PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DA PARAÍBA
GABINETE DA PRESIDÊNCIA

RESOLUÇÃO Nº 28 de 2020

Dispõe sobre a reformulação da Política de Segurança da Informação do Poder Judiciário do Estado da Paraíba

O **TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA**, no uso de suas atribuições constitucionais, legais e regimentais, e

CONSIDERANDO a Resolução nº 211/2015, do Conselho Nacional de Justiça (CNJ), que dispõe sobre os requisitos de nivelamento de Tecnologia da Informação no âmbito do Poder Judiciário, notadamente a elaboração e aplicação da política, gestão e processo de Segurança da Informação;

CONSIDERANDO a Instrução Normativa nº 54/2013, do CNJ, que dispõe sobre o uso dos recursos de tecnologia da informação e comunicação do CNJ e dá outras providências;

CONSIDERANDO a Norma ISO/IEC 27002:2005, traduzida pela Associação Brasileira de Normas Técnicas em ABNT NBR ISO/IEC 27002:2005, que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação em instituições de qualquer esfera;

CONSIDERANDO a Norma Complementar nº 17/IN01/DSIC/GSIPR, de 10 de abril de 2013, que estabelece diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF), bem como a ampliação do conhecimento de seus profissionais, a troca de experiências, a capacitação e consequente evolução da SIC nos órgãos e entidades da APF;

CONSIDERANDO a Lei 9.609/98 (Lei do Software), que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização e dá outras providências;

CONSIDERANDO a Resolução nº 35/2015, do Tribunal de Justiça da Paraíba (TJPB), que dispõe sobre o Plano Estratégico de Tecnologia da Informação no âmbito do Poder Judiciário, bem como, em seu Anexo I, define como um dos objetivos estratégicos a promoção da segurança da informação;

CONSIDERANDO a necessidade de estabelecer políticas, diretrizes e procedimentos de segurança da informação, tendo em vista a imprescindibilidade de fornecer um ambiente tecnológico com níveis aceitáveis de controle e confiabilidade, de forma a disponibilizar as informações necessárias aos processos de trabalho deste Tribunal com garantias de integridade, de disponibilidade, de confidencialidade, de autenticidade e de legalidade;

CONSIDERANDO a importância dos ativos de informação e a necessidade de regular a concessão de acessos aos sistemas informatizados e à rede de computadores; o uso da Internet e seus recursos; a utilização do serviço de correio eletrônico corporativo; bem como o controle, monitoramento e auditoria de segurança da informação no âmbito deste Tribunal;

CONSIDERANDO o dever do Estado de proteção das informações pessoais dos cidadãos.

RESOLVE, *ad referendum* do Tribunal Pleno:

Art. 1º Fica reformulada por esta Resolução a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário Estadual da Paraíba, à qual integram normas e procedimentos complementares editados por este Tribunal de Justiça, declarando o comprometimento e apoio da alta direção com a gestão da segurança da informação.

VISÃO GERAL E DEFINIÇÕES

Art. 2º A PSI é o conjunto de diretrizes, podendo incluir normas, procedimentos e políticas auxiliares, que regulamentam o uso adequado dos recursos de tecnologia da informação deste Tribunal, conferindo direitos, deveres e responsabilidades a todos quantos deles desfrutem,

devendo ser conhecida, compreendida e obedecida por todos os usuários dos recursos de tecnologia da informação do TJPB.

Art. 3º O uso adequado dos recursos de tecnologia da informação objetiva garantir a continuidade da prestação jurisdicional neste Tribunal.

Art. 4º A utilização dos recursos de tecnologia da informação do TJPB deve ser pautada nos seguintes princípios: celeridade, ética, segurança, responsabilidade e legalidade.

Art. 5º Para os efeitos desta Resolução, aplicam-se as seguintes definições:

I - **Segurança da Informação:** ações que visam a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A proteção da informação inclui a viabilização e a preservação da disponibilidade, da confidencialidade e da integridade desta e dos sistemas que a processam; adicionalmente, outras propriedades, tais como autenticidade, não repúdio e confiabilidade, podem também estar envolvidas [ISO/IEC 27002:2005];

II - **Recursos de Tecnologia da Informação do TJPB:** todo e qualquer dispositivo ou sistemas de *software* que processe informações dentro dos domínios administrativos do TJPB, incluindo computadores, *notebooks*, impressoras, rede de comunicação de dados, dispositivos de armazenamento de dados, serviços de armazenamento de dados via rede, serviço de e-mail institucional, entre outros;

III - **Comitê de Segurança da Informação (CSI)**: equipe multidisciplinar, subordinada à Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações de segurança da informação no TJPB;

IV - **Coordenador de Segurança da Informação:** é o responsável pelas ações técnico-científicas de segurança da informação no TJPB e pela Coordenação de Segurança da Informação;

V - **Ativo:** algo, tangível ou intangível, que tenha valor para a organização [ISO/IEC 13335-1:2004];

VI - **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

VII - **Evento de Segurança da Informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004];

VIII - **Incidente de Segurança da Informação:** é indicado por um evento simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
IX - **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO/IEC 13335-1:2004];
X - **Risco:** combinação da probabilidade de ocorrer um evento e de suas consequências [ABNT ISO/IEC Guia 73:2005];
XI - **Controle/Proteção/Contramedida:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;
XII - **Gestão de Riscos:** atividades coordenadas para direcionar e controlar uma organização no que se refere aos riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos [ABNT ISO/IEC 73:2005];
XIII - **Processo de Elaboração, Acompanhamento e Revisão da PSI:** processo de gestão de TI que visa instituir os procedimentos para elaboração, revisão e acompanhamento do cumprimento das diretrizes da PSI;
XIV - **Política de Mesa Limpa e tela protegida:** procedimento de controle da segurança no âmbito da mesa de trabalho do usuário, incluindo o bloqueio da tela do computador com uso de senha e o cuidado com os papéis deixados sobre a mesa;
XV – **Software com potenciais danosos para a Segurança da Informação**: são aqueles que, reconhecidamente, possuem funcionalidades específicas que podem ser utilizadas para quebra da privacidade, confidencialidade, integridade ou disponibilidade dos recursos de tecnologia da informação (e.g., *softwares* de varredura de vulnerabilidades, exploradores de vulnerabilidades (i.e, *exploits*), interceptadores de tráfego de rede (i.e, *sniffers*), *keyloggers, backdoors,* vírus, etc).

DA APROVAÇÃO E REVISÃO

Art. 6º Compete ao Tribunal Pleno a apreciação e aprovação da PSI do TJPB, autorizada, por este ato, a alteração desta em face de processo de acompanhamento e revisão, por ato do Comitê de Segurança da Informação (CSI), com comunicação ao Tribunal Pleno.

Art. 7º A PSI será submetida a revisões e análises críticas sistemáticas, com acompanhamento contínuo, a fim de mantê-la alinhada com os objetivos estratégicos institucionais e de tecnologia da informação.

Art. 8º O processo de elaboração, acompanhamento e revisão da PSI, devidamente instituído, definirá as atividades necessárias à sua consecução, obedecida a forma instituída no art. 6º desta Resolução.

DOS OBJETIVOS E DA ABRANGÊNCIA

Art. 9º A PSI do TJPB tem como objetivos:

I - Estabelecer diretrizes e controles para o tratamento dos riscos (i.e. reduzir, transferir, comunicar, aceitar ou evitar) referentes à violação da privacidade dos usuários, interrupções de serviços essenciais (definidos no Catálogo de Acordo de Nível de Serviços Essenciais de TI), revelação de informações sensíveis, modificações indevidas em ativos de informação (e.g, arquivos, inclusive em banco de dados, *softwares*, cabos de rede, impressoras, etc), perda de dados institucionais, destruição ou perda de recursos computacionais e roubo de propriedade intelectual;

II – informar e conscientizar os usuários sobre suas responsabilidades com relação ao uso adequado dos recursos de tecnologia informação do TJPB, tendo em vista incrementar e preservar os níveis de segurança de tais recursos;

III - promover a adoção de soluções de segurança integradas;

IV - declarar, formalmente, o compromisso deste Tribunal com a Segurança da Informação.

Art. 10. A PSI do Tribunal de Justiça da Paraíba se aplica às atividades executadas por todas as partes que utilizam os recursos de tecnologia da informação deste Tribunal, bem como a seus executores, incluindo magistrados, servidores, colaboradores, consultores, estagiários e prestadores de serviço que exercem atividades no âmbito do Poder Judiciário, internos ou externos, além de qualquer outra parte que esteja a desfrutar de acesso à infraestrutura ou informações regidas por esta Resolução.

Art. 11. Fica instituído o Comitê de Segurança da Informação (CSI) do TJPB, equipe multidisciplinar com atribuições de caráter consultivo, normativo e fiscalizador.

§ 1º O CSI, designado pela Presidência do TJPB, compor-se-á dos seguintes membros:

I – um Desembargador, que será seu presidente;

II – o juiz auxiliar da Presidência, integrante do Comitê de Governança de TI - CGovTI;

III – o juiz auxiliar da Corregedoria Geral de Justiça, integrante do Comitê de Governança de TI - CGovTI;

IV – o Diretor de Tecnologia da Informação;

V – o Coordenador de Segurança da Informação;

VI – o Gerente de Segurança Institucional e Militar;

VII - o Encarregado de Proteção de Dados Pessoais.

§ 2º O CSI será auxiliado pela Coordenação de Segurança da Informação e por outros integrantes da Diretoria de Tecnologia da Informação com aptidões técnico-científicas para atuação na área de segurança da informação.

Art. 12. Compete ao CSI do TJPB:

I – Propor a elaboração de normas e políticas auxiliares, especificando as obrigações e procedimentos particulares de acordo com as áreas de atuação, tais como:

a) Política de Backup;

b) Política de Senhas;

c) Regras para classificação das informações;

d) Plano de gestão de mudanças;

e) Plano de continuidade do negócio;

f) Política de uso do correio eletrônico;

g) Política de uso da Internet e redes sociais;

h) Processos de gestão e governança de TI voltados à segurança da informação.

II – Constituir grupo de trabalho incumbido de realizar análises e avaliações de riscos, em conformidade com a norma ABNT NBR ISO/IEC 27005:2008, que devem guiar as ações estratégicas de segurança da informação;

III - promover a cultura de segurança da informação;

IV – deliberar sobre revisões da PSI, consoante definido no art. 6º, desta Resolução;

V - definir e fiscalizar o uso de padrões de segurança da informação nas soluções tecnológicas desenvolvidas ou adquiridas pelo TJPB, sejam em nível de *hardware* ou de *software*;

VI - analisar e deliberar os pedidos de autorização para uso de ferramentas, soluções e serviços com potenciais danosos para a segurança da informação;

VII - constituir, quando necessário, grupos de trabalho para tratar de questões específicas sobre segurança da informação;

VIII – deliberar sobre a realização de auditorias em ativos e serviços de tecnologia da informação do TJPB quando houver suspeita de violações;

IX - propor normas e procedimentos internos relativos à segurança da informação, em conformidade com a legislação vigente;
X - realizar reuniões, com periodicidade mínima semestral, para acompanhamento dos resultados, das metas e processos de gestão relativos à segurança da informação;
XI – tratar os casos omissos ou divergências de interpretação dos artigos dessa PSI e dos seus documentos auxiliares.

Art. 13. O CSI coordenará a elaboração e execução de um Plano de Tratamento de Incidentes de Segurança da Informação, contemplando responsabilidades e procedimentos visando assegurar respostas rápidas, ordenadas e efetivas a incidentes de segurança da informação conforme o disposto no processo de gerenciamento de incidentes de SI devidamente instituído.

Art. 14. As deliberações do CSI serão tomadas pela maioria de seus membros.

Art. 15. Cabe a Coordenação de Segurança da Informação:
I – coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;
II - acompanhar as investigações e as avaliações dos danos decorrentes de violações de segurança da informação, conduzindo a equipe e os procedimentos técnicos adotados;
III - propor recursos necessários às ações de segurança da informação;
IV - realizar e acompanhar estudos de novas tecnologias de segurança da informação com potenciais de agregar valor aos recursos de tecnologia da informação do TJPB.

Art. 16. Os convênios e contratos firmados pelo TJPB que envolvam a utilização de recursos de tecnologia da informação devem observar o disposto nesta PSI.

DA GESTÃO DE CONTINUIDADE DO NEGÓCIO

Art. 17. O CSI deve coordenar a elaboração e execução de um Plano de Continuidade do Negócio, que tem como objetivo a manutenção ou recuperação dos serviços, assegurando, após a ocorrência de interrupções ou falhas em processos críticos, a disponibilidade da informação no nível requerido e na escala de tempo adequada.
Parágrafo único. O Plano de Continuidade do Negócio deve ser elaborado, testado e atualizado regularmente, de forma a certificar sua pertinência e efetividade, observando o processo de gerenciamento da continuidade dos serviços essenciais devidamente instituído.

Art. 18. A DITEC deve elaborar e executar procedimentos de *backup* dos dados dos sistemas, os quais devem ser submetidos a testes e análises críticas periódicas, bem como aprovados pelo CSI, observando o processo de backup e restore devidamente instituído.

Parágrafo único. Em caso de perdas devido a sinistros ou falhas de sistemas ou de segurança, o *backup* deve permitir a recuperação das informações em tempo hábil, de forma a reduzir os impactos nas atividades e serviços prestados pelo TJPB.

DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 19. As informações, sistemas e métodos gerados ou criados no âmbito deste Tribunal são de sua propriedade, independente da sua apresentação e armazenamento, e serão adequadamente protegidos e utilizados exclusivamente para os fins relacionados às atividades do Poder Judiciário;

Parágrafo único. Os conteúdos produzidos por terceiros para uso exclusivo do Tribunal serão sigilosos, sendo vedada sua reutilização em projetos para outrem sem prévia autorização do TJPB.

Art. 20. Toda informação gerada pelo Tribunal deve ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade, devendo ser elaborado um padrão de classificação da informação para o TJPB, contemplando os seguintes níveis:

I - **Pública**: é toda informação que pode ser acessada por usuários do TJPB, prestadores de serviços, fornecedores e o público em geral;

II - **Interna**: é a informação de interesse exclusivo dos usuários internos do TJPB. O acesso pelo público em geral deve ser evitado, sob risco de causar danos ao Tribunal;

III - **Restrita**: é toda informação que requer autorização de acesso explícita, indicada pelo nome do usuário, grupo ou área a que pertence. O acesso ou divulgação não autorizado deste tipo de informação pode gerar sérios danos ao TJPB, bem como acarretar em penalização nos termos da legislação vigente, sanções administrativas, civis e penais.

Parágrafo único. A Lei Geral de Proteção de Dados (LGPD) deverá ser observada para a classificação da informação.

Art. 21. O TJPB deve providenciar os recursos necessários para a devida proteção das informações e instalações no nível proporcional ao seu grau de sigilo.

DA AUDITORIA E CONFORMIDADE

Art. 22. A DITEC realizará o monitoramento do uso dos recursos de tecnologia da informação pelos usuários, incluindo os acessos realizados pelos administradores e operadores dos sistemas, observando o processo de gerenciamento de acessos instituído, validando a eficácia dos controles adotados e a respectiva conformidade com as diretrizes definidas nesta PSI e nas suas políticas auxiliares.

Parágrafo único. Os registros (*logs*) de auditoria, contendo atividades dos usuários no uso da Internet, do e-mail corporativo, do serviço de troca de mensagens (bate-papo) institucional, dos servidores de arquivos e do acesso aos sistemas e infraestrutura de TI serão produzidos e mantidos por um período de tempo definido pelo CSI, para fins de auxiliar em possíveis investigações e para verificação de conformidade.

Art. 23. Cabe ao CSI conceder e revogar o acesso de pessoas aos registros de auditoria que contenham dados que possam comprometer a privacidade dos usuários.

Parágrafo único. O acesso aos registros de auditoria deve ser controlado pelo CSI e monitorado continuamente, a fim de assegurar a proteção da privacidade dos usuários, observado o disposto nas políticas e normas internas relacionadas a LGPD.

Art. 24. O CSI poderá delegar à DITEC a concessão de acesso aos registros descritos no artigo anterior, bem como a outras informações com potencial de expor a privacidade dos usuários, uma vez observados os seguintes requisitos:

I – quando for necessário acessar dados contendo registros de eventos dos usuários, estes devem ser realizados por grupos de trabalho ou pessoas previamente autorizadas, seja pelo CSI ou pela DITEC;

II – os acessos que conduzirem à quebra da privacidade de usuários devem ser documentados e, quando solicitados, submetidos ao CSI;

III - O encarregado de proteção de dados pessoais deverá ser informado e consultado sobre qualquer ação inerente aos dados pessoais de usuários internos e externos.

Parágrafo único. É dispensável a documentação ou comunicação formal nos acessos aos registros de *logs* de sistemas que não tenham propósitos de identificar os usuários executores de ações específicas, mas apenas sua ocorrência.

Art. 25. Os mecanismos e atividades de monitoramento devem ser analisados criticamente, com frequência proporcional aos riscos envolvidos.

Art. 26. Os relatórios decorrentes das auditorias ordinárias realizadas pela DITEC serão encaminhados ao CSI.

Art. 27. Em caso de indícios de incidentes de segurança da informação, o CSI deverá ser informado para as providências cabíveis conforme o disposto nesta Resolução.

VIOLAÇÃO E SANÇÕES

Art. 28. A violação desta PSI, das suas normas ou dos procedimentos auxiliares de segurança da informação caracteriza infração funcional, a ser apurada em procedimento administrativo disciplinar, podendo resultar em penalização nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 29. Integram a presente Resolução as Normas Auxiliares e Controles constantes do Anexo I desta Resolução.

Art. 30. Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário e a Resolução nº 10, de 9 de março de 2016 deste Tribunal.

Tribunal de Justiça, em 03 de setembro de 2020.

MARCIO MURILO DA CUNHA RAMOS:4684231

Assinado de forma digital por MARCIO MURILO DA CUNHA RAMOS:4684231
Dados: 2020.09.03 10:22:20 -03'00'

Desembargador **MÁRCIO MURILO DA CUNHA RAMOS**

Presidente do Tribunal de Justiça da Paraíba

ANEXO I

Normas Auxiliares e Controles

DOS DEVERES E COMPETÊNCIAS GERAIS

Art. 1º É dever de todos os usuários dos ativos de tecnologia da informação do TJPB:

I - conhecer e cumprir a política de segurança da informação, bem como suas normas e políticas auxiliares que se apliquem às atividades do usuário;

II - utilizar os recursos de tecnologia da informação do TJPB apenas para os fins previstos institucionalmente;

III - comunicar à DITEC, imediatamente, qualquer ocorrência de eventos ou situações adversas, presença de fragilidades, vulnerabilidades, ameaças, entre outros, que tenham potencial de violar a política de segurança da informação e, consequentemente, causar impactos na área fim;

IV - seguir as orientações da DITEC quanto às boas práticas de segurança da informação, inclusive quanto à seleção e uso de senhas de acesso aos recursos de tecnologia da informação do TJPB;

V - adotar a política de mesa limpa e tela protegida, conforme definição disponível nesta PSI;

VI - firmar o Termo de Responsabilidade e Confidencialidade das informações.

Parágrafo único. Notificações ou denúncias de eventos, incidentes, ameaças, vulnerabilidades ou qualquer outro assunto relacionado à segurança da informação, devem ser comunicados à DITEC.

Art. 2º É vedado a todos os usuários dos recursos de tecnologia da informação do TJPB:

I – divulgar, compartilhar e transmitir informações institucionais a pessoas ou entidades que não possuam o devido nível de autorização, incluindo, mas não se limitando, a publicação de informações em redes sociais, fórum online ou *blogs*;

II – utilizar-se de qualquer meio com potencial de violar os mecanismos de proteção da rede de dados, dos sistemas, da privacidade dos usuários ou de informações institucionais sigilosas, o que inclui, mas não se limita, ao uso de *softwares* de varredura de vulnerabilidades, exploradores de vulnerabilidades (i.e, *exploits*), interceptadores de tráfego de rede (i.e, *sniffers*), *keyloggers, backdoors,* entre outros. O uso de tais *softwares* é restrito às equipes de Tecnologia da Informação (TI) no cumprimento das suas atribuições, quando houver necessidade explícita, desde que detenham a devida autorização para tal;

III – baixar ou instalar qualquer tipo de *software* ilegal (pirata) ou não autorizado pelo TJPB. A aquisição (*download*) e instalação de *softwares* caberão exclusivamente aos servidores de TI que detenham as devidas permissões;

IV – salvar/armazenar nos diretórios/pastas da rede do TJPB ou nas estações de trabalho ou em outros dispositivos institucionais de armazenamento de dados, arquivos não relacionados com a atividade fim deste Tribunal ou que violem leis de direitos autorais, a exemplo de músicas, filmes, imagens, entre outros;

V – divulgar suas senhas de acesso aos sistemas, servidores de aplicação e banco de dados do TJPB ou utilizar a senha de outrem, ainda que com consentimento das partes.

Art. 3º É responsabilidade da Diretoria de Tecnologia da Informação (DITEC):

I – emitir, remover ou suspender credenciais de acesso mediante solicitação formal do Diretor/Gestor do usuário;

II - remover ou suspender credenciais de acesso quando identificado um cenário com risco iminente à segurança da informação;

III - adicionar, remover ou bloquear direitos de acesso dos usuários que mudem de cargo ou função, ou daqueles que deixem o Tribunal; quando formalmente comunicado pela Diretoria de Gestão de Pessoas;

IV - conceder o nível/permissões de acesso de acordo com as necessidades ou atribuições dos usuários;

V - realizar análise crítica dos direitos de acesso dos usuários com periodicidade máxima semestral, considerando, ainda, as informações disponíveis no sistema de recursos humanos;

VI – apoiar as campanhas de conscientização de segurança da informação, fornecendo os recursos necessários;

VII - promover a segurança da informação;

VIII – assegurar a proteção dos dados e da privacidade dos usuários;

IX – implantar controles de monitoramento, com finalidade de detectar divergências entre as normas que integram a política de segurança da informação e os respectivos registros de eventos monitorados;

X – estabelecer e implementar quotas de armazenamento de dados por usuários e/ou unidades de trabalho, seja no uso do servidor de arquivos, e-mail institucional ou outros, de acordo com a necessidade de trabalho e disponibilidade dos recursos.

Art. 4º É responsabilidade dos Gestores das Unidades Judiciais ou Administrativas:

I - conhecer, divulgar, cumprir e estimular o cumprimento da PSI;
II – Assegurar a observância da PSI no âmbito de sua unidade, bem como comunicar, de imediato, ao CSI, qualquer irregularidade constatada, para as providências;
III – solicitar formalmente à DITEC a concessão de permissões de acesso aos usuários sob sua supervisão, sempre com base no binômio: necessidade e mínimo de permissões;
IV – comunicar formalmente à Diretoria de Gestão de Pessoas e à Diretoria de Tecnologia da Informação, qualquer ocorrência de mudança de lotação, afastamento, retorno ou desligamento dos seus integrantes;
V – manter o zelo, em nível físico e lógico, pelos recursos de tecnologia da informação sob sua unidade de atuação;
VI - identificar o uso inadequado dos ativos e adotar as medidas apropriadas.

Art. 5º É responsabilidade da Diretoria de Gestão de Pessoas:
I – manter atualizadas as informações do sistema recursos humanos, priorizando aquelas que se referem a desligamentos, retornos, afastamentos, ou qualquer outra mudança no quadro funcional do TJPB e órgãos subordinados;
II – apoiar as campanhas de conscientização de segurança da informação;
III – Incluir o Termo de Responsabilidade e Confidencialidade como documento obrigatório para o exercício dos cargos e funções, bem como proceder com a guarda segura e adequada dos documentos assinados, conforme estabelecido pela tabela de temporalidade vigente.

DO CONTROLE DE ACESSO

Art. 6º O acesso aos recursos de tecnologia da informação do TJPB é permitido mediante identificação e autenticação do usuário, por meio de senha pessoal e intransferível.
§ 1º As senhas de identificação devem observar os seguintes requisitos:
I – tamanho mínimo de oito caracteres;
II – utilização de letras, números e caracteres especiais;
III – exigência de alteração em intervalos não superiores a doze meses.
§ 2º Caso haja tentativas fracassadas de acesso, com fornecimento de senhas incorretas, o *login* do usuário poderá ser bloqueado à critério da DITEC.

Art. 7º As solicitações de concessão, suspensão ou remoção definitiva ou temporária de direitos de acesso aos recursos de tecnologia da informação do TJPB deverão ser encaminhadas à

Central de Atendimento (GEATE) pelo Diretor/Gestor do usuário, sem prejuízos às demais obrigações perante a Gerência de Controle e Acompanhamento.

§ 1º Para as demais solicitações relativas a demandas de TI (e.g, requisição de serviços, suporte, reparos, etc) o próprio usuário poderá contatar a Gerência de Atendimento e Suporte - GEATE através de chamado.

§ 2º A DITEC manterá o registro, em meio digital, de todas as solicitações de suporte recebidas e os respectivos procedimentos de atendimento adotados.

Art. 8º As concessões ou modificações de direitos/permissões de acesso aos recursos de tecnologia da informação do TJPB para Desembargadores ou Juízes devem ser solicitadas pelo próprio interessado.

Art. 9º Os prestadores de serviços terceirizados poderão desfrutar de acesso aos recursos de tecnologia da informação do TJPB, devendo o gestor da unidade em que o prestador de serviço estiver lotado enviar requerimento fundamentado para a DITEC, constando informações sobre o tempo de validade/duração do acesso, sua justificativa, respeitada a duração do estágio ou contrato.

Art. 10. Em caso de perda da senha de acesso aos recursos de tecnologia da informação do TJPB, o usuário deverá comunicar ao seu Diretor/Gestor para que este solicite à GEATE a geração de uma nova senha, na forma estabelecida no Art. 2º desta política auxiliar.

Art. 11. A senha fornecida pela DITEC é temporária e deve ser alterada no momento do primeiro acesso ao sistema.

Art. 12. Fica vedada a concessão, retirada ou modificações dos direitos/permissões de acesso quando solicitados apenas verbalmente ou por aplicativos de mensagem, seja por magistrados, servidores ou qualquer outro usuário, exceto em situações de risco iminente e irreparável aos negócios ou à segurança das informações, com posterior registro formal à DITEC.

Art. 13. A Gerência de Controle e Acompanhamento informará à DITEC, por meio eletrônico, os afastamentos definitivos, ou temporários por período superior a 60 (sessenta) dias, para que sejam asseguradas as medidas restritivas de acesso aos recursos de tecnologia da informação do TJPB.

DO ARMAZENAMENTO DE DADOS

Art. 14. Cada usuário e/ou unidades de trabalho dispõe de quota limitada de armazenamento de dados, a ser estabelecida e implementada pela DITEC de acordo com as necessidades e disponibilidade de recursos.

Parágrafo único. O servidor de armazenamento *web,* acessível através do endereço eletrônico *drive.tjpb.jus.br*, poderá ser usado para armazenamento e compartilhamento de arquivos de trabalho.

Art. 15. Os arquivos de trabalho devem ser armazenados na estrutura de diretórios do servidor de arquivos disponível na rede de dados.

§ 1º A cópia de segurança (*backup*) dos arquivos armazenados no disco rígido das estações de trabalho (i.e., microcomputadores e notebooks) é da responsabilidade do usuário.

DO USO DO E-MAIL INSTITUCIONAL

Art. 16. Entende-se por e-mail institucional a conta criada no domínio *@tjpb.jus.br* ou outros domínios que venham a ser adotados pelo TJPB.

Parágrafo Único. As regras e padrões para utilização do e-mail institucional (correio eletrônico) tais como: conceitos e definições, cadastro de acesso, utilização dos recursos e gestão do serviço estão normatizadas no Ato da Presidência nº 42/2019 e devem ser observados em complementação à esta Política.

Art. 17. A mensagem de e-mail é considerada informação institucional, podendo o remetente ser responsabilizado pelo seu conteúdo.

Art. 18. O acesso às mensagens de e-mail está restrito ao remetente e ao(s) destinatário(s), sendo estas invioláveis, salvo por determinação administrativa autorizada pelo CSI, ou por motivo de segurança institucional.