativos de informação e processamento disponibilizados pelo Tribunal;

II - ativo de informação: patrimônio composto por todos os dados e informações gerados, manipulados ou descartados nos processos envolvendo atividades do PJTO;

III – ativo de processamento: patrimônio composto por todos os elementos de *hardware* e *software* necessários à execução de processos envolvendo atividades do PJTO, tanto produzidos internamente quanto adquiridos;

IV – *hardware*: componente ou conjunto de componentes físicos de um computador ou de seus periféricos;

V – *software*: conjunto de instruções e dados processado pelos computadores, também referenciado como programas, aplicativos ou sistemas;

VI – confidencialidade: garantia de que o acesso ao ativo de informação seja obtido somente por pessoas, entidades ou processos autorizados;

VII – integridade: garantia de que o ativo de informação seja disponibilizado sempre exato e completo;

VIII – autenticidade: garantia de que a origem do dado ou da informação é verdadeira e fidedigna;

IX - disponibilidade: garantia de que os usuários autorizados obtenham acesso aos ativos de informação e processamento, sempre que necessário;

X – termo de responsabilidade: acordo de confidencialidade quanto ao sigilo de informações, dando conhecimento ao usuário da correta utilização dos ativos de informação e processamento do PJTO e das responsabilidades e sanções pelo seu uso indevido;

XI – servidor de rede local: ativo de processamento dedicado ao fornecimento de serviços para a realização das atividades do PJTO.

Título II

DIRETRIZES DE SEGURANÇA

Capítulo I

SEGURANÇA ORGANIZACIONAL

Art. 4º A presidência do Tribunal de Justiça deve estabelecer, na sua estrutura organizacional, área responsável pela gestão da segurança da informação.

Capítulo II

PROPRIEDADE DA INFORMAÇÃO

Art. 5º Todo ativo de informação gerado, adquirido ou custodiado pelo usuário na realização de atividades para o PJTO é considerado de propriedade do Tribunal e deve ser protegido segundo as regras definidas nesta PSI e demais regulamentações em vigor.

§ 1º O Tribunal deve providenciar junto ao fornecedor documentação formal relativa à cessão de direitos sobre o ativo de informação, antes de utilizá-lo.

§ 2º Nos casos de cessão de ativo de informação do Tribunal, o responsável pelo ativo, assessorado pela área jurídica do PJTO deve, se necessário, providenciar documentação formal relativa à cessão de direitos sobre o respectivo ativo.

Capítulo III

GESTÃO DE ATIVOS

Art. 6º Todos os ativos de informação e processamento devem ser inventariados periodicamente e a eles atribuído um responsável.

§ 1º Cada ativo de informação e processamento deve ser classificado, segundo os critérios definidos pelo PJTO, quanto aos aspectos de confidencialidade, integridade e disponibilidade por seu respectivo responsável, observando sua importância para os processos do PJTO, a fim de receberem níveis de proteção adequados.

§ 2º O responsável pelo ativo de informação e processamento, ao classificá-lo, deve considerar o balanceamento entre a classificação a ser atribuída e o custo das medidas de segurança necessárias à sua proteção, podendo, para tanto, recorrer à área do Tribunal responsável pela Gestão da Segurança da Informação para auxiliá-lo na definição.

Art. 7º Os ativos de informação e processamento disponibilizados pelo PJTO devem ser utilizados estritamente dentro do seu propósito.

Parágrafo único. Fica proibido a qualquer usuário o uso desses recursos para fins pessoais (próprios ou de terceiros) ou para promover ações que violem a legislação em vigor e as regulamentações internas ou que prejudiquem a imagem do PJTO.

Art. 8º Os ativos de informação e processamento devem dispor de mecanismos que minimizem os riscos inerentes a problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios de integridade, disponibilidade e confidencialidade das informações.

Capítulo IV

SEGURANÇA EM PESSOAS

Art. 9º A PSI deve ser comunicada e disponibilizada a todos os usuários com a finalidade de divulgar as regras de utilização dos ativos de informação e processamento, bem como as responsabilidades decorrentes, de forma a se obter maior cooperação e efetividade no cumprimento do seu objetivo.

Parágrafo único. Os contratos firmados pelo Tribunal com terceiros devem conter cláusulas que determinem a observância ao cumprimento desta norma.

Art. 10. Os incidentes que possam afetar a segurança dos ativos de informação e processamento devem ser imediatamente reportados à área responsável pela gestão da segurança da informação do PJTO.

Capítulo V

SEGURANÇA FÍSICA E DO AMBIENTE

Art. 11. A área responsável pela gestão da segurança da informação deve avaliar, periodicamente, os riscos de acesso aos ativos de informação e processamento, bem como as instalações físicas do PJTO, de forma a estabelecer perímetros de segurança física para prevenir, além de acesso não autorizado, dano ou perda de informações que comprometam a continuidade das atividades institucionais.

Capítulo VI

GESTÃO DE OPERAÇÕES E COMUNICAÇÕES

Art. 12. A Presidência do Tribunal deve definir procedimentos e responsabilidades pela gestão e operação dos ativos de processamento.

Parágrafo único. O responsável pelo ativo de informação e processamento deve realizar projeções de demandas de uso, com o apoio, se necessário, da área de informática, com o intuito de reduzir sobrecargas que possam provocar paralisações e panes nos processos que suportam os objetivos de negócio do PJTO.

Art. 13. Os ativos de informação em formato eletrônico e processamento devem ser providos de mecanismos de cópia de segurança e recursos de reserva de forma a viabilizar a recuperação das atividades do Tribunal no menor tempo possível.

Art. 14. O uso de ativos de informação e processamento de propriedade do PJTO, fora das instalações do Tribunal, deve obedecer às regulamentações desta PSI e normas específicas a este fim, sem prejuízos das regulamentações para uso interno.

Art. 15. Os ativos de informação em formato eletrônico devem ser armazenados nos servidores de rede local e os não eletrônicos mantidos em local que os salvaguardem adequadamente.

Art. 16. O descarte de ativos de informação do PJTO deve observar as tabelas de temporalidade do órgão e a legislação vigente, as regras definidas nesta PSI, normas e o nível de classificação atribuído a esses ativos.

Capítulo VII

CONTROLE DE ACESSO

Art. 17. O acesso aos ativos de informação e processamento disponibilizado ao usuário deve ser somente o necessário para a realização de suas atividades no Tribunal.

Art. 18. O Tribunal deve estabelecer regras de concessão, controle e direitos de acesso aos ativos de informação, levando-se em consideração a classificação da informação.

§ 1º Ao usuário deve ser disponibilizada de forma pessoal e intransferível identificação de acesso aos ativos de informação e processamento e atribuída responsabilidade por sua guarda e uso.

§ 2º O acesso aos ativos de informação em formato não eletrônico deve guardar, no que couber, as mesmas cautelas dispensadas aos ativos de informação em formato eletrônico.

Art. 19. Os usuários que transitam pelas instalações do PJTO devem portar, de forma visível, identificação de acesso autorizado.

Capítulo VIII

DISPOSIÇÕES FINAIS

GESTÃO DE INCIDENTES E SEGURANÇA DA INFORMAÇÃO

Art. 20. O Tribunal deve adotar procedimentos de gerenciamento de incidentes de segurança, bem como estabelecer controles para identificação e redução de riscos, de forma a limitar as consequências de danos aos ativos de informação e processamento e garantir recuperação rápida, efetiva e ordenada de suas atividades.

Capítulo IX

GESTÃO DE CONTINUIDADE

Art. 21. A área responsável pela gestão da segurança da informação deve elaborar, implantar, revisar e testar periodicamente plano de continuidade do negócio, visando reduzir para um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos ativos de informação e processamento do PJTO.

Capítulo X

MONITORAMENTO

Art. 22. Respeitados os direitos e garantias individuais, bem como a legislação vigente, o uso dos ativos de informação e processamento disponibilizados pelo PJTO é passível de monitoramento e rastreamento.

Capítulo XI

CONFORMIDADE

Art. 23. As regulamentações e procedimentos referentes à segurança dos ativos de informação e processamento devem estar em conformidade com a legislação em vigor.

Capítulo XII

AVALIAÇÃO E REVISÃO

Art. 24. Esta Norma deve ser revisada periodicamente ou na hipótese de fato superveniente que exija ação imediata.

Art. 25. A segurança dos ativos de informação e processamento deve ser analisada por meio de auditoria periódica.

Art. 26. Os casos omissos devem ser encaminhados à área responsável gestão da segurança da informação.

Capítulo XIII

PENALIDADES

Art. 27. O descumprimento desta PSI e demais normas correlatas sujeita o usuário às sanções penais, cíveis e administrativas, no que couber.

Art. 28. Os usuários devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área responsável pela gestão da segurança da informação.

Art. 29. Em caso de quebra de segurança da informação por meio de recursos de informática, a área responsável pela gestão da segurança da informação deve ser imediatamente acionada para adotar as providências necessárias.

Art. 30. Ao infrator desta norma serão aplicadas as sanções cabíveis, conforme previsto na legislação em vigor.

Art. 31. A revisão desta norma deve ocorrer em intervalos planejados, pelo menos anualmente ou sempre que existirem alterações das regras ora editadas.

Art. 32. Os casos omissos devem ser encaminhados à área responsável pela gestão segurança da informação para o devido tratamento.

Art. 33. Compõem a Política de Segurança da Informação neste Tribunal os seguintes documentos e normas, constantes dos Anexos I e II desta Portaria.

I - Manual de Organização de Conceitos

II - Normas Complementares

Art. 34. Esta Portaria entra em vigor na data de sua publicação.

Palmas, 26 de junho de 2017.

ANEXO I

(Portaria nº 3.433, de 26 de junho de 2017)

MANUAL DE ORGANIZAÇÃO DE CONCEITOS

Este manual apresenta os termos e definições utilizados na documentação da Política de Segurança da Informação do Poder Judiciário do Tocantins.

1. Diretoria de Tecnologia da Informação: área responsável por desenvolver e manter os recursos computacionais e de telecomunicações do Poder Judiciário do Tocantins (Resolução TJTO nº 17/2009), competindo-lhe:

1.1. manter a integração e a conectividade dos sistemas, veiculando as informações de todas as áreas informatizadas;

1.2. desenvolver e gerenciar sistemas de computação necessários ao bom funcionamento do Poder Judiciário;

1.3. elaborar Estudos Preliminares e Termos de Referência para os editais de aquisição de equipamentos e suprimentos de informática e telecomunicações;

1.4. gerenciar os serviços de telefonia fixa e móvel;

1.5. manter o bom funcionamento de todo o parque tecnológico;

1.6. propiciar treinamento interno aos usuários dos recursos computacionais disponíveis.

1.7. prover o parque de *hardware* e *software*, prover suporte ao uso de soluções de tecnologia da informação para os usuários, bem como identificar novas demandas.

2. Divisão de Sistema da Informação: responsável pelo desenvolvimento de sistemas e programas computacionais relativos às atividades-fim e meio do Poder Judiciário, bem como à manutenção e à assistência técnica daqueles em funcionamento. (Resolução TJTO nº 17/2009);

3. Divisão de Administração e Segurança de Rede: compete gerenciar redes com formatos em diferentes ambientes de dados, como interfaceamento de sistemas de plataformas e com redes abertas e redes virtuais. (Resolução TJTO nº 17/2009);

4. Divisão de Administração de Banco de Dados: compete a participação em projetos de modelagem de dados, manutenção em objetos de banco de dados, monitoramento e administração das bases de dados corporativas do Poder Judiciário, assim como controle de acesso, instalação lógica e física, implementação de rotinas de segurança, *backup* e recuperação de dados. (Resolução TJTO nº 17/2009);

5. Divisão de Manutenção e Suporte: compete dar suporte aos usuários e manutenção dos computadores e periféricos, no Poder Judiciário do Tocantins. (Resolução TJTO nº 17/2009);

6. Arquivo público: conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias (Lei Federal nº 8.159/91).

7. Acesso: possibilidade de consulta e/ou reprodução aos documentos de arquivo.

8. Alta direção: diretoria executiva e conselho de administração.

9. Ativo: qualquer coisa que tenha valor para a organização.

10. Áreas de segurança: locais onde estão armazenadas ou são manipuladas informações classificadas como confidenciais.

11. *Backup*: cópia de segurança dos arquivos de computador.

12. Classificação: atribuição, pelo classificador, de grau de segurança a dado, informação, documento ou material (Decreto Federal nº 7.845/12).

13. Classificador: agente público responsável por tomar decisões em nome do Tribunal no que diz respeito ao acesso, à classificação, à reclassificação, à desclassificação e a proteção de uma informação ou de um ativo específico.

14. Código móvel: código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário.

15. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

16. Coordenação de Segurança da Informação: grupo responsável por tomar decisões estratégicas de assuntos relacionados com a segurança da informação.

17. Credencial de segurança: certificado concedido por autoridade competente, que habilita uma pessoa a ter acesso a ativo sigiloso ou ambiente físico reservado.

18. Criptografia: técnica utilizada em sistemas de segurança, que transforma, por meio de combinações matemáticas, um arquivo de texto legível em texto codificado, que somente poderá ser decodificado por alguém que tiver a tabela ou fórmula de decriptografia específica para aquele arquivo.

19. Custodiante: agente público ou unidade organizacional responsável pela guarda e transporte de ativos e manutenção das medidas de proteção estabelecidas.

20. Código malicioso: programa de computador (uma parte do código executável) com capacidade de auto-replicação. Da mesma forma que os vírus biológicos, os códigos maliciosos de computador podem se disseminar com rapidez e a sua erradicação normalmente é difícil. Eles podem se anexar a praticamente qualquer tipo de arquivo e se disseminam como arquivos que são copiados e enviados de uma pessoa para outra.

21. Ambiente de Alta Disponibilidade (AAD): compreende as salas seguras, sendo uma principal na sede do Tribunal de Justiça (AAD-TJTO) e uma secundária no Fórum de Palmas (AAD-FORUM).

22. NOC: significa *Network Operations Center* (centro de operação de rede);

23. Desclassificação: cancelamento, por autoridade ou por transcurso de prazo, da classificação, tornando ostensivos dados e informações.

24. Disponibilidade: propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada.

25. Diretoria Executiva: colegiado composto pelos diretores e presidente.

26. Documento: registro de um determinado fato ou evento ocorrido em determinado espaço de tempo, independente do meio em que foi efetuado tal registro.

27. Documento confidencial: documento que contém assunto classificado como sigiloso e que, portanto, requer medidas especiais de acesso.

28. Documento eletrônico (documento digital): trata-se de um documento produzido por aplicativos de computador e armazenado em meio eletrônico como peça de substituição de documento em papel;

29. Equipamentos de interconexão: equipamentos que possibilitam a interligação de dois ou mais recursos de informática, tais como servidores de rede e estações de trabalho.

30. Formato digital: formato no qual a informação é armazenada em mídia digital, por exemplo: *CD-rom, DVD-rom*, fita magnética, disco rígido, fita cartucho, memória *flash*, etc.

31. Comissão: grupo de pessoas formado para estudo de um tema específico.

32. Gestor do processo: colaborador responsável por um determinado processo dentro da organização.

33. Grau de segurança: gradação de segurança atribuída a ativos em decorrência de sua natureza ou conteúdo (Decreto Federal nº 7.845/12).

34. Incidente de segurança: todo e qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança das informações ou dos recursos de informática.

35. Identificação de acesso: conjunto do "nome de usuário" e "senha".

36. Integridade: propriedade de salvaguarda da exatidão e completeza de ativos.

37. Manipulação: manuseio da informação, ou seja, todo tratamento que ela recebe, tais como: cópia, processamento, etc.

38. Medidas de proteção: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais aos ativos (Decreto Federal nº 7.845, de 14 de novembro de 2012).

39. Partes externas: fornecedores, parceiros e clientes que trocam informações com o Tribunal;

40. Plano de Continuidade de Negócios: conjunto de ações que uma Instituição deve tomar para assegurar a continuidade das operações essenciais em caso de falhas nos processos de negócios.

41. Processo crítico: conjunto de ações vitais para o Tribunal que devem ser conduzidas adequadamente, a fim de evitar prejuízos financeiros, comprometimento da sua imagem e até a inviabilização do seu negócio.

42. RAID (Conjunto Redundante de Discos Independentes): é um meio de se criar uma unidade virtual composta por vários discos individuais, com a finalidade de ganhar segurança e desempenho.

43. Reclassificação: alteração da classificação de ativos pelo classificador. (Decreto Federal nº 7.845, de 2012).

44. Recursos de Informática: estações de trabalho, servidores de rede e equipamento de interconexão de propriedade ou custodiados pelo PJTO.

46. Registro (*log*) ou *log* de eventos: arquivo eletrônico com a finalidade de registrar eventos, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado.

47. Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

48. Servidores de rede: recurso de informática com a finalidade de disponibilizar ou gerenciar serviços.

49. Sigilo: garantia de que a informação é acessível somente por pessoas autorizadas (NBR ISO/IEC 27002:2005).

50. Sinistro: qualquer ocorrência que coloque em risco os ativos do PJTO.

51. *Software*: um programa de computador é composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.

52. Tabela de Temporalidade: instrumento arquivístico da gestão documental, resultado da avaliação de documentos. Nele estão dispostos os códigos de classificação, os assuntos, os prazos de guarda e a destinação final da massa documental produzida e recebida pelo Tribunal.

53. Usuário: todo servidor público, estagiário, prestador de serviço ou empresa contratada pelo PJTO que, no exercício de atividades do Tribunal, tenha acesso às informações e aos recursos de informática.

54. Computação em Nuvem: o conceito de computação em nuvem (*cloudcomputing*) refere-se à utilização da memória e das capacidades de armazenamento de computadores e servidores compartilhados e interligados por meio da *internet*.

55. Função *Hash*: mecanismo criptográfico usado para garantir a integridade da informação.

56. Assinatura Digital: aplicação da função *hash* a um documento original, gerando um resumo. Em seguida, utiliza-se a chave privada do Certificado Digital para cifrar o resumo. O resumo cifrado é comumente chamado de Assinatura Digital;

57. Certificado Digital: recurso tecnológico advindo da criptografia moderna. Credencial que possui a função de identificar uma pessoa física ou jurídica, um computador ou um sítio *web* e associar essa identidade a um par de chaves criptográficas, conhecida como criptografia de chave pública, que é composta por chave pública e chave privada;

58. ICP-Brasil: Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), foi instituída pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

59. Autoridades Certificadoras: autoridades que emitem, assinam e revogam Certificados Digitais;

60. *Token* Criptográfico: dispositivo eletrônico que pode ser conectado ao computador, geralmente pela porta USB, que armazena as chaves privadas e certificados digitais e possuem suporte para vários algoritmos de criptografia. É o dispositivo usado para assinar documentos eletrônicos no *e*-Proc/PJTO, Sistema Eletrônico de Informações (SEI), etc.

ANEXO II

(Portaria nº 3.433, de 26 de junho de 2017)

NORMAS COMPLEMENTARES

O Comitê Gestor de Segurança da Informação estrutura as seguintes normas complementares, que tratam especificamente de gestão dos recursos de tecnologia da informação e que devem ser expressamente cumpridas, a saber:

1. Norma-TIC-01: Responsabilidades do Usuário;

2. Norma-TIC-02: Troca de informações com partes externas;

3. Norma-TIC-03: Responsabilidade dos Ativos;

4. Norma-TIC-04: Controle de Acesso do Usuário;

5. Norma-TIC-05: Manuseio de Mídias;

6. Norma-TIC-06: Controle de Acesso ao Conteúdo *Web*.

As Normas Complementares devem ser divulgadas na *internet* e *intranet* para todos os usuários dos recursos internos de tecnologia da informação (membros, servidores, estagiários, colaboradores, terceiros e demais agentes públicos e/ou particulares que, oficialmente executem atividade vinculada à atuação institucional do Poder Judiciário Tocantinense).

Em hipótese alguma será permitido o descumprimento das Normas Complementares sob a alegação de desconhecimento por parte do usuário.

Os casos omissos serão tratados em novas normas, conforme recomendação do Comitê Gestor de Segurança da Informação.

1. **Norma-TIC-01** - Responsabilidades do Usuário: regras a serem seguidas pelos usuários quanto ao uso de senha, de equipamento, mesa e tela limpas.

1.1. Disposições iniciais

1.1.1. O usuário deve conhecer e cumprir a política de segurança da informação do PJTO e a legislação que regulamenta as atividades do servidor público estadual.

1.1.1. A Diretoria de Tecnologia da Informação deve estabelecer um processo de divulgação permanente da sua política de segurança da informação para a conscientização de todos os usuários.

1.2. Uso de recursos de informática e informações

1.2.1. Os usuários devem proteger os recursos de informática e as informações do PJTO contra acesso, modificação, destruição ou divulgação não autorizada.

1.2.2. Utilizar os recursos de informática colocados à sua disposição somente para os fins aos quais eles se destinam.

1.2.3. Não alterar as configurações de qualquer estação de trabalho ou computador portátil. Estas configurações são padronizadas conforme definições da Diretoria de Tecnologia da Informação. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada via sistema de atendimento ao usuário à Divisão de Manutenção e Suporte ao Usuário.

1.2.4. Não abrir o gabinete das estações de trabalho ou computador portátil nem modificar a configuração do *hardware* e *software*, sendo essa uma atribuição exclusiva da Diretoria de Tecnologia da Informação.

1.2.5. Não instalar *software* de sua propriedade ou de terceiros sem prévia homologação e autorização da Diretoria de Tecnologia da Informação.

1.2.6. Desligar a estação de trabalho ou computador portátil correta e diariamente ao final de seu expediente, seguindo os procedimentos do sistema operacional.

1.2.7. As estações de trabalho ou computadores portáteis do PJTO não devem ser ligados em pontos elétricos (tomada) não estabilizadas, bem como ligados em conjunto com outros equipamentos elétricos que não sejam de microinformática.

1.2.8. Arquivos com informações institucionais devem ser armazenados nos Servidores de Arquivos disponibilizados na rede local. Deve-se evitar o armazenamento local nas estações de trabalho ou computador portátil.

1.2.9. Evitar realizar conversas em locais públicos ou sem a reserva adequada sobre assuntos sensíveis do Tribunal, restringindo-se a tratá-los somente em locais que ofereçam a proteção adequada.

1.2.10. Colaborar ativamente na solução de problemas e no aprimoramento dos processos de segurança da informação do PJTO.

1.3. Uso de computadores portáteis

1.3.1. Sempre que não estiverem sendo utilizados, os computadores portáteis do PJTO devem ser guardados em local seguro, onde o responsável, por estes possa garantir que os mesmos não serão utilizados por pessoas não autorizadas.

1.3.2. Computadores portáteis de terceiros ou particulares somente poderão se conectar na Rede Local do PJTO com prévia autorização formal do chefe imediato do usuário e após homologação da Diretoria de Tecnologia da Informação.

1.4. Uso da identificação e senhas de acesso

1.4.1. O usuário somente deve ter acesso às informações e aos recursos de informática após a conclusão do processo de concessão de acesso entre a chefia imediata do usuário, a Diretoria de Gestão de Pessoas e o setor de Infraestrutura.

1.4.2. A cada usuário poderá ser disponibilizada apenas uma identificação de acesso aos recursos de informática, a qual deve ser única, pessoal e intransferível.

1.4.3. O usuário é responsável por todas as ações realizadas com sua identificação de acesso à rede e aos recursos de informática PJTO.

1.4.4. A senha de acesso ao recurso de informática e à rede local do PJTO é pessoal e intransferível, qualificando o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela Diretoria de Tecnologia da Informação.

1.4.5. Os direitos e perfis de acesso seguem as definições da chefia imediata do usuário.

1.4.6. O usuário não deve compartilhar sua senha de acesso com outras pessoas.

1.4.7. O usuário deve trocar sua senha de acesso aos recursos de informática e à rede local na periodicidade e conformeas orientações da Diretoria de Tecnologia da Informação.

1.5. Política de mesa e tela limpa.

1.5.1. Os documentos impressos devem ser tratados de acordo com a definição descrita na norma de classificação, ou seja:

1.5.1.1. Devemser guardados em local seguro e com controle de acesso;

1.5.2. Bloquear o acesso à estação de trabalho ou computador portátil que lhe foi confiado sempre que deles se ausentar.

2. **Norma-TIC-02:** Norma de Segurança da Informação sobre Troca de Informações com Partes Externas: regras de segurança que regem a troca de informações do Tribunal com os prestadores de serviço e empresas contratadas pelo PJTO.

2.1. Disposições iniciais

2.1.1. Para efeitos desta norma, consideramos parte externa os prestadores de serviço, empresas contratadas pelo PJTO, outros Tribunais e convênios estabelecidos com o PJTO que manipulam as informações do Tribunal.

2.1.2. O PJTO deve levantar e documentar os processos, recursos de informática e informações que são manipuladas pela parte externa de forma a implementar controles apropriados de acesso.

2.2. Acordos para a troca de informações e ativos, no âmbito da tecnologia da informação.

2.2.1. A parte externa somente deve ter acesso às informações ou recursos de informática do PJTO após terem ciência das políticas e normas de segurança em vigor no Tribunal.

2.2.2. A troca de informações entre a parte externa e o Tribunal deve ser precedida de um contrato formal ou assinatura do Termo de Confidencialidade que assegure sigilo das informações, responsabilidades, sanções e o cumprimento da Política de Segurança do PJTO pelas partes envolvidas.

2.3. Identificação dos riscos relacionados com as partes externas

2.3.1. Os riscos à segurança da informação oriundos de acesso aos recursos de informática e às informações do Tribunal por partes externas devem ser identificados e controles devem ser implementados antes da concessão de acesso.

2.4. Identificando segurança da informação nos acessos

2.4.1. Os acordos com as partes externas envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de informática e da informação do Tribunal devem cobrir todos os requisitos de segurança da informação relevantes.

2.4.2. A área do PJTO que está solicitando a prestação do serviço por uma parte externa deve, com o apoio da Diretoria de Tecnologia da Informação, identificar previamente e avaliar os riscos à segurança da informação e quais os controles devem ser aplicados quanto aos acessos lógicos e físicos da parte externa aos recursos de informática e às informações do Tribunal.

2.4.3. O acesso lógico da parte contratada aos recursos de informática e às informações do Tribunal deve ser realizado por meio de conta de acesso com o prazo limitado à execução das suas atividades e vigência do contrato.

2.4.4. Essa conta de acesso deve utilizar uma nomenclatura diferenciada das demais contas de acesso, possibilitando uma rápida e fácil identificação.

2.4.5. Os acessos lógicos e físicos da parte externa aos recursos de informática e às informações deve ser o mínimo necessário que a realização dos trabalhos.

2.5. Segurança de mídias em trânsito

2.5.1. A embalagem das mídias deve ser suficiente para proteger o conteúdo contra danos físicos e divulgação indevida, sendo seguidas também as especificações dos fabricantes das mídias em uso.

2.5.2. O PJTO deve adotar controles que impeçam a revelação, interceptação e captação de informações do Tribunal por usuários não autorizados.

2.5.3. Os usuários devem estar cientes da proibição de divulgação, por qualquer meio, de informações confidenciais do Tribunal em locais públicos, em escritórios abertos ou mesmo em reuniões realizadas em sala sem a devida adoção dos requisitos de segurança.

2.5.4. O envio de informações impressas deve ser realizado obedecendo a sua classificação e o seu respectivo tratamento.

2.5.5. A transmissão de arquivos eletrônicos de conteúdo confidencial deve ser realizada de forma segura, por meio de implementações de controles, como por exemplo, criptografia, certificados digitais, autenticações fortes, dentre outros.

2.5.6. A cessão de base de dados ou parte dela deve ser feita por meio de autorização do gestor do negócio e/ou gestor do contrato sobre a informação contida na base de dados.

3. **Norma-TIC-03:** Norma de Segurança da Informação sobre Responsabilidade dos Ativos: regras de segurança referentes aos cuidados e responsabilidades sobre os recursos de informática do PJTO.

3.1. Disposições iniciais

3.1.1. Os recursos de informática devem ser classificados de modo a assegurar a sua proteção e manipulação adequada.

3.1.2. Os recursos de informática que não suportam mais a demanda de serviço, depois de identificados, devem ser catalogados para serem substituídos pela sua obsolescência.

3.1.3. Todos os recursos de informática devem ter um proprietário ou responsável designado.

3.2. Inventário dos recursos de informática

3.2.1. Todos os recursos de informática devem ser inventariados e identificados de forma única.

3.2.2. Os recursos de informática, que não sejam de propriedade do PJTO, devem possuir uma identificação diferenciada dos demais.

3.2.3. O inventário dos recursos de informática deve incluir todas as informações necessárias sobre o recurso de forma a permitir sua recuperação ou substituição eficiente, tais como:

3.2.3.1. tipo do recurso;

3.2.3.2. localização;

3.2.3.3. informações sobre cópia de segurança;

3.2.3.4. informações sobre licenças de *software*;

3.2.3.5. descrição do *hardware* e *software*.

3.2.4. O inventário deve ser realizado quando solicitado pelo Comitê Gestor de Segurança da Informação.

3.3. Configuração dos recursos de informática

3.3.1. Os recursos de informática devem ser configurados seguindo padrões de segurança estabelecidos pela Diretoria de Tecnologia da Informação.

3.3.2. Os serviços desnecessários ao funcionamento dos recursos de informática devem ser desinstalados.

3.3.3. Os recursos de informática devem possuir data e horário sincronizado, obedecendo ao fuso horário de sua localização geográfica.

3.3.4. O compartilhamento de pastas entre os recursos de informática deve preservar a confidencialidade, a integridade e a disponibilidade dos ativos. A Diretoria de Tecnologia da Informação deve fornecer serviço de transferência de arquivos e de compartilhamento de pastas nos servidores de rede.

3.3.5. Os recursos de informática devem ser atualizados sempre que for detectada alguma vulnerabilidade ou quando for implementada uma nova funcionalidade, caso essa nova funcionalidade seja necessária e não traga impactos ao funcionamento do recurso.

3.3.6. Implementações, alterações ou atualizações nos recursos de informática devem ser homologadas antecipadamente pela Diretoria de Tecnologia da Informação.

3.3.7. O processo de homologação dos recursos de informática deve, entre outras atividades, avaliar o impacto da utilização desses na segurança das informações do PJTO.

3.3.8. O processo de homologação dos recursos de informática deve respeitar a política de segurança da informação e demais normas em vigor no Tribunal.

3.3.9. Os recursos de informática devem ser configurados de forma a permitir a liberação do acesso somente após o fornecimento de identificação e autenticação do usuário.

3.3.10.Os recursos de informática devem ter instalados apenas *softwares* homologados no PJTO.

3.3.11. Os *softwares* não homologados devem ser desinstalados dos recursos de informática pela Diretoria de Tecnologia da Informação, devendo esta informar o fato, tanto ao usuário quanto à sua chefia imediata.

3.4. Manutenção dos recursos de informática

3.4.1. A administração e gerenciamento remoto dos recursos de informática, como servidores de rede e equipamentos de interconexão, devem ocorrer por meio de canal criptografado.

3.4.2. Os espaços em disco dos servidores de rede devem ser monitorados, impedindo que as informações armazenadas e processadas por esses equipamentos sejam afetadas.

3.4.3. Os recursos de informática não devem ser ligados em pontos elétricos (tomadas) não estabilizadas, bem como ligados em conjunto com outros equipamentos elétricos que não sejam de informática.

3.4.4. O manuseio dos recursos de informática deve ser feito de forma a preservar sua integridade física e lógica, respeitando-se as recomendações de conservação e uso do fabricante.

3.4.5. As manutenções corretivas ou preventivas e falhas ocorridas nos recursos de informática devem ser registradas.

3.4.6. As correções de falhas e manutenções corretivas devem priorizar os recursos de informática que se encontrem indisponíveis e sejam de maior relevância às atividades do PJTO.

4. **Norma-TIC-04:** Norma de Segurança da Informação sobre o Controle de Acesso do Usuário: regras de controle de acesso dos usuários às informações e à rede do PJTO.

4.1. Disposições iniciais

4.1.1. O usuário deve conhecer e cumprir a Política de Segurança da Informação do PJTO e a legislação que regulamenta as atividades do PJTO.

4.1.2. A Diretoria de Tecnologia da Informação deve estabelecer um processo de divulgação permanente da sua Política de Segurança da Informação para a conscientização de todos os usuários.

4.2. Registro de usuário

4.2.1. As chefias de cada divisão da Diretoria de Tecnologia da Informação devem definir o perfil de acesso que cada usuário terá às informações e recursos de informática do PJTO.

4.2.2. O usuário somente deve ter acesso às informações e aos recursos de informática após a conclusão do processo de concessão de acesso entre a chefia imediata do usuário, a Diretoria de Gestão de Pessoas e a Diretoria de Tecnologia da Informação.

4.2.3. A cada usuário poderá ser disponibilizada apenas uma identificação de acesso aos recursos de informática, a qual deve ser única, pessoal e intransferível.

4.2.4. O usuário é responsável por todas as ações realizadas com sua identificação de acesso à rede e aos recursos de informática PJTO.

4.2.5. Os usuários responsáveis pela administração dos recursos de informática devem possuir um perfil de usuário com privilégios administrativos.

4.3. Gerenciamento de privilégios

4.3.1. O Chefe imediato deverá informar todas as inclusões e alterações de privilégios para a Diretoria de Tecnologia da Informação.

4.3.2 A Diretoria de Gestão de Pessoas deverá informar/notificar todas as nomeações e mudanças como desligamento e movimentação de pessoas para que a Diretoria de Tecnologia da Informação possa implementar procedimentos de concessões do acesso dos usuários versus o respectivo perfil, para que os acessos não mais necessários sejam cancelados.

4.3.3. Os usuários somente deverão ter acesso às informações e aos recursos de informática necessários para a realização das respectivas atividades.

4.3.4. A Diretoria de Tecnologia da Informação deve implementar mecanismos de registros das ações realizadas pelos usuários no manuseio das informações e dos recursos de informática.

4.4. Gerenciamento da identificação e senha dos Usuários

4.4.1. Os recursos de informática do PJTO devem ser configurados de forma a solicitarem que o Usuário troque sua senha de acesso periodicamente;

4.4.2. Os recursos de informática do PJTO devem ser configurados para registrar, em arquivo de eventos (*logs*), as ações praticadas pelos respectivos usuários.

4.4.3. O PJTO deve implementar procedimentos que comprovem a propriedade do usuário no ato de uma solicitação de alteração da senha.

4.4.4. O usuário deve alterar imediatamente sua senha de identificação de acesso à rede do PJTO caso suspeite de um possível vazamento e comunicar o fato ao setor de Segurança da Informação por meio de registro na Divisão de Manutenção e Suporte Técnico, para que sejam tomadas as providências necessárias.

4.4.5. Em casos de suspeita de violação da senha do usuário, os arquivos de registros de eventos (*logs*) devem ser retidos para análise.

4.4.6. A Diretoria de Tecnologia da Informação deve implementar mecanismos de controle e criptografia nas bases de dados que contenham as informações das identificações e senhas dos Usuários.

5. **Norma-TIC-05:** Norma de Segurança da Informação que trata do Manuseio de Mídias: regras de proteção que visam prevenir danos aos ativos e interrupções das atividades do PJTO.

5.1. Disposições iniciais

5.1.1. Para efeito desta norma, considera-se que mídias sejam controladas e fisicamente protegidas, procedimentos operacionais apropriados sejam estabelecidos para proteger documentos, mídias magnéticas e computadores (fitas, discos), dados de entrada e saída e documentação.

5.2. Gerenciamento de mídias removíveis

5.2.1. Os servidores e equipamentos de comunicação que processem ou transmitam informações corporativas devem possuir cópia de segurança das suas configurações e dos seus dados.

5.2.2. Cabe a cada responsável da Diretoria de Tecnologia da Informação estabelecer periodicidade mínima da cópia de segurança dos dados e tempo de retenção das mídias custodiadas pela última.

5.2.3. Mídias magnéticas que não possuem uso frequente devem ter suas informações periodicamente regravadas em outras mídias, de acordo com a vida útil especificada pelo fabricante.

5.2.4. As mídias devem ser armazenadas em local seguro, cujas condições de temperatura e umidade obedeçam à especificação do fabricante.

5.2.5. Deve-se tomar o devido cuidado quando se descartar mídias, de forma a garantir que suas informações não sejam divulgadas para pessoas externas ao PJTO.

5.2.6. As mídias de armazenamento utilizadas para geração da cópia de segurança têm um período de vida útil que deve ser obedecido, bem como as demais recomendações estabelecidas pelo fabricante.

5.3. Descarte de Mídias

5.3.1. As mídias devem ser descartadas de forma segura e protegida quando se tornarem desnecessárias.

5.3.2. O descarte de informações deve ser feito com a destruição do material de modo que não seja possível recuperá-las, como por exemplo, através de fragmentação ou da eliminação de dados por outra aplicação.

5.3.3. O usuário deve estar atento quanto aos itens abaixo, que podem requerer descarte seguro:

5.3.3.1. documentos em papel;

5.3.3.2. gravação de voz ou de outros tipos;

5.3.3.3. relatórios impressos;

5.3.3.4. fitas magnéticas;

5.3.3.5. discos removíveis e cartuchos;

5.3.3.6. meio de armazenamento ótico (quaisquer formas, incluindo qualquer mídia utilizada pelos fabricantes para distribuição de *software*);

5.3.3.7. listagem de programas;

5.3.3.8. dados de teste;

5.3.3.9. documentação de sistemas.

5.3.4. Periodicamente, deve ser implementada a coleta e o descarte seguro das mídias a serem inutilizadas.

5.3.5. No caso de descarte realizado por empresa terceirizada, deve-se verificar os requisitos básicos de segurança para a contratação do prestador de serviço, como por exemplo, sua experiência e os controles adotados para garantir a segurança do descarte.

5.3.6. O descarte de mídias, sempre que possível, deverá ser registrado para manter trilhas de auditoria.

5.4. Procedimento para tratamento de informação

5.4.1. No tratamento das informações, os seguintes controles devem ser considerados:

5.4.1.1. identificação dos meios magnéticos;

5.4.1.2. acesso restrito a usuários não autorizados;

5.4.1.3. registro formal de destinatários autorizados a acessar dados armazenados. Ex.: *e-mail*;

5.4.1.4. armazenamento de mídias conforme especificação dos fabricantes;

5.4.1.5. identificação eficaz das cópias de segurança;

5.4.1.6. análise crítica das listas de distribuição e das listas dos destinatários autorizados em intervalos regulares.

5.4.2. Procedimentos que contêm informações específicas, por exemplo, local e nome dos responsáveis pelo tratamento de informações confidenciais e as respectivas mídias, devem ser armazenados em local seguro e ter o acesso liberado somente com autorização formal do responsável pelo processo de negócio.

5.5. Segurança da documentação dos sistemas

5.5.1. A documentação dos sistemas deve ser armazenada em local seguro e com acesso controlado aos usuários autorizados.

5.5.2. A documentação de configuração dos ativos deve ser mantida atualizada, com o arquivamento (se aplicável) ou descarte das versões anteriores.

5.5.3. A relação de pessoas autorizadas a acessar a documentação dos sistemas deve ser controlada e realizada apenas com a autorização dos responsáveis.

6**. Norma-TIC-06:** Norma de Segurança da Informação que trata do Controle de Acesso ao Conteúdo *web*: regras de segurança para garantir disponibilidade da rede de serviços do PJTO, bem como controlar o acesso ao conteúdo *web*.

6.1. Disposições iniciais

6.1.1. Para efeito desta norma, o gerenciamento do acesso ao conteúdo *web*, que pode ir além dos limites do PJTO, requer cuidadosas considerações relacionadas ao fluxo de dados, implicações legais, monitoramento, proteção e controle de aplicações.

6.2. Controles da rede

6.2.1. A utilização de recursos compartilhados deve ser feita de forma protegida, visando preservar a confidencialidade, a integridade e a disponibilidade dos ativos.

6.2.2. As transmissões de dados que requerem acesso remoto à rede do PJTO devem obedecer às regras e possuir responsabilidades.

6.2.3. O recurso de informática utilizado pela representação do PJTO em outros Estados, quando de propriedade do PJTO, deve ser monitorado pela Divisão de Administração e Segurança de Redes, podendo esta utilizar ferramentas de gerenciamento remoto, desde que garantidos os requisitos mínimos de segurança quanto à autenticação da conta privilegiada.

6.2.4. O acesso externo aos sistemas mantidos pela Diretoria de Tecnologia da Informação deve ser provido de meios de segurança que protejam a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN e certificados digitais.

6.3. Da Prioridade a Rede de Serviços do PJTO

6.3.1. A Diretoria de Tecnologia da Informação deve fomentar campanhas do uso adequado da rede de serviços do PJTO;

6.3.2. Implementar controles de aplicação, evitando a concorrência dos sistemas jurisdicionais com os serviços externos;

6.4. Do Controle do acesso ao conteúdo Web

6.4.1. É vedado aos usuários dos equipamentos e serviços de informática deste Tribunal:

6.4.1.1. Conectar computadores pessoais ou de terceiros, hubs, modem ADSL, pontos de acesso sem fio (*access points* – AP) à rede de dados (cabeada ou sem fio), salvo computadores portáteis (*notebook*) ou outros equipamentos portáteis similares, que o PJTO tenha fornecido a magistrados ou servidores;

6.4.1.2. Configurar ou alterar as configurações de rede e de acesso à *internet*, incluindo as configurações de Rede IP, DNS, WINS, GATEWAY, PROXY e a instalação ou reconfiguração de clientes PROXY;

6.4.1.3. Acessar sites e/ou recursos via *web* que possam comprometer os sistemas jurisdicionais tais como: consumidores de banda, pornografia, violação de segurança, sites de relacionamento, jogos, canais de *stream* de áudio, vídeo e TV e similares;

6.4.1.4. Acessar sites, instalar e utilizar programas de troca de mensagens instantâneas divergentes dos sistemas homologados pelo PJTO;

6.4.1.5. Instalar ou operar, através de CD/DVD de inicialização, sistema operacional diferente do utilizado atualmente nos microcomputadores do Tribunal; e

6.4.1.6. Utilizar as unidades de entrada e saída de dados (CD/DVD, USB etc) dos microcomputadores, bem como as unidades centralizadas de armazenamento de dados (*storages*), para instalar, copiar, inserir dados (textos, fotos, vídeo, som etc) que não tenham relação com a atividade/atribuição do usuário.

6.4.2. Cabe à Diretorias de Tecnologia da Informação prover toda infraestrutura necessária para implementar o disposto neste item.

6.5. Controle de Banda

6.5.1. Os controles da banda dos *links* de comunicação de dados das Unidades Judiciárias devem garantir o uso em até 80% (oitenta por cento) da capacidade total da velocidade da banda existente. Caso o consumo ultrapasse esse percentual, serão aplicados controles de banda, visando garantir a disponibilidade dos serviços essenciais ao Poder Judiciário.

6.5.2. Dentro da banda garantida será implementado o uso de controles de qualidade de serviço com a “Política 80/20”, descrita da seguinte forma:

6.5.2.1. 20% do Link de comunicação com a Intranet/Internet podem ser alocados, para acesso às mídias sociais, comunicação, áudio, vídeo, rádio e tv com teor e objetivos acadêmico e das áreas do conhecimento e/ou serviços das áreas de comunicação do Judiciário Tocantinense;

6.5.2.2. 80% do Link de comunicação com a Intranet/Internet serão dedicados ao conteúdo dos Sistemas Internos das áreas Jurídicas, Administrativa e aos conteúdos gerais da Internet;

6.6. Perfis de Acesso

6.6.1. Os controles de aplicação, bem como o gerenciamento e acessibilidade aos sítios *web* são balizados nos seguintes perfis de acesso:

6.6.1.2. Perfil Jurídico: aplicado aos desembargadores e juízes de direito;

6.6.1.1. Perfil Jurídico: aplicado aos desembargadores e juízes de direito;

6.6.1.2. Perfil Administrativo: aplicado a todos os usuários das comarcas, juizados, anexos e da sede do Tribunal de Justiça;

6.6.1.3. Perfil Acadêmico: aplicado na Escola Superior da Magistratura Tocantinense (ESMAT);

6.6.2. Cada perfil de acesso possui características peculiares com relação ao controle de banda, controle de aplicação e filtragem de conteúdo *web*.

6.6.3. Estes perfis serão gerenciados e monitorados conforme regras de negócio e recomendação do Comitê Gestor de Segurança da Informação.

Publique-se. Cumpra-se.

Documento assinado eletronicamente por **Desembargador Eurípedes Lamounier**, **Presidente**, em 26/06/2017, às 19:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no link http://sei.tjto.jus.br/verifica/ informando o código verificador **1553013** e o código CRC **5E6E5535**.