TEXTO INTEGRAL

RESOLUÇÃO 5/2019

RESOLUÇÃO TJ/OE Nº 05/2019

Institui a Política de Segurança da Informação (PSI) do Poder Judiciário do Estado do Rio de Janeiro.

O ÓRGÃO ESPECIAL DO TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pelo disposto no inc. I do art. 96 e no art. 99 da Constituição da República, bem como na alínea "a", inc. VI, do art. 3º do Regimento Interno, e tendo em vista o decidido na sessão realizada no dia 25 de fevereiro de 2019 (Processo nº 2018-107905);
CONSIDERANDO que o Poder Judiciário do Estado do Rio de Janeiro recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;
CONSIDERANDO o número progressivo de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;
CONSIDERANDO a Resolução TJ/OE n.º 09/2017, que instituiu os Comitês de Governança de Tecnologia da Informação e Comunicação (CGTIC), de Diretores Gestão de Tecnologia da Informação e Comunicação (CDGTIC) e Gestor de Segurança da Informação (CGSI) deste Tribunal;
CONSIDERANDO os termos da Resolução CNJ n.º 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e estabeleceu as diretrizes para sua governança, gestão e infraestrutura;
CONSIDERANDO o estudo realizado pelo Grupo de Trabalho criado pela Portaria n.º 108/2018 para elaboração da política de segurança da informação do Poder Judiciário do Estado do Rio de Janeiro;
CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;
CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Gestão de Riscos de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27005:2011, que trata da segurança da informação;
CONSIDERANDO que a Lei Federal nº 12.527/2011 (Lei de Acesso à Informação), bem como, no âmbito do Judiciário, a Resolução CNJ n.º 215/2015, disciplinam que todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
CONSIDERANDO que a segurança e a preservação dos documentos digitais devem estar associadas a um repositório digital confiável que ofereça acesso seguro e de longo prazo aos documentos considerados permanentes do PJERJ, de acordo com os parâmetros da Resolução TJ/OE nº 34/2014;
CONSIDERANDO que o acervo de documentos em mídia não digital, de caráter histórico e permanente, custodiado na rede de arquivos do PJERJ, necessita de uma política de segurança da informação arquivística, no que tange ao acesso e à integridade física dos documentos, assegurando a sua autenticidade e fidedignidade;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
Seção I
Dos Princípios Básicos da PSI

Art. 1º. Instituir a Política de Segurança da Informação (PSI) do Poder Judiciário do Estado do Rio de Janeiro (PJERJ), que tem como princípios básicos:
I.a proteção do direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição Federal;
II.a proteção de informações relacionadas a assuntos que mereçam tratamento especial, conforme definição do Comitê Gestor de Segurança da Informação;
III.a capacitação dos segmentos das tecnologias sensíveis;
Iv.a criação, desenvolvimento e manutenção de uma cultura relacionada à segurança da informação, alinhada com as diretrizes nacionais de segurança da informação e com a legislação federal, propiciando uma integração com os demais órgãos do Judiciário e com outros Poderes.

Seção II

Da Estrutura Normativa da Segurança da Informação

Art. 2º. A Estrutura Normativa da Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro é constituída por:
I.Política de Segurança da Informação (PSI) aqui instituída;
II.Normas de Segurança da Informação, que devem contemplar as obrigações a serem seguidas de acordo com os objetivos e diretrizes estabelecidos nesta PSI;
III.Normas de gerenciamento e tratamento de riscos de TIC;
IV.Procedimentos de Segurança da Informação, que definem regras operacionais de acordo com as Normas de Segurança da Informação.
Parágrafo único. A Estrutura Normativa da Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro tem como objetivo garantir os princípios básicos da segurança da informação, quais sejam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio, bem como contribuir para que a missão do Judiciário do Estado do Rio de Janeiro seja cumprida.
Seção III
Das Definições relativas à PSI

Art. 3º. Para efeitos desta Política, ficam estabelecidos os seguintes conceitos:
I.ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, a integridade, a disponibilidade e a autenticidade da informação;
II.ativo de informação: os meios de armazenamento físicos ou eletrônicos, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
III.ativo crítico: ativos, dispositivos ou sistemas mínimos imprescindíveis para a prestação dos serviços essenciais do PJERJ;
IV.ativo estratégico: ativos, dispositivos ou sistemas cujo funcionamento é estratégico para as atividades finalísticas do PJERJ, porém não necessariamente prioritários em caso de incidentes;
V.autenticidade: propriedade de como a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;
VI.ciclo vital dos documentos: sucessivas fases por que passam os documentos arquivísticos, de sua produção à guarda permanente ou eliminação;
VII.confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;
VIII.defeito: imperfeição ou inconsistência em serviço, software ou processo que leve a uma não conformidade;
IXdisponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;
X.erro: resultado não esperado proveniente de um defeito ou falha;
XI.falha: comportamento inesperado de um software ou sistema;
XII.gestor de ativo de informação: são os titulares das unidades responsáveis pela gestão e operação dos ativos de informação;
XIII.incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita;
XIV.informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que se materialize ou da forma pela qual seja veiculado;
XV.informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
XVI.integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;
XVII.não repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;
XVIII.plano de continuidade de serviços essenciais: documentação dos procedimentos e informações necessárias para manter os ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo previamente definido, em casos de incidente;
XIX.plano de recuperação de serviços essenciais: documentação dos procedimentos e informações necessárias para que se operacionalize o retorno das atividades críticas à normalidade;
XX.preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo acesso e interpretação dos documentos digitais pelo tempo que for necessário;
XXI.público alvo: é o conjunto de usuários internos e externos atendidos pelo 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);

XXII.risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;
XXIII.segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XXIV.serviços essenciais: são aqueles que são imprescindíveis à atividade finalística do Tribunal de Justiça do Estado do Rio de Janeiro (TJERJ);
XXV.unidade gestora de segurança da informação: é a unidade responsável pela gestão de segurança da informação no TJERJ;
XXVI.usuário externo: qualquer pessoa física ou jurídica não caracterizada como usuário interno, que tenha acesso a informações produzidas pelo TJERJ de forma autorizada;
XXVII.usuário interno: qualquer servidor, magistrado, prestador de serviço terceirizado, estagiário ou qualquer outro colaborador que tenha credencial de acesso às informações produzidas pelo TJERJ de forma autorizada; e
XXIII.vulnerabilidade: fragilidade de um ou mais ativos, processos e serviços que, se explorados de maneira negativa por uma ou mais ameaças, gera impacto na Segurança da Informação.

Seção III
Dos Objetivos da PSI

Art. 4º. São objetivos desta Política de Segurança da Informação:
I.dotar as unidades do PJERJ de instrumentos jurídicos, normativos e organizacionais que as capacitem a assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações produzidas e armazenadas;
II.estabelecer diretrizes e normas gerais para a efetiva implementação da segurança da informação;
III.subsidiar a promoção das ações necessárias à implementação e à manutenção dos processos de gestão de riscos, gestão de incidentes de segurança da informação, gestão da continuidade de serviços essenciais e gestão do uso dos recursos de Tecnologia da Informação e Comunicação (TIC); e
IV.promover o intercâmbio científico-tecnológico entre o TJERJ, os demais órgãos e entidades do Judiciário do país e as instituições públicas e privadas sobre as atividades de segurança da informação.

CAPÍTULO II
DAS DIRETRIZES GERAIS
Seção I
Da Classificação e Tratamento da Informação

Art. 5º. Os critérios gerais aplicáveis à classificação e ao tratamento da informação serão definidos por Ato Normativo da Presidência, elaborado pelo Comitê Gestor de Segurança da Informação (CGSI), com a participação de representantes de todas as unidades do PJERJ que produzem, recepcionam ou custodiam informações essenciais às atividades finalísticas.
§ 1º. Toda informação documentada produzida ou recebida no âmbito do PJERJ pertence ao próprio Tribunal, possui valor e deve ser protegida para permitir o uso adequado à consecução dos objetivos institucionais, por meio de atividades operacionais e de negócio.
§ 2º. As informações devem ser classificadas e protegidas de acordo com o grau de sigilo e sensibilidade, respeitando o ciclo vital dos documentos exigido pelas atividades do PJERJ.

Art. 6º. A informação existe nos seguintes formatos:
I.físico (impressa ou escrita em papel);
II.digital (armazenada em mídias e discos rígidos, entre outros);
III.imagem e voz (fotografias, vídeos e áudios).
§ 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 do meio pelo qual ela possa ser exibida ou compartilhada, sempre deverá ser protegido adequadamente, de acordo com os controles definidos, pela presente Política e por seus documentos complementares.
§ 3º. A informação sigilosa deverá seguir os parâmetros da Lei de Acesso à Informação (Lei Federal nº 12.527/2011).

Seção II
Da Gestão de Riscos de Segurança da Informação

Art. 7º. A gestão de riscos é realizada por meio de processo definido de maneira formal, contendo as fases de análise, avaliação e tratamento dos riscos.

§ 1º. O processo de gestão de riscos deverá, sempre que possível e necessário, ser apoiado por uma ferramenta computacional que contemple as atividades mencionadas no caput deste artigo.
§ 2º. A política de gestão de riscos será regulada por Ato Normativo próprio.

Art. 8º. Os gestores dos ativos de informação são os responsáveis pela execução das fases de análise, avaliação e tratamento dos riscos.
Parágrafo único. A unidade gestora de segurança da informação supervisionará os gestores de ativos de informação nas atividades mencionadas no caput deste artigo.

Art. 9º. O escopo da gestão de riscos de TIC será definido anualmente pelas áreas envolvidas nas atividades finalísticas, coordenadas pela Diretoria Geral de Tecnologia da Informação e Comunicações (DGTEC), com a aprovação do CGSI, mantendo a correspondência com os serviços essenciais, preferencialmente.
Parágrafo único. Os critérios gerais aplicáveis para aceitação de riscos serão definidos anualmente pelo CGSI, com a orientação técnica da DGTEC.

Art. 10. A unidade gestora de segurança da informação elaborará relatório anual de gestão de riscos para o CGSI, contendo as ações tomadas frente às ameaças e as recomendações utilizadas para tratar os riscos identificados.

Seção III
Da Gestão do Acesso e Uso dos Recursos de Tecnologia da Informação e Comunicação

Art. 11. A gestão de acesso e uso dos recursos relacionados à segurança da informação, disponibilizados pelo PJERJ, será regulada por Ato Normativo próprio, contendo, no mínimo, descrição do recurso, seu gestor, seu uso, política de utilização e sanções em caso de violação.

Art. 12. Estão sujeitos à regulamentação de que trata o caput do art. 11 os usuários internos e externos do PJERJ que, de maneira autorizada, tenham acesso aos recursos de TIC prestados por este Tribunal.
Parágrafo único. A utilização desses recursos está condicionada à aceitação desta política por parte dos usuários mediante assinatura de termo de uso, preferencialmente em meio eletrônico.

Art. 13. Os recursos de tecnologia da informação disponibilizados devem ser utilizados, exclusivamente, em atividades estritamente relacionadas às funções institucionais.

Art. 14. Os recursos de tecnologia da informação, no âmbito do PJERJ, serão passíveis de monitoração pela Diretoria-Geral de Tecnologia da Informação e Comunicação de Dados (DGTEC), em caso de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas, de serviços ou de informações.

Seção IV
Da Gestão e Controle de Ativos de Informação

Art. 15. A gestão e controle dos ativos de informação é realizada por meio de processo definido de maneira formal, contendo as fases de cadastro, atualização e exclusão, e será regulada por Ato Normativo próprio.
Parágrafo único. O processo de gestão e controle dos ativos de informação deverá, sempre que possível e necessário, ser apoiado por ferramenta computacional que contemple as atividades mencionadas no caput deste artigo.

Art. 16. Os gestores dos ativos de informação são os responsáveis pela execução das fases de cadastro, atualização e exclusão.
Parágrafo único. A unidade gestora de segurança da informação do PJERJ fiscalizará os gestores de ativos de informação nas atividades mencionadas no caput deste artigo, conforme estabelecido no Ato Normativo de Gestão de Segurança da Informação.

Seção V
Da Gestão de Incidentes de Segurança da Informação

Art. 17. A gestão de incidentes de segurança da informação é realizada por meio de processo definido de maneira formal, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Art. 18. O Comitê Gestor de Segurança da Informação (CGSI) é o fórum para aprovar ações decorrentes de um incidente ou ameaça de segurança que afetem a imagem institucional ou a confidencialidade das informações do PJERJ.

§ 1º. O Grupo Técnico e de Gestão para Tratamento e Respostas aos Incidentes de Segurança da Informação do Tribunal de Justiça do Estado do Rio de Janeiro (GTRISC) prestará todo o apoio técnico ao CGSI.
§ 2º. Excepcionalmente, diante de grave incidente ou de grave ameaça que ponha em risco a segurança da informação, o GTRISC terá autonomia para determinar a realização de procedimentos emergenciais para a sua contenção e/ou recuperação.

Art. 19. O GTRISC é composto por representantes das áreas de Tecnologia da Informação e Comunicações, Segurança Institucional, Planejamento Estratégico e Comunicação Institucional e poderá solicitar apoio das áreas jurídica, pesquisas judiciárias, controle interno, dentre outras, para responder aos incidentes de segurança da informação de forma adequada e tempestiva.

Art. 20. O funcionamento do GTRISC será regulado por Ato Normativo próprio, devendo nele constar, no mínimo, os seguintes pontos:
I.definição da missão;
II.público-alvo;
III.modelo de implementação;
IV.canal de comunicação de incidentes de segurança; e
V.os serviços que serão prestados.

Seção VI
Da Gestão da Continuidade de Serviços Essenciais de TIC

Art. 21. A gestão da continuidade dos serviços essenciais de TIC é realizada por meio de processo definido de maneira formal, contendo as fases de análise de impacto e definição das estratégias pelos CGSI e CGTIC do TJERJ e, por fim, a elaboração de planos.
§ 1º. Os planos mencionados no caput deste artigo são:
I.o de Continuidade de serviços essenciais de TIC; e
II.o de Recuperação de serviços essenciais de TIC.
§ 2º. Os planos referidos no § 1º serão submetidos ao CGTIC.

Art. 22. A definição dos serviços essenciais será feita pelo CGTIC, com apoio técnico da DGTEC.

Art. 23. A unidade gestora de segurança da informação do PJERJ é responsável por estabelecer e manter o processo formal da gestão de continuidade de serviços essenciais de TIC, que deverá ser observado pelo responsável pelo funcionamento do serviço.

Art. 24. Os gestores dos ativos de informação são os responsáveis pela execução dos procedimentos técnicos constantes nos Planos de Continuidade e de Recuperação de serviços essenciais de TIC.

Art. 25. Os Planos de Continuidade e de Recuperação de serviços essenciais de TIC, após aprovados, serão exercitados e testados anualmente, e os resultados serão documentados de forma a garantir a sua efetividade.

Art. 26. Os Planos de Continuidade e de Recuperação de serviços essenciais de TIC serão revisados nas seguintes situações:
I.no mínimo, uma vez por ano;
II.em função dos resultados dos testes realizados; e
III.após alguma mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

Seção VII
Da Comunicação da Política de Segurança da Informação

Art. 27. O Plano de Comunicação Institucional do PJERJ deverá propor ações para a divulgação, sensibilização e prospecção da Política de Segurança da Informação (PSI) e dos seus instrumentos.
Parágrafo único. O Comitê Gestor de Segurança da Informação indicará Grupo Técnico que, juntamente com as áreas educacionais e de comunicação do PJERJ, elaborará e revisará anualmente o Plano de Comunicação Institucional do PJERJ.

CAPÍTULO III
DAS RESPONSABILIDADES
Seção I
Do Comitê Gestor de Segurança da Informação

Art. 28. Cabe ao CGSI, assessorado pela unidade gestora de segurança da informação, adotar as seguintes diretrizes para todas as unidades do PJERJ:
I.propor normas e procedimentos internos relativos à segurança da informação, em conformidade com as legislações existentes sobre o tema;
II.promover cultura de segurança da informação no PJERJ e implementar programas contínuos destinados à conscientização e capacitação do corpo técnico e dos usuários internos, bem como campanhas de divulgação para os usuários externos;
III.propor recursos necessários às ações de segurança da informação;
IV.constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
V.estabelecer critérios de classificação dos dados e das informações, com vistas à garantia dos níveis de segurança desejados e à normatização do acesso e uso das informações;
VI.garantir que os objetivos propostos no art. 4º desta Política sejam alcançados.

Seção II
Da Diretoria Geral de Tecnologia da Informação e Comunicação

Art. 29. Cabe à DGTEC implantar e gerenciar os controles relativos:
I.à gestão de todos os ativos de TIC, a fim de inventariar e identificar seus responsáveis;
II.à gestão da segurança das configurações da rede de comunicação de dados, para garantir a proteção das informações disponíveis na rede e a infraestrutura de suporte;
III.à gestão da segurança física dos ambientes computacionais, com o apoio da DGSEI, a fim de impedir e/ou repelir o acesso físico não autorizado e a ocorrência de danos e interferências nas instalações e informações digitais do órgão;
IV.à gestão das operações tecnológicas, a fim de garantir a operação segura dos recursos de processamento da informação;
V.à gestão das cópias e restauração de dados eletrônicos do PJERJ, para manter a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações e dos recursos de processamento de informação;
VI.ao uso dos recursos tecnológicos e aos acessos às informações e serviços em rede do PJERJ, a fim de garantir o acesso somente aos usuários autorizados a operar as informações acessadas;
VII.ao gerenciamento de incidentes de segurança da informação, com o apoio das demais unidades detentoras de ativos de segurança da informação, a fim de permitir o controle das fragilidades, vulnerabilidades e eventos que porventura coloquem em risco a segurança das informações e dos serviços do PJERJ;
VIII.às modificações nos recursos de processamento da informação e sistemas do PJERJ, considerando a criticidade dos sistemas e serviços essenciais.

Seção III
De todos os usuários internos

Art. 30. Cabe aos usuários internos:
I.conhecer e cumprir esta PSI e suas normas e procedimentos complementares;
II.seguir as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do órgão;
III.utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do PJERJ;
IV.comunicar ao órgão ou à autoridade diretamente superior, assim definida em ato normativo da presidência, quaisquer ocorrências ou suspeitas de incidentes de Segurança da Informação.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 31. A inobservância dos dispositivos constantes desta Política de Segurança da Informação pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 32. A Estrutura Normativa da Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro deve ser analisada criticamente a cada dois anos, ou quando ocorrerem mudanças, para assegurar a sua pertinência, adequação e eficácia.

Art. 33. A presente Resolução entra em vigor na data da sua publicação, revogadas as disposições em contrário.

Rio de Janeiro, 25 de fevereiro de 2019.

Desembargador CLAUDIO DE MELLO TAVARES
Presidente

Este texto não substitui o publicado no Diário Oficial.