TEXTO INTEGRAL

ATO NORMATIVO 8/2019

ATO NORMATIVO TJ N.º 08/2019
Estabelece as normas para Gestão de Segurança da Informação (GSI) do Poder Judiciário do Estado do Rio de Janeiro e dá outras providências.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO, Desembargador CLÁUDIO DE MELLO TAVARES, no uso de suas atribuições legais;

CONSIDERANDO o que dispõe a Lei Federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal;

CONSIDERANDO o que dispõe a Lei Federal nº 13.709/2018, de 14 de agosto de 2018, sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

CONSIDERANDO o que dispõe a Resolução nº 91/2009, do Conselho Nacional de Justiça - CNJ, que instituiu o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MOREQ-JUS);

CONSIDERANDO o que dispõe a Resolução n.º 211/2015 do Conselho Nacional de Justiça - CNJ, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o que dispõe a Resolução nº 215/2015 do Conselho Nacional de Justiça - CNJ, sobre o acesso à informação e a aplicação da Lei 12.527, de 18 de novembro de 2011, no âmbito do Poder Judiciário;

CONSIDERANDO o que dispõe a Resolução TJ/OE nº 34/2014, de 24 de novembro de 2014, que aprova o Programa de Gestão Documental do Poder Judiciário do Estado do Rio de Janeiro - PROGED/PJERJ;

CONSIDERANDO o que dispõe a Resolução TJ/OE n.º 09/2017, de 07 de agosto de 2017, aprovada na sessão administrativa do Órgão Especial do dia 07 de agosto de 2017 (Processo Administrativo n.º 2016-000230);

CONSIDERANDO o que dispõe Ato Normativo n.º 08/2018, de 22 de maio de 2018, sobre o Serviço de Informação ao Cidadão, do Acesso às Informações do Poder Judiciário do Estado do Rio de Janeiro e dá outras providências.

CONSIDERANDO o que dispõe a Resolução TJ/OE n.º 05/2019, de 27 de fevereiro de 2019, sobre a política de segurança da informação, aprovada na sessão administrativa do Órgão Especial do dia 25 de fevereiro de 2019 (Processo Administrativo n.º 2018-107905);

RESOLVE:

TÍTULO I
DAS DISPOSIÇÕES INICIAIS
Art. 1º. A Gestão e a Segurança da Informação no âmbito do Poder Judiciário do Estado do Rio de Janeiro (PJERJ) serão disciplinadas, de acordo com a sua classificação e relevância, pelo presente Ato Normativo.

Art. 2º. O PJERJ é titular de toda informação documentada produzida ou recebida no âmbito deste Poder, relacionadas às atividades institucionais.

Art. 3º. As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual do PJERJ, não cabendo a seus criadores qualquer forma de direito autoral.

Art. 4º. Quando as informações forem produzidas por terceiros para uso exclusivo do PJERJ, a obrigatoriedade do seu sigilo e propriedade deve ser estabelecida em instrumento adequado, respeitada a legislação vigente.
Parágrafo único. Caso as informações de propriedade de terceiros não sejam produzidas exclusivamente para uso deste Poder, caberá ao PJERJ apenas o controle das informações para garantir a sua segurança.

Art. 5º. O acesso à informação sob o domínio do PJERJ seguirá o princípio do privilégio mínimo, ou seja, serão concedidas permissões necessárias e suficientes para que um usuário possa realizar suas atividades, por um tempo

limitado e com os direitos mínimos necessários para tarefas.

Art. 6º. As informações mencionadas neste Título possuem valor e deverão ser protegidas para permitir o uso adequado à consecução dos objetivos institucionais, por meio de atividades operacionais e de negócio.

TÍTULO II
DA CLASSIFICAÇÃO E DO TRATAMENTO DA INFORMAÇÃO
Art. 7º. A informação existe nos seguintes formatos:
I. físico (impresso ou escrito em papel);
II. digital (armazenado em mídias, discos rígidos, entre outros);
III. imagem e voz (fotografias, vídeos e áudio).
§ 1º. A gestão da informação documentada abrange os documentos produzidos, recebidos e armazenados, independentemente da forma ou do suporte, estejam eles em ambientes convencionais, digitais, não digitais ou híbridos.
§ 2º. O acesso à informação, independentemente da forma ou o meio pelo qual ela possa ser exibida ou compartilhada, sempre deverá ser protegido adequadamente, de acordo com os controles definidos na Política de Segurança da Informação (PSI) do PJERJ e por seus documentos complementares.

Art. 8º. As informações devem ser classificadas e protegidas de acordo com o respectivo grau de sigilo e sensibilidade, respeitando o ciclo vital dos documentos em suas fases corrente, intermediária e permanente, exigido pelas atividades do PJERJ, independente do suporte da informação.
Parágrafo Único. Expirados os prazos de guarda definidos na Tabela de Temporalidade de Documentos, a eliminação de documentos eletrônicos no âmbito do PJERJ seguirá os parâmetros de gestão documental emanados pelo Conselho Nacional de Justiça (CNJ) e deve assegurar a preservação da documentação considerada permanente em repositórios digitais confiáveis.

Art. 9º. A classificação de informação em grau de sigilo é disciplinada pelo Ato Normativo TJ n.º 08/2018, que será revisado sempre que necessário para atender as demandas de acesso às informações.
Parágrafo único. Na Tabela de Temporalidade de Documentos do PJERJ será inserido campo específico para informar o grau de sigilo dos assuntos ou do tipo documental.

Art. 10. O tratamento da informação deve seguir os parâmetros estabelecidos na Resolução CNJ nº 91/2009 e na Resolução TJ/OE n.º 34/2014, ou legislação superveniente.

Art. 11. As informações pessoais devem ser tratadas de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem, bem como às liberdades e garantias individuais.
§ 1º. Os sistemas informatizados do PJERJ devem assegurar o acesso restrito a tais informações, independentemente de classificação de sigilo, pelo prazo máximo de 100 anos, a contar da sua produção.
§ 2º. O PJERJ poderá autorizar sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

Art. 12. A informação também pode ser classificada por níveis:
I. Estratégica: informação relevante e fundamental para subsidiar o processo de decisão;
II. Tática: informação agrupada de média complexidade de apoio à decisão gerencial;
III. Operacional: informação não complexa de uso comum nas operações e execução de tarefas cotidianas.

Art. 13. A difusão da informação estratégica pode ser classificada a partir dos seguintes filtros mínimos:
I. alto grau de difusão: a informação específica é amplamente difundida na organização e está livremente disponível para consulta, no nível operacional;
II. médio grau de difusão: a informação específica é transmitida de acordo com a necessidade, até o nível tático da organização;
III. baixo grau de difusão: a informação específica é transmitida somente para o nível estratégico da organização, por razões de sigilo, interesse institucional ou natureza do conteúdo.

TÍTULO III
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO
Art. 14. Além do conjunto normativo adotado pelo PJERJ, a gestão de segurança da informação deverá se pautar pelos procedimentos de boas práticas, baseados na biblioteca ITIL (Information Technology Infrastructure Library).

Art. 15. Caberá ao Comitê Gestor de Segurança da Informação (CGSI) propor à Presidência as diretrizes, políticas, ações de melhoria da segurança da informação no âmbito do PJERJ.

Art. 16. O CGSI, até a última reunião do ano vigente, proporá a agenda do próximo exercício.
§ 1º. As reuniões poderão ser presenciais ou virtuais.
§ 2º. A agenda do exercício poderá ser adequada ao longo do ano de acordo com o aparecimento de novas demandas.
§ 3º. As priorizações de ações da área de segurança da informação deverão ser deliberadas preferencialmente na primeira reunião de cada exercício do CGSI.
§ 4º. As deliberações do CGSI se darão por maioria de votos de seus membros.

Art. 17. A segurança da informação em meio eletrônico deve englobar processos de infraestrutura de TIC e desenvolvimento de aplicações.

Art. 18. A resposta a incidentes de segurança no âmbito do PJERJ compete à DGTEC e à DGSEI (Diretoria Geral de Segurança Institucional)
§ 1º. A DGSEI atuará quando o incidente envolver processos ou procedimentos físicos com pessoas em qualquer instalação do PJERJ.
§ 2º. DGTEC atuará quando o incidente envolver processos ou procedimentos eletrônicos com pessoas ou ativos de TIC.

Art. 19. Todos os contratos, convênios e acordos deverão ter cláusulas que estabeleçam a observância da Política de Segurança da Informação.

CAPÍTULO I
DA GESTÃO DE SEGURANÇA TECNOLOGIA DA INFORMAÇÃO
SEÇÃO I
DA GESTÃO DE INFRAESTRUTURA DE TIC
Art. 20. Compete à DGTEC a gestão dos recursos que compõem a infraestrutura de TIC do PJERJ, que incluem, dentre outros:
I. Computadores servidores e unidades de armazenamento;
II. Bancos de dados;
III. Recursos de rede e segurança, switches, firewall, proxy, IPS.

Art. 21. Qualquer demanda que implique alteração da configuração da infraestrutura de TIC estará condicionada à avaliação e autorização prévia pela DGTEC.
Parágrafo Único. A mudança deverá ser submetida para apreciação na forma padrão determinada em normas pertinentes, incluindo justificativas, análise de riscos, plano de reversão e outras informações que a DGTEC julgar necessárias.

Art. 22. A administração de dados e de serviços do Centro de Processamento de Dados (CPD ou Data Center) observará, obrigatoriamente, as melhores práticas de mercado e aquelas recomendadas pelos fabricantes das tecnologias em uso, e utilizará mão de obra qualificada, com perfil técnico adequado.

Art. 23. A função de administrador do CPD e do sistema de autenticação forte para acesso físico às suas dependências deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TIC.

Art. 24. Os sistemas elétrico e de refrigeração do CPD deverão ter funcionamento pleno e ininterrupto, devendo a área do PJERJ responsável por sua manutenção emitir anualmente relatórios com informações relativas ao seu estado de funcionamento, a ser encaminhado ao CGSI.

SUBSEÇÃO I
DA GESTÃO DE SERVIDORES
Art. 25. Os ativos de processamento e de armazenamento de dados do PJERJ deverão ser instalados em sala cofre segura, que disponha de mecanismos de monitoração visual por câmeras e que mitiguem, no mínimo, os seguintes riscos de segurança de natureza física:
I. condições ambientais adversas;
II. desastres naturais;
III. incêndios;
IV. variações de temperatura; e
V. acesso indevido.

§ 1°. A sala cofre segura de que trata este artigo deve dispor de controles de corrente elétrica (rede estabilizada), temperatura, umidade e acesso físico restrito por meio de mecanismo de autenticação forte.
§ 2°. A credencial de acesso assim como o cadastramento de biometria para acesso físico contínuo à sala cofre segura deverá seguir o critério de exceção de forma que só devem possuí lo as pessoas que necessitem expressamente de tal acesso.

Art. 26. Os ativos de TIC sob administração da área de servidores da DGTEC deverão passar por processo de gestão de vulnerabilidades, cujo objetivo é detectar e corrigir vulnerabilidades existentes em itens como kernel, sistema operacional, firmware e aplicações, com a frequência determinada em procedimento próprio.
§ 1º. O processo de gestão de vulnerabilidades deverá contemplar, no mínimo, as seguintes atividades:
I. detecção;
II. classificação;
III. avaliação de risco e impacto;
IV. priorização;
V. correção;
VI. testes.
§ 2º Após aplicadas correções disponíveis para vulnerabilidades, deverão ser realizados testes - conforme escopo e regra previamente definidos - para verificação de sua eficácia e da funcionalidade dos ativos de TIC que as receberam.
§ 3º A impossibilidade de se corrigir determinada vulnerabilidade deve ser documentada e fundamentada - inclusive com informações de eventuais soluções de contorno - em relatório a ser encaminhado ao CGSI.

Art. 27. Para que o PJERJ possa garantir a prestação jurisdicional essencial, deve-se garantir que, no mínimo, os sistemas e serviços críticos estejam hospedados em infraestrutura de servidores e armazenamento que disponha de segurança física e lógica com tolerância a falhas e redundância de processamento, rede de comunicação, armazenamento e sistemas elétricos e de refrigeração.

Art. 28. Os equipamentos que estejam instalados na sala cofre segura, ainda que não estejam sendo utilizados em qualquer fase do ciclo de vida, deverão possuir monitoramento que permita identificar falhas, quando o equipamento fica inacessível, e falhas de componentes físicos, tais como memória, disco, processador e interfaces de rede.

Art. 29. A infraestrutura de servidores e equipamentos de armazenamento deverá ser segregada em desenvolvimento, treinamento, homologação e produção.
§ 1°. O ambiente de produção não deve ser compartilhado e utilizado para demandas que não se caracterizem como tal.
§ 2°. O ambiente de produção só deve ser acessado por pessoas autorizadas e com conta de acesso válida no sistema de gerenciamento de identidade.
§ 3°. O ambiente de homologação deve ser o máximo possível semelhante ao de produção, sendo indispensável a mesma arquitetura e configuração, de forma a permitir que seja utilizado como referência de funcionamento.
§ 4°. Informações e documentos produzidos no ambiente de homologação não têm validade jurídica.
§ 5°. Os ambientes especificados podem ser eventualmente aprovisionados, mediante clonagem, com o objetivo de se ter um ambiente condizente com a realidade operacional e a fim de obter maior precisão no diagnóstico de problemas.

Art. 30. A disponibilização de novas versões de sistemas em ambiente de produção deve ser controlada e gerenciada através do processo de gestão de mudanças e liberação e precedida por controle de qualidade realizado em ambiente de homologação que avalie no mínimo:
I. O resultado dos testes de funcionalidade;
II. O impacto gerado na capacidade do ambiente após execução de testes de carga;
III. Eventuais riscos, incluindo os de segurança, decorrentes da mudança.

Art. 31. O acesso aos computadores servidores, equipamentos de armazenamento, softwares de gerenciamento e de camada de aplicação, sistemas operacionais, serviços de infraestrutura de rede estará submetido às políticas de controle de acesso vigentes no PJERJ.

SUBSEÇÃO II
DA GESTÃO DE ARMAZENAMENTO E REDUNDÂNCIA DA INFORMAÇÃO
Art. 32. Os dados e informações dos sistemas corporativos do PJERJ, bem como os documentos relevantes produzidos em ferramentas informatizadas serão armazenados, supervisionados e controlados pela DGTEC, em ambiente que permita redundância e procedimentos periódicos de cópia de segurança.

Art. 33. Os equipamentos de armazenamento podem estar fisicamente nas instalações do PJERJ ou em ambiente externo, por contratação de serviços, desde que não haja comprometimento da segurança dos dados e informações, observada a legislação sobre Segurança da Informação vigente.
Parágrafo único. Os contratos para armazenamento de informação em ambiente externo deverão conter cláusulas prevendo o atendimento das normas de segurança adotadas pelo PJERJ.

Art. 34. Os arquivos de documentos produzidos e utilizados nas atividades institucionais do PJERJ deverão ser armazenados nos recursos de TI disponibilizados pela DGTEC para essa finalidade, como servidores de rede e solução em nuvem, que possuem funcionalidades para garantir a segurança do armazenamento, inclusive cópia de segurança que permita a recuperação de arquivos acidentalmente excluídos.
§ 1º. O espaço para armazenamento de dados será limitado com atribuição de quotas para cada unidade do PJERJ cabendo ao usuário a utilização eficiente do recurso, inclusive com a exclusão de arquivos obsoletos ou desnecessários.
§ 2º. O responsável pela unidade, ou pessoa por ele indicada, informará os usuários que terão permissão de acesso ao espaço fornecido para armazenamento.
§ 3º. O armazenamento dos arquivos apenas localmente, nas estações de trabalho, não oferece segurança quanto à preservação dos dados armazenados, não sendo a DGTEC responsável por eventuais perdas de informação associadas a essa prática.
§ 4º. É vedado o armazenamento de arquivos pessoais ou quaisquer outros não relacionados às atividades institucionais do PJERJ nos recursos de TI disponibilizados pela DGTEC, que poderá excluí-los definitivamente, após comunicação ao usuário e à chefia imediata.
§ 5º. É vedado o acesso a partir da rede corporativa do PJERJ a sites e outros recursos de armazenamento de dados e arquivos que não tenham sido disponibilizados ou autorizados pela DGTEC.

SUBSEÇÃO III
DAS CÓPIAS DE SEGURANÇA (BACKUP)
Art. 35. A DGTEC deverá utilizar recursos adequados para a geração de cópias de segurança que garantam a recuperação de informações e sistemas, armazenados em servidores e storages sob sua responsabilidade, em caso de falhas físicas e lógicas, erros e desastres.
Parágrafo Único. A realização de cópia de segurança dos dados contidos em discos rígidos das estações de trabalho é de responsabilidade do usuário.

Art. 36. O serviço de cópia de segurança deve ser automatizado e executado de forma a não prejudicar as atividades da prestação jurisdicional.

Art. 37. A DGTEC poderá utilizar as seguintes tecnologias, isoladamente ou combinadas, a fim de obter maior eficiência na cópia e restauração de informações e sistemas:
I. fitas magnéticas;
II. discos rígidos;
III. VLT (Virtual Tape Libraries);
IV. imagem do ambiente (Snapshots);
V. replicação síncrona e assíncrona;
VI. armazenamento em nuvem.
§ 1º. Qualquer que seja a tecnologia empregada, a cópia de segurança deverá ser gerenciada por uma ferramenta centralizada, homologada pela DGTEC.

§ 2º. No caso de utilização de fitas magnéticas, sua administração, manuseio e renovação deverão ser contemplados em normas complementares sobre o serviço, objetivando manter sua segurança e integridade.

Art. 38. A ferramenta utilizada para a cópia de segurança (backup) deverá ser mantida atualizada, considerando no mínimo as seguintes características:
I. atualizações de correção;
II. novas versões;
III. ciclo de vida;
IV. garantia;
V. melhorias.

Art. 39. As cópias de segurança deverão ser armazenadas em instalações seguras, controladas, preferencialmente com estrutura de cofres, salas cofre e localização diversa das bases originais.

Art. 40. A periodicidade, o tempo de retenção e o tempo de restauração das cópias de segurança devem ser definidos de acordo com o grau de importância da informação e/ou do sistema.

Art. 41. As cópias de segurança históricas, especiais ou críticas, exigem regra de retenção especial, a ser prevista em procedimentos específicos, de acordo com normas de classificação da informação pública e determinações fiscais e legais.

Art. 42. A execução de rotinas de cópia de segurança (backup) e restauração (restore) deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

Art. 43. A DGTEC deverá garantir que os serviços na nuvem tenham cópia de segurança e restauração previstas em contrato, seguindo as melhores práticas de mercado.

Art. 44. A DGTEC deverá executar testes periódicos de restauração para validar a integridade dos dados existentes nas cópias de segurança.

SUBSEÇÃO IV
DO BANCO DE DADOS

Art. 45. Todo sistema corporativo informatizado do PJERJ, em relação a aspectos de segurança de informação, deverá possuir no respectivo SGBD (Sistema de Gerenciamento de Banco de Dados) somente os privilégios mínimos necessários ao não prejuízo à execução das respectivas regras de negócios definidas em sua construção.
Parágrafo único. A restrição de privilégios deverá ser obtida, quando possível, segregando dentro do respectivo SGBD o usuário a ser utilizado pelo sistema/aplicação do usuário dono das tabelas do respectivo sistema.

Art. 46. Todo registro das operações realizadas por usuários de sistemas corporativos do PJERJ, cujo respectivo sistema corporativo armazene no próprio SGBD, deverá ser preservado em tabelas armazenadas separadamente das tabelas do respectivo sistema, de forma protegida e permitindo auditoria de alterações.
Parágrafo único. A proteção estabelecida neste artigo estende-se aos registros de auditoria do próprio software de SGBD.

Art. 47. O privilégio de administração de SGBD que armazene dados de sistema corporativo do PJERJ, em qualquer meio, deverá estar restrito a DGTEC, e deverá ser auditado e individualizado sempre que possível tecnicamente.
Parágrafo único. Na inviabilidade técnica de restrição do presente artigo, devido a requisitos de funcionamento inerentes ao software ou solução de TIC utilizada ou adquirida de terceiros, a administração e a responsabilidade pelo respectivo SGBD deverão ser compartilhadas com o demandante da respectiva solução de TIC.

Art. 48. Todo software de SGDB que armazene dados de sistemas corporativos do PJERJ deverá ser mantido atualizado com as correções de segurança disponibilizados pelos respectivos fabricantes do SGBD.
Parágrafo único. A respectiva equipe da DGTEC responsável pela administração de bancos de dados deverá manter rotina revisada periodicamente mantendo-a compatível e alinhada com as melhores práticas do mercado e com as recomendações do fabricante do respectivo SGBD.

Art. 49. Toda conexão com SGBD que armazene dados de sistemas corporativos do PJERJ somente deverá ser estabelecida através software e componentes homologados e recomendados pelos respectivos fabricantes de SGBD, sempre de forma segura e protegida.

Art. 50. Todo SGBD de sistema corporativo do PJERJ deve possuir rotina de cópia de segurança em meio de armazenamento diverso do próprio SGBD.
Parágrafo único. A rotina deverá ser implementada e revisada periodicamente para garantir a efetiva recuperabilidade dos dados armazenados, bem como deverá seguir as melhores práticas do mercado e recomendações do respectivo fabricante do SGBD.

SUBSEÇÃO V
DA GESTÃO DE REDES

Art. 51. Compete à DGTEC a gestão de segurança da rede corporativa do PJERJ.

Art. 52. A conexão à rede corporativa do PJERJ de qualquer recurso de TIC, inclusive através de VPN (rede privada virtual), deverá ser aprovada pelo CGSI e autorizada pela Presidência.

§1º. O CGSI proporá as situações, que serão aprovadas pela Presidência, em que a DGTEC terá competência para autorizar a conexão.
§2º. A DGTEC determinará regras, condições e parâmetros para criação e configuração da VPN.
§3º. Os responsáveis pelos recursos de TIC que se conectarem à rede corporativa do PJERJ obrigam-se a observar as normas pertinentes definidas pelo PJERJ, inclusive quanto à configuração dos recursos.

Art. 53. Dispositivos particulares poderão ter acesso a uma sub-rede de visitantes, obedecendo os critérios de segurança da Informação adotados pelo PJERJ e a regulamentação em vigor.

Art. 54. Poderá ser bloqueada a conexão à rede corporativa, inclusive a sub-rede de visitantes, caso sejam detectadas ações suspeitas ou que constituam ameaças à segurança da informação.

Art. 55. Compete à DGTEC determinar ou autorizar a criação e utilização de redes segregadas utilizando recursos de segmentação lógica.

Art. 56. Toda informação trafegada na rede corporativa poderá ser monitorada pela DGTEC a fim de se garantir a segurança da informação, em caso de fragilidades, ameaças, ocorridas ou suspeitas.

SEÇÃO II
DA GESTÃO DE DESENVOLVIMENTO DE TIC
Art. 57. Toda solução de TIC desenvolvida pela DGTEC, sob sua supervisão ou adquirida de fornecedores ou fabricantes externos, deverá:
I. utilizar o Ciclo de Vida de Desenvolvimento de Sistemas (CVDS) (Security Development Lifecycle (SDL));
II. utilizar preferencialmente as normas: ABNT NBR ISO/IEC 27002, 27005 ou equivalentes, no que for cabível;
III. utilizar as recomendações dos fabricantes das tecnologias adotadas pela solução, de forma a proporcionar computação confiável e resistir a ataques mal-intencionados;
IV. ser disponibilizada para uso em produção após inspeção automatizada realizada por ferramentas de segurança, que constatem não haver neles vulnerabilidades conhecidas, exceto para sistemas legados na qual a tecnologia utilizada não seja compatível com as ferramentas de segurança;
V. submeter-se com sucesso a execução e análise de testes de segurança e invasão com o objetivo de garantir a segurança da rede corporativa do PJERJ quando de sua homologação;
VI. permitir a geração de logs de erro da aplicação, bem como de processamentos para efeitos de auditoria;
VII. obedecer aos princípios de arquitetura de, no mínimo, 3 (três) camadas (camada de apresentação, camada de negócio e camada de dados), para novos sistemas ou atualizações de sistemas atuais do PJERJ;
VIII. utilizar preferencialmente protocolo de transporte seguro TSL ou SSL no seu desenvolvimento para acesso sob conexão segura (https).
§ 1º. Caso a DGTEC identifique a possibilidade do surgimento de uma nova vulnerabilidade no desenvolvimento de uma correção emergencial, que seja imperativa para o pleno funcionamento da prestação jurisdicional, caberá ao CGSI analisar e propor à Presidência para autorizar e ao usuário final do sistema, juntamente com o Magistrado da área, assumir expressamente os riscos pela disponibilização da correção em produção.
§ 2º. Todo evento de uma solução que gere alteração numa informação deverá ser registrado em trilha de auditoria preferencialmente ou de forma que seja possível futura consulta ou relatório, contemplando no mínimo as seguintes informações: data, hora, usuário, evento, informação original, informação atualizada. Não havendo necessidade de um registro redundante para tal, quando não for possível.
§ 3º. A solução deve prover relatórios e/ou consultas de qualquer alteração numa informação.

Art.58. A DGTEC juntamente com os usuários das áreas responsáveis por soluções de TIC legadas deverão apresentar em até 12 (doze) meses um plano de migração destas soluções para protocolos mais seguros.

TÍTULO IV
DA GESTÃO DE CONTINUIDADE DE SERVIÇOS
Art. 59. A implantação do processo de Gestão de Continuidade de Serviços busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do PJERJ, além de recuperar, em um nível aceitável, ativos de informação afetados, por intermédio de ações de prevenção, resposta e recuperação.

Art. 60. O PJERJ deverá elaborar e manter Programa de Gestão de Continuidade de Negócios (PGCN), suportado pela Alta Administração, baseado nas melhores práticas e com recursos necessários para:
I. garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial;

II. manter estratégias e planos de recuperação;
III. garantir a continuidade de fornecimento de produtos e serviços por meio de análises críticas, testes, treinamentos e manutenção.

Art. 61. O PGCN do PJERJ deverá ser composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:
I. Plano de Gerenciamento de Incidentes (PGI): plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, órgãos, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes;
II. Plano de Continuidade de Negócios (PCN): documentação dos procedimentos e informações necessárias para que o PJERJ mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em casos de incidentes;
III. Plano de Recuperação de Negócios (PRC): documentação dos procedimentos e informações necessárias para que o PJERJ operacionalize o retorno das atividades críticas à normalidade.
§ 1º. Os planos acima definidos deverão ser testados e revisados sempre que necessário, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.
§ 2º. As revisões anuais dos planos acima deverão ser aprovadas pelo CGSI até o mês de outubro e disponibilizadas no sítio institucional do PJERJ.

Art. 62. Para subsidiar a elaboração de seu PGCN, o PJERJ deverá definir quais são suas atividades críticas, ou seja, quais são as atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Art. 63. Os procedimentos previstos no PGCN deverão ser executados em conformidade com os requisitos de segurança da informação e comunicação necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, incluindo pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicação.

TÍTULO V
DO MONITORAMENTO E DA AUDITORIA
Art. 64. Para garantir a aplicação das diretrizes estabelecidas nesta norma, o PJERJ deverá:
I. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros recursos da rede, de forma a identificar usuários, acessos efetuados, e ações executadas;
II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de determinação judicial ou por determinação da Presidência;
III. Realizar, a qualquer tempo, inspeção física nos equipamentos, de sua propriedade ou de terceiros, em uso no PJERJ;
IV. Instalar sistemas de proteção, prevenção e detecção de intrusão que garantam a segurança das informações e dos perímetros de acesso;
V. Desinstalar, a qualquer tempo, softwares ou sistemas que representem risco ou estejam em situação de não conformidade com as políticas, normas e procedimentos vigentes;
VI. Desconectar, a qualquer tempo, servidores e equipamentos de rede que constituam riscos iminentes para a segurança da rede do PJERJ.

Art. 65. Os acessos ao CPD serão objeto de auditorias, realizadas com a frequência determinada em procedimento próprio.

Art. 66. A DGTEC, com autorização do Presidente do PJERJ, poderá acessar estações de trabalho, computadores servidores, arquivos, registros ou quaisquer recursos de TIC, em caso de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas, de serviços ou de informações sempre que necessário realizar investigações de caráter técnico.

Art. 67. As solicitações de auditorias de segurança, análise ou informação quanto ao uso dos recursos de TIC deverão ser dirigidas à DGTEC e serão atendidas - observada a temporalidade dos registros - após aprovação da autoridade competente.

Art. 68. É dever de todos os usuários reportar imediatamente à autoridade diretamente superior e à DGTEC fragilidades, ameaças ou ações indevidas de que tiver conhecimento ou suspeita, relacionadas à segurança dos

sistemas, serviços, informações ou quaisquer recursos de TIC, inclusive daqueles que não estejam sob sua responsabilidade.
Parágrafo Único. É vedado ao usuário realizar por conta própria investigações nos recursos de TIC.

Art. 69. O PJERJ poderá contratar auditorias externas independentes, testes de intrusão ou outros serviços relacionados, para avaliar a segurança de sua infraestrutura, sistemas e demais recursos de TIC.

TÍTULO VI
DOS PROCESSOS DE COMUNICAÇÃO E CONSCIENTIZAÇÃO INSTITUCIONAL
Art. 70. O PJERJ desenvolverá Plano de Comunicação Institucional de Segurança da Informação (PCISI) que deverá contemplar ações para a divulgação, sensibilização e prospecção da PSI e dos seus instrumentos.
§ 1º. O CGSI indicará Grupo Técnico que, sob a orientação da Diretoria-Geral de Comunicação e de Difusão do Conhecimento (DGCOM), elaborará e revisará o PCISI;
§ 2º. O PCISI deverá conter os meios e os critérios de comunicação da informação, considerando o público-alvo ao qual se destina;
§ 3º. O PCISI deverá ser avaliado, ordinariamente, pelo CGSI, bianualmente, até o mês de maio para aprovação da Presidência e disponibilizado no sítio institucional do PJERJ;
§ 4º. O PCISI será parte integrante do Plano de Comunicação Institucional do PJERJ;
§ 5º. As campanhas de comunicação interna deverão ser recorrentes e seguidas de mecanismos para averiguar sua efetividade.

Art. 71. A DGCOM é a unidade responsável pela criação e pela realização das campanhas de sensibilização em segurança da informação, com o apoio da DGTEC e da DGSEI, com o objetivo de incentivar a adoção de boas práticas de segurança da informação.

Art. 72. Cumpre ao usuário interno do PJERJ comunicar imediatamente à autoridade diretamente superior e à DGTEC, através de seus canais de atendimento, quaisquer indícios de ameaças à segurança da informação, de que tome conhecimento.

Art. 73. O CGSI proporá a Presidência o fluxo de comunicação da ocorrência do incidente, considerando o seu grau e a sua abrangência, encaminhando ao Grupo Técnico e de Gestão para Atuação no Tratamento e Respostas aos Incidentes de Segurança da Informação do Tribunal de Justiça do Estado do Rio de Janeiro (GTRISC), criado pelo Ato Executivo TJ n.º 111/2018, quando necessário;

Art. 74. Compete à DGCOM, quando demandada, orientar sobre o canal de comunicação apropriado para divulgação do tratamento e da resposta relacionados ao incidente de segurança da informação.

Art. 75. A DGTEC poderá recomendar capacitação específica a usuários sempre que identificar incidência expressiva de ações não conformes com as boas práticas de segurança da informação.

Art. 76. O PJERJ ministrará aos usuários - em cursos da ESAJ, campanhas de comunicação interna ou outros recursos - capacitações regulares em temas de Segurança da Informação.
Parágrafo único. Em até dois anos da publicação desta norma, todos os usuários internos do PJERJ deverão estar capacitados com relação a boas práticas no uso de senhas e cópias de segurança e defesa contra ameaças mais comuns como phishing e engenharia social.

TÍTULO VII
DAS DISPOSIÇÕES FINAIS
Art. 77. O PJERJ publicará norma específica para disciplinar a Gestão de Riscos de Segurança da Informação.

Art. 78. Qualquer alteração ou tentativa de alteração não autorizada na configuração de recursos de TIC constituirá infração a esta norma.

Art. 79. Os casos de desrespeito a esta norma serão encaminhados pela DGTEC ao CGSI para a avaliação e proposição das providências cabíveis, nos termos da legislação vigente.

Art. 80. A inobservância dos dispositivos desta norma pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 81. Os casos omissos ou divergências de interpretação dos dispositivos deste Ato Normativo serão resolvidos pela Presidência.

Art. 82. O presente Ato Normativo entrará em vigor na data de sua publicação, revogando as disposições em contrário.

Rio de Janeiro, 24 de julho de 2019.

Desembargador CLÁUDIO DE MELLO TAVARES
Presidente