ESTADO DA PARAÍBA
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

Publicado no Diário da Justiça
Em 17 de 03 de 2016
GERÊNCIA DE PRIMEIRO GRAU
Brunno José Lins Lima Cavalcante
Gerência de Primeiro Grau
Supervisor

RESOLUÇÃO nº 10 , 9 de março de 2016.

Dispõe sobre os requisitos de nivelamento de Tecnologia da Informação no âmbito do Poder Judiciário, bem como define a Segurança da Informação como uma das atividades estratégicas para os órgãos do Poder Judiciário.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA**, no exercício de suas atribuições,

CONSIDERANDO a Resolução nº 90/2009, do Conselho Nacional de Justiça (CNJ), que dispõe sobre os requisitos de nivelamento de Tecnologia da Informação no âmbito do Poder Judiciário, bem como define a Segurança da Informação como uma das atividades estratégicas para os órgãos do Poder Judiciário;

CONSIDERANDO a Resolução nº 99/2009, do Conselho Nacional de Justiça (CNJ), que institui o Planejamento Estratégico de Tecnologia da Informação e Comunicação (TIC);

CONSIDERANDO a Instrução Normativa nº 54, do Conselho Nacional de Justiça (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 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece diretrizes para a elaboração da Política de Segurança da Informação e Comunicação nos órgãos e entidades da Administração Pública Federal;

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 o decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

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 necessidade de estabelecer políticas, diretrizes e procedimentos de segurança da informação, tendo em vista oferecer 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 do Tribunal e;

CONSIDERANDO o dever do Estado de proteção das informações pessoais dos cidadãos, resolve:

Art. 1º Fica instituída 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.

CAPÍTULO I
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. Essa deve, assim, 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 visa garantir a continuidade da prestação jurisdicional deste 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 efeito 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 conduzir e fiscalizar as ações de segurança da informação no TJPB;

IV - **Gestor de Segurança da Informação:** é o responsável pelas ações técnico-científicas de segurança da informação no TJPB e pela coordenação do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação;

V - **Ativo:** qualquer coisa, 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 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 - **Diretriz:** descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas [ISO/IEC 13335-1:2004].

XIV - **Política de Mesa Limpa e tela protegida:** procedimento de controle da segurança no âmbito da mesa de trabalho do funcionário, incluindo o bloqueio da tela do computador com uso de senha e o cuidado com os papeis 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).

CAPÍTULO III
DA APROVAÇÃO E REVISÃO

Art. 6º A PSI é um documento que requer apreciação e aprovação pelo Tribunal Pleno do TJPB.

Art. 7º A PSI deve ser submetida a revisões e análises críticas sistemáticas, com periodicidade máxima anual, a fim de mantê-la alinhada com os objetivos estratégicos do TJPB. A condução das revisões é de responsabilidade do Comitê de Segurança da Informação (CSI).

Art. 8º As atualizações na PSI ou nos seus documentos auxiliares devem ser submetidas à aprovação da Presidência deste Tribunal.

CAPÍTULO IV
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 (e.g, ejus, pje, vep, rh, etc), revelação de informações sensíveis, modificações indevidas em ativos de informação (e.g, arquivos, *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 da 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.

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. Estão incluídos os 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 e composta por pessoal do quadro permanente deste Tribunal.

§ 1º O CSI, designado pela Presidência do TJPB, compor-se-á dos seguintes membros, em observância ao disposto no Art. 11:

I – um Desembargador, integrante da Comissão de Segurança do TJPB;
II – um juiz auxiliar da Presidência;
III – um juiz auxiliar da Corregedoria Geral de Justiça;
IV – Diretor de Tecnologia da Informação;
V – Gestor de Segurança da Informação;
VI – Diretor Administrativo;
VII – Diretor de Economia e Finanças;
VIII – Diretor de Gestão de Pessoas;
IX – um representante do Comitê de Magistrados para Tecnologia da Informação (CMTI);
X – Diretor de Processo Administrativo;
XI – um membro da Comissão de Segurança;
XII – Gerente de Suporte de Tecnologia de Informação;
XIII – Diretor de Segurança Institucional;
XIV – Um membro da Associação dos Magistrados da Paraíba (AMPB), indicado pela Presidência da Entidade.

§ 2º O CSI deve ser, ainda, auxiliado por três integrantes da Diretoria de Tecnologia da Informação, os quais devem comportar aptidões técnico-científicas para atuarem na área de segurança da informação.

§ 3º O CSI será presidido pelo Desembargador.

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;

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 – revisar a PSI consoante ao definido no Art. 6º e encaminhá-la à

Presidência para fins de aprovação;

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 com potenciais danosos para a segurança da informação;

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

VIII – constituir e autorizar grupos de trabalho capacitados para realizar auditorias em recursos 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 máxima semestral, para acompanhamento dos resultados e das metas relativas 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.

Art. 14. As decisões do CSI subordinar-se-ão à Presidência do TJPB.

Art. 15. Cabe à Presidência nomear um Gestor de Segurança da Informação, pessoa do quadro permanente deste Tribunal, a quem caberá:

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.

CAPÍTULO V
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 à 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 testado e atualizado regularmente, de forma a certificar sua pertinência e efetividade.

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.

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.

CAPÍTULO VI
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 ínsitas do Poder Judiciário;

Parágrafo único. Quanto a conteúdos produzidos por terceiros para uso exclusivo do Tribunal, ficam seus criadores obrigados ao sigilo permanente de tais, sendo vedada sua reutilização em projetos para outrem.

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 desse tipo de informação pode gerar sérios danos ao TJPB, bem como acarretar em penalização nos termos da legislação vigente, sanções administrativas, civis e penais.

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.

CAPÍTULO VII
DA AUDITORIA E CONFORMIDADE

Art. 22. A fim de checar a eficácia dos controles adotados e a respectiva

conformidade para com as diretrizes definidas nesta PSI e nas suas políticas auxiliares, a DITEC realizará o monitoramento do uso dos recursos de tecnologia da informação do TJPB por parte dos usuários, incluindo os acessos realizados pelos administradores e operadores dos sistemas.

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 acordado, 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.

Art. 24. Pode o CSI delegar à DITEC a concessão de acesso a tais registros, bem como a outras informações com potenciais de expor a privacidade dos usuários, uma vez que se observem 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 culminem na quebra da privacidade de usuários devem ser documentados e, quando solicitados, submetidos ao CSI.

Parágrafo único. Em se tratando de registros de *logs* de sistemas, que não tenham propósitos de identificar os usuários executores de ações específicas, mas apenas a ocorrência destas últimas, faz-se desnecessário a documentação ou comunicação formal.

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 específicos, a chefia imediata ou superior comunicará ao CSI para as providências devidas.

CAPÍTULO VIII
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, sendo cabíveis 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 a partir da data de sua publicação.

Art. 31. Ficam revogadas as disposições em contrário.

Desembargador **MARCOS CAVALCANTI DE ALBUQUERQUE**
Presidente do Tribunal de Justiça do Estado da Paraíba

Publicado no Diário da Justiça
Em 17 de 03 de 2016
GERÊNCIA DE PRIMEIRO GRAU

Brunno José Lins Lima Cavalcante
Gerência de Primeiro Grau
Supervisor

ANEXO 01 – 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 um 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, podem ser comunicados por meio do envio de mensagem para o endereço eletrônico: seguranca@tjpb.jus.br.

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

I – divulgar, compartilhar ou 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, e 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 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 ou 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 Diretores/Gestores:

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 a 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 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 corretivas 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 nos 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 e números;

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 a 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, seguindo as orientações da Cartilha de Atendimento (http://www.tjpb.jus.br/wp-content/uploads/Cartilha_DITEC.pdf), 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 GEATE, seguindo as orientações da Cartilha de Atendimento.

§ 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. No requerimento deve constar o tempo de validade/duração do acesso, acompanhado de sua justificativa, respeitando o limite superior igual à 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 esse solicite a GEATE a geração de uma nova senha, na forma estabelecida no Art. 2º desta política auxiliar.

Parágrafo único. A recuperação de senha por meio da GEATE só será atendida quando não houver a opção de recuperação automática da senha no próprio recurso de tecnologia da informação (e.g, no sistema de Recursos Humanos), ou quando esta opção estiver inoperante.

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, seja por magistrados, servidores ou qualquer outro usuário, exceto em situações de risco iminente e irreparável aos negócios ou à segurança das informações, o que ensejará posterior justificativa, em expediente direcionado à citada Diretoria.

Art. 13 A Gerência de Controle e Acompanhamento informará a GEATE, 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.

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

Parágrafo único. 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.

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

Art. 18 É vedado o envio não autorizado de qualquer informação sigilosa ou material com conteúdo difamatório, obsceno, ameaçador, ofensivo, preconceituoso, libidinoso, pornográfico, profano ou ilegal, cabendo ao usuário sanções administrativas conforme o contrato de sigilo assinado pelo usuário e as leis vigentes.

Art. 19 O e-mail institucional não deverá ser utilizado para fins particulares, de recreação ou para envio de mensagens com tamanho total superior a 10MB (10 *Mega Bytes*), incluindo os seus respectivos anexos.

Art. 20 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.

Art. 21 Quando se tratar de movimentação de pessoa que indique desligamento definitivo com o Poder Judiciário, após um prazo de 60 dias contados da data de desligamento, fica a DITEC autorizada a proceder com a exclusão segura de qualquer dado armazenado na caixa de e-mail do usuário, no servidor de arquivos e nos discos dos computadores por ele outrora utilizados.

Art. 22 Ao usuário é permitida a participação em listas de discussão que contemplem assuntos relacionados com suas atribuições ou aos interesses do TJPB.

Art. 23 A regra de denominação do endereço de correio eletrônico institucional será, preferencialmente, o prenome do usuário, seguido por um ponto final, seguido pelo sobrenome, em letras minúsculas, sem acentos, cedilhas ou caracteres especiais, acrescido do sufixo "@tjpb.jus.br".

DO ACESSO À INTERNET E ÀS REDES SOCIAIS

Art. 24 Para os efeitos desta Resolução, entende-se por redes sociais os ambientes virtuais que têm como objetivo reunir pessoas, empresas ou instituições, os chamados membros, que uma vez inscritos, podem expor seu perfil com dados pessoais, textos, mensagens e vídeos, além de interagir com outros membros, gerando listas de amigos e comunidades. Inclui-se neste escopo o *facebook, twitter* e outros.

Art. 25 Perfis institucionais mantidos nas redes sociais deverão ser administrados e gerenciados por servidores ocupantes de cargo efetivo ou comissionados ou terceirizados, sob a responsabilidade de um gestor, ou por pessoa designada pela Presidência do TJPB.

Parágrafo único. O acesso a redes sociais pelos demais usuários através dos recursos de tecnologia da informação do TJPB está expressamente proibido, exceto quando estiver diretamente relacionado com as atribuições do servidor, o que demandará a análise e aprovação pelo CSI.

Art. 26 Fica proibida a divulgação ou compartilhamento indevido de informações da área administrativa em listas de discussão, comunidades de relacionamento, salas de bate-papo, comunicadores instantâneos ou qualquer outra

tecnologia correlata.

Art. 27 A DITEC manterá controles de monitoramento dos meta-dados relacionados com os acessos às páginas de Internet que possam oferecer riscos à segurança da informação.

Art. 28 A DITEC fica autorizada a bloquear os acessos a sites de Internet que contenham conteúdo pornográfico, racista ou que possa ser ofensivo à moral e aos bons costumes.

Art. 29 O acesso a sites de notícias é tolerável, desde que esta prática não seja abusiva, não comprometa o desempenho da rede e não influencie o bom andamento dos trabalhos.

Parágrafo único. Cabe a DITEC disciplinar estes acessos, bem como removê-los a qualquer tempo, sem notificação prévia, a fim de preservar e garantir o bom uso de seus recursos.

Art. 30 Os problemas ocorridos durante o acesso aos serviços de Internet ou Intranet deverão ser comunicados a GEATE, vinculada à DITEC, mediante abertura de chamado técnico por meio do endereço eletrônico: http://suporte.tjpb.jus.br.

Art. 31 É vedado o uso da Internet nas seguintes situações:

I - acesso a sites não relacionados com as atividades/atribuições do usuário, principalmente àqueles de conteúdo pornográfico, racista, que faça apologia ao uso de drogas, sites de jogos e àqueles que tenham objetivo de anonimizar a navegação;

II – para *downloads* de programas não autorizados, jogos, filmes, músicas, e outros tipos de conteúdos que não sejam de interesse institucional;

III - participação em jogos ou salas de bate papo *on-line*, salvo neste último caso para atividades relacionadas ao Poder Judiciário do Estado da Paraíba.

Art. 32 Caso seja constatado o descumprimento do inciso II do Art. 31, os conteúdos poderão ser excluídos dos equipamentos nos quais estiverem armazenados, sem comunicação prévia ao responsável, além de serem adotadas as devidas sanções administrativas.

DO ACESSO À REDE SEM FIO

Art. 33 O Tribunal de Justiça do Estado da Paraíba provê essa modalidade de conexão à rede como uma facilidade de acesso a seus serviços, e não oferece garantias de ubiquidade no âmbito de suas instalações físicas nem de que as conexões estarão sempre disponíveis. Desta forma, o uso de conexões às redes sem fio disponibilizadas não se constitui em um direito do usuário.

Art. 34 O acesso através de uma rede sem fio pública e aberta será concedido apenas aos sites e sistemas publicados na Internet quais sejam atualmente essenciais aos usuários do Poder Judiciário, mediante aceitação de política de utilização específica. Estão incluídos os sites e sistemas das seguintes fontes:

I - órgãos judiciários brasileiros;

II – órgãos e entidades da Administração Pública;

III - principais provedores de e-mail do mundo;

Art. 35 O acesso aos recursos de intranet, incluindo acesso a sistemas e arquivos internos, bem como acesso amplo a Internet, serão concedidos apenas a magistrados e servidores ocupantes de cargo efetivo ou comissionados ou terceirizados, mediante cadastro prévio e procedimento de autenticação com *login* e senha, em consonância com a Resolução nº 614/2013 da Agência Nacional de Telecomunicações.

Art. 36 O usuário estará sujeito a obedecer à legislação e às regulamentações vigentes e aplicáveis ao uso de redes de computadores e da Internet. Não será tolerado o uso da rede sem fio para realizar ataques ou qualquer atividade ilegal contra outros usuários ou dispositivos da mesma rede ou da Internet.

Art. 37 O Tribunal de Justiça do Estado da Paraíba não assume responsabilidade sobre a segurança do dispositivo utilizado para realizar a conexão à rede sem fio, bem como dos dados armazenados no mesmo. O usuário aceita todos os riscos associados à disponibilização e transmissão de seus dados enquanto estiver conectado na rede sem fio.