TJAM/DVTIC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

2018/2020

AV. André Araújo S/N – Aleixo – CEP: 69.060-000
Fone: (092) 2129-6832 / 2129-6767 - E-mail: tj@tjam.jus.br

Histórico de Versões

VERSÃO	DESCRIÇÃO	RESPONSÁVEL
1.0	Versão 2018/2020 Politica de Segurança da Informação (PSI)	Dir. Thiago Facundo

Histórico de Inclusões e Alterações

DATA	INCLUSÃO / ALTERAÇÃO	MODIFICADO POR:
02/09/2019	Modificação do Layout do documento	Humberto F. Junior

Sumário

I – DA FINALIDADE

1 – A presente norma, desenvolvida pela Divisão de Tecnologia da Informação e Comunicação (DVTIC) tem por finalidade o estabelecimento das regras gerais de utilização dos recursos do ambiente de Tecnologia da Informação (TI), com vistas à proteção contra ameaças internas e externas, com base nos princípios da disponibilidade, integridade, confidencialidade e autenticidade.

II – DA FUNDAMENTAÇÃO LEGAL

2 – A presente Norma foi elaborada de acordo com os seguintes instrumentos legais:

a) Constituição Federal – CF – 1988 – art. 37, § 6º - dispõe sobre a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, estabelece obediência aos princípios de legalidade, da impessoalidade, da moralidade, da publicidade e da eficiência.

b) Lei nº 8027, de 12 de Abril de 1990 – dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providencias.

c) Lei nº 12.527, de 18 de novembro de 2011 - 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, altera a Lei nº 8.112, de 11 de dezembro de 1990, revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências;

d) Norma ABNT ISO/IEC 27002:2005, de 31 agosto de 2005, denominada Código de prática para a gestão da Segurança da Informação;

e) Norma ABNT ISO/IEC 27001:2006, de 31 de março de 2006, denominada Sistemas de Gestão de Segurança da Informação - Requisitos;

f) Norma ABNT ISO/IEC 27005:2011, de 17 de novembro de 2011, denominada Gestão de Riscos de Segurança da Informação;

g) Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008 - Metodologia de Gestão de Segurança da Informação e Comunicações

h) Norma Complementar nº 04/IN01/DSIC/GSIPR e seu anexo, de 14 de agosto de 2009 - Diretrizes para o Processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;

i) Norma Complementar nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009 - estabelece Diretrizes para a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

j) Norma Complementar nº 07/IN01/DSIC/GSIPR, de 06 de maio de 2010 - estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

k) Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 - estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

l) Norma Complementar nº 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 - estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

III – DOS CONCEITOS E SIGLAS

3 - Para os efeitos desta Norma considera-se:

a) **Administrador de rede** - pessoa responsável pela administração e pela manutenção dos recursos da infraestrutura de TI do tribunal;

b) **Ameaça** - causa potencial de um incidente indesejado que possa resultar em danos e prejuízos ou que possa afetar a imagem do Tribunal de Justiça do Amazonas;

c) **Ativo** - elemento integrante do processo que manipula e processa a informação e possui valor para o Tribunal de Justiça do Amazonas;

d) **Ativo de TI (recurso computacional)** - além da própria informação eletrônica, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

e) **Autenticidade** - garantia de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, sistema, órgão ou entidade;

f) **Backup (cópia de segurança)** - cópia de um arquivo em conjunto de dados mantidos por questão de segurança no original ou cópia principal;

g) **Confidencialidade** - garantia de que a informação não esteja disponível ou seja revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

h) **Conta administrativa** - conta ou login de acesso que possui privilégio de administração sendo, necessariamente, vinculada a uma estação de trabalho, não podendo ser utilizada em uma rede corporativa;

i) **Conta com privilégio de administração** - conta ou login de acesso que possui privilégio de administração vinculada, exclusivamente, a uma única estação de trabalho, usualmente àquela utilizada pelo empregado;

j) **Conta de correio eletrônico** - espaço disponibilizado nos servidores do Tribunal de Justiça do Amazonas para utilização dos recursos e funcionalidades do correio eletrônico;

k) **Conta de identificação ou conta de usuário** - código identificador do usuário nos ativos de TI do Tribunal de Justiça do estado do Amazonas;

l) **Conta de serviço** - conta ou login de acesso que possui privilégio de administração, livre de vinculação a uma estação de trabalho, em todos os casos em que for utilizada;

m) **Conta genérica** - conta corporativa utilizada por mais de um indivíduo, onde não é possível a identificação singular do usuário que a utiliza;

n) **Controle de acesso** - restrição de acesso a espaços físicos ou sistemas de informação somente a pessoas autorizadas;

o) **Serviço de correio eletrônico** - possibilita a troca de mensagens, controle de calendário, contato e tarefas, por meio da rede de computadores do Tribunal de Justiça do Amazonas;

p) **Dado** - qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, a compreensão de determinado fato ou situação;

q) **Disponibilidade** - garantia de que a informação esteja acessível e utilizável sob demanda por pessoa física ou determinado sistema, órgão ou entidade;

r) **Dispositivo de segurança física** - utilizado para proteger fisicamente um equipamento contra furtos ou acesso indevido;

s) **Dispositivo móvel de armazenamento** - suporte de mídia digital (pen drives, CDs, DVDs e outros dispositivos similares) usado para o transporte físico de informações;

t) **Download** - processo de cópia de arquivos provenientes de outro computador, geralmente por intermédio da Internet;

u) **DVTIC** - Divisão de Tecnologia da Informação e Comunicação;

v) **Endereço de correio eletrônico (e-mail)** - conta de correio eletrônico para um usuário, uma unidade organizacional ou lotação do Tribunal de Justiça do Amazonas;

w) **Equipamento móvel** - equipamento que pode ser transportado e utilizado em diferentes lugares. Não são fixos, portanto, não dependem de um lugar específico para serem utilizados. Como exemplo: smartphone, notebook e tablet;

x) **Equipamento periférico** - equipamento acessório que seja ligado ao computador. São exemplos: impressora, mouse, teclado, dentre outros.

y) **Estação de trabalho** - conjunto de computador e equipamentos periféricos disponíveis para utilização pelo usuário da rede de computadores do Tribunal de Justiça do Amazonas;

z) **Hardware** - parte física do computador, ou seja, o conjunto de componentes eletrônicos de uma máquina ou sistema;

aa) **HD (hard disk)** - também conhecido como disco rígido, é responsável por armazenar dados e sistemas de informação. Pode localizar-se internamente no computador ou ser portátil;

bb) **Impacto** - tamanho do prejuízo, de propriedade mensurável ou abstrata, causado por determinada ameaça;

cc) **Incidente de segurança** - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores;

dd) **Informação** - dado organizado e inserido em um contexto, de maneira a propiciar determinado retorno ao manipulador, permitindo a escolha entre vários caminhos que possam levar a um resultado;

ee) **Informação sensível** - toda informação corporativa que, por sua natureza, deve ser de conhecimento privativo de pessoa ou grupo diretamente envolvido com o assunto;

ff) **Integridade** - garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

gg) **Log** - registro de eventos relevantes em um sistema computacional;

hh) **Logon** - processo de identificação e autenticação do usuário na rede de computadores, sistemas ou estações de trabalho do Tribunal de Justiça do Amazonas;

ii) **Logon interativo** - acesso local a uma estação de trabalho, sem necessidade de uma rede de computadores disponível;

jj) **Mantenedor** - pessoa responsável pelos serviços de instalação, configuração e manutenção dos ativos de TI;

kk) **Não repúdio** - capacidade de prevenir a rejeição ou repúdio por parte do remetente ou do receptor de uma comunicação ou acesso a um sistema de informação;

ll) **Patch** - programa utilizado para atualizar ou corrigir um software;

mm) **Prestador de serviço** - todo aquele que exerce qualquer tipo de atividade no âmbito do tribunal e que não seja empregado do Quadro de Cargos Regulares do mesmo, servidor contratado para cargo em comissão ou requisitado de outros órgãos. Enquadram-se neste conceito consultores externos, estagiários, colaboradores, auditores externos, menores aprendizes, dentre outros;

nn) **Privilégio de acesso** - vantagem de acesso ou permissão especial concedida a um ou mais usuários, com exclusão de outros e contra a regra geral;

oo) **Rede de computadores** - dois ou mais computadores e outros dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos;

pp) **Responsabilidade** - obrigação de responder pelos próprios atos e de justificar as razões desses atos;

qq) **Risco** - medida que indica a probabilidade de concretização de determinada ameaça, combinada com os impactos que ela trará para o Tribunal de Justiça do Amazonas;

rr) **Segurança da informação** - visa à proteção de ativos que contêm informações, preservando sua disponibilidade, integridade, confidencialidade e autenticidade;

ss) **Senha de acesso** - utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser;

tt) **Serviço de chamado para o usuário (Helpdesk)** - atendimento aos usuários dos ativos de TI do Tribunal de Justiça do Estado do Amazonas, a fim de resolver solicitações e problemas;

uu) **Sessão de trabalho** - período em que o usuário, utilizando a sua conta de identificação, encontra-se conectado à rede de computadores do tribunal ou a uma estação de trabalho;

vv) **Sistema de informação** - conjunto de meios de comunicação, computadores e redes de computadores, dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

ww) **Software** - programa, geralmente armazenado no computador, utilizado para operar ou executar uma tarefa;

xx) **Termo de responsabilidade** - instrumento legal para assegurar que os usuários estão cientes de suas responsabilidades e obrigações ante aos recursos computacionais disponibilizados;

yy) **TI** - Tecnologia da Informação;

zz) **VPN (Virtual Private Network)** - uma rede de comunicação privada, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet);

aaa) **Vulnerabilidade** - falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por uma pessoa mal intencionada, resulta na violação da segurança de um computador.

IV – DO ESCOPO

4 – As regras gerais de utilização dos recursos do ambiente de tecnologia da informação referem-se:

a) Aos aspectos estratégicos e organizacionais, preparando a base para elaboração de documentos normativos do tribunal de justiça no âmbito de TI;

b) À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços ofertados pela Área de Tecnologia da Informação do tribunal.

V – DAS RESPONSABILIDADES

5 – **Do usuário:**

a) Utilizar de forma responsável sua(s) conta(s) de identificação na rede de computadores do Tribunal de Justiça do Estado do Amazonas;

b) b) Manter sigilo e não fazer uso privado de informações geradas, adquiridas ou utilizadas pelo tribunal, às quais tenha tido acesso no exercício de suas atividades;

c) Manter sigilo de suas senhas de acesso aos recursos, sistemas e serviços da rede de computadores;

d) Manter seguras as informações manuseadas no âmbito da rede de computadores do Tribunal de justiça do Amazonas;

e) Observar que as informações armazenadas na estação de trabalho e nos demais dispositivos móveis utilizados para o desempenho de suas funções serão de sua inteira responsabilidade, não havendo previsão de backup realizado pela DVTIC para tais unidades;

f) Não emitir opiniões anônimas na Internet e na Intranet fazendo referência às atividades desempenhadas no Tribunal de Justiça do Estado do Amazonas (correio eletrônico, bate-papo e demais canais de comunicação);

g) Garantir o encerramento da sessão de trabalho ou seu bloqueio por senha ao afastar-se da estação, ainda que temporariamente;

h) Manter sua estação de trabalho em perfeitas condições de uso, na forma que lhe foi entregue;

i) Informar qualquer evento que possa comprometer a segurança dos ativos de TI do Tribunal de Justiça do Amazonas;

j) Informar à DVTIC a existência de informações sensíveis na estação de trabalho, quando necessária a manutenção do equipamento;

k) Manter a guarda, a segurança e a integridade dos ativos físicos e lógicos que estejam sob sua responsabilidade ;

l) Responder por todos os atos realizados por meio de seu identificador, tais como login de rede, endereço de correio eletrônico, usuário de sistema e assinatura digital;

m) Observar e acatar as recomendações para a utilização segura dos ativos de TI e, em caso de dúvidas ou problemas, contatar à DVTIC através do sistema de Helpdesk;

n) Utilizar os sistemas e serviços de informação somente para os fins legais;

o) Manter, sob qualquer circunstância, o sigilo de informações sensíveis para do Tribunal de Justiça do Amazonas;

p) Informar imediatamente quaisquer eventos, fragilidades ou ameaças ao ambiente computacional, suspeitos ou plenamente identificados, no sistema de Helpdesk;

5.1 – É vedado ao usuário:

a) Utilizar, copiar ou armazenar programas de computador ou qualquer outro material que viole a lei de direitos autorais;

b) Tomar ação própria, sob qualquer circunstância, no intuito de conter um incidente de segurança dos ativos de TI;

c) Promover atividades comerciais próprias ou de terceiros, incluindo oferta de serviços ou produtos;

d) Enviar mensagens não institucionais para grupos ou pessoas que não as solicitaram ou autorizaram;

e) Enviar mensagens cuja veracidade não possa ser confirmada;

f) Enviar mensagens que, de alguma forma, violem a legislação vigente;

g) Contribuir com a continuidade de correntes de mensagens eletrônicas;

h) Ler ou tentar ler mensagens de outras pessoas sem autorização expressa;

i) Executar jogos pela internet ou pela rede de computadores do Tribunal de Justiça do Amazonas;

j) Executar atividades pessoais que interfiram em suas responsabilidades no trabalho;

k) Respeitar as regras e limitações de acesso aos sites disciplinadas na presente política.

6 – Das Chefias Imediatas:

a) Zelar pela aplicação da presente política junto aos seus subordinados bem como reportar, de imediato, à DVTIC, qualquer incidente que venha a conflitar com as normas estabelecidas neste documento.

b) b) Solicitar, via e-mail, análise para a concessão/exclusão de privilégios de acesso na rede de dados do Tribunal de Justiça aos usuários que a necessitarem e estiverem sob sua supervisão ou para si, bem como, responsabilizar-se por tal solicitação até a ocasião de seu cancelamento;

7 – Da Divisão de Tecnologia da Informação e Comunicação:

a) Assegurar a disponibilidade e a integridade dos recursos de tecnologia da informação do tribunal;

b) Registrar todos os acessos ou tentativas realizados da Internet para a rede de computadores interna do tribunal e definir, inclusive, os prazos de armazenamento e guarda desses registros;

c) Promover ações de divulgação e conscientização dos usuários para a correta utilização dos ativos de TI do tribunal;

d) Realizar auditoria nos recursos computacionais e serviços prestados pela área de TI;

e) Verificar periodicamente possíveis ocorrências de descumprimento desta Norma;

f) Manter os sistemas e as ferramentas de segurança corretamente instalados e operacionais;

g) Manter os equipamentos e sistemas em conformidade;

h) Projetar, avaliar e implantar processos com o intuito de mitigar as vulnerabilidades existentes no parque computacional do tribunal;

i) Disciplinar os procedimentos necessários à execução de tarefas administrativas nos equipamentos servidores, estações de trabalho e dispositivos de rede.

8 – Da Divisão de Pessoal:

a) Informar mensalmente à DVTIC a movimentação de usuários (admissão, demissão, transferência, afastamentos e outros) para fins do controle de acesso físico, lógico e no âmbito dos sistemas institucionais.

VI – DOS PROCEDIMENTOS

9 – Das contas e senhas:

a) As contas de usuários da rede de computadores só serão criadas, após a comunicação da Divisão de Pessoal à DVTIC, para usuários em atividade no Tribunal de Justiça do Amazonas, ressalvados os casos especiais em função da necessidade do serviço;

b) As contas de usuários caracterizados como prestadores de serviço devem ter prazo de utilização determinado, o qual deverá ser informado pela Divisão de Pessoal, e poderá ser estendido em casos especiais, em função da necessidade do serviço;

c) O usuário perderá a concessão de acesso à rede local segundo determinações legais e normativos vigentes;

d) O servidor do quadro, cedido ou afastado no interesse do serviço para realização de cursos ou trabalhos externos vinculados às suas atividades, poderá manter sua conta de rede e e-mail, mediante solicitação formal à DVTIC.

10 – Das contas administrativas e contas de serviço:

a) Só devem ter permissão para serem utilizadas nos equipamentos, servidores, estações de trabalho e dispositivos de rede para as quais foram criadas;

b) Os procedimentos de criação, manutenção e remoção de contas administrativas e de serviço serão disciplinados pela DVTIC.

c) O uso de contas administrativas e contas de serviço são de inteira responsabilidade do usuário.

d) A senha de acesso deve ser elaborada e modificada por cada servidor de acordo com as diretrizes estabelecidas pela DVTIC.

e) As senhas de acessos dos usuários devem ser individuais, secretas, intransferíveis e armazenadas de forma segura.

f) Não é permitida a concessão de privilégio de administração do equipamento ou estação de trabalho.

11 – Do uso do Hardware:

g) É vedada a alteração da configuração de hardware da estação de trabalho, salvo mediante autorização expressa da DVTIC;

h) O acesso físico às salas técnicas de TI deverão seguir orientações do setor responsável e seu acesso limitado a pessoas autorizadas;

i) Os equipamentos que contêm informações importantes, sensíveis ou críticas para o Tribunal devem estar fisicamente trancados;

j) Os recursos de tecnologia da informação pertencentes ao Tribunal de justiça somente podem ser retirados do local de origem sob autorização prévia da Direção da DVTIC;

12 – Do uso de Software:

a) As estações de trabalho devem ser configuradas de acordo com os padrões estabelecidos pela DVTIC, sendo vedada sua alteração;

b) Os equipamentos servidores de rede e estações de trabalho do tribunal trabalharão exclusivamente com softwares previamente homologados pela DVTIC;

c) A identificação de software não homologado na estação de trabalho ensejará na remoção do mesmo, sem aviso prévio, pela equipe da DVTIC;

d) A instalação e a configuração de software adquirido pelo tribunal na estação de trabalho ou em equipamentos servidores de rede somente devem ser realizadas pelo suporte de DVTIC, as quais são responsáveis pela guarda das mídias e por eventuais desinstalações, quando necessárias;

e) As atualizações de software e sua abrangência dar-se-ão por critério definido exclusivamente pela DVTIC, bem como o estabelecimento de cronograma para tal.

13 – Do uso de equipamentos móveis:

a) O notebook que constituir patrimônio do tribunal deverá ser conectado periodicamente à rede interna para fins de atualizações de segurança;

b) Não é permitido o uso de dispositivos móveis particulares conectados à rede de computadores, com ou sem fio. Casos específicos serão analisados pela DVTIC após solicitação formal;

c) As mídias de armazenamento de informações devem ser examinadas pelos técnicos de suporte de Tecnologia da Informação antes de ser descartadas, para garantir que foram devidamente destruídas, apagadas ou sobre gravadas, evitando que recuperações futuras sejam realizadas.

14 – Do armazenamento de informações:

a) As informações e os dados corporativos ficarão disponíveis em áreas de armazenamento em equipamentos servidores da rede administrada pela DVTIC;

b) As informações e dados corporativos armazenados em equipamentos servidores, administrados pela Tecnologia da Informação, devem possuir cópias de segurança atualizadas;

c) Não é permitido armazenar arquivos pessoais em equipamentos servidores de rede local ;

d) A DVTIC disciplina a realização de cópias de segurança de informações e de dados corporativos;

e) Outras regras, procedimentos e disponibilização para utilização das áreas de armazenamento da rede e cópias de segurança seguem normativos vigentes e suas exceções deverão ser encaminhadas à DVTIC.

VII – DO ACESSO

15 – Do uso da rede de dados interna:

f) a) Os dados e as informações produzidos, armazenados ou trafegados no ambiente de TI do Tribunal de justiça podem ser de natureza pública ou corporativa;

g) b) As informações corporativas devem ser protegidas contra acesso não autorizado durante todo o seu ciclo de vida, incluindo a criação, o manuseio, o armazenamento, o transporte e o descarte;

h) c) As informações sensíveis, tramitadas em meio eletrônico, deverão observar os mesmos princípios daquelas tramitadas em meio físico;

i) d) Não é permitido o acesso a rede de computadores do tribunal de justiça por equipamentos externos que não façam parte do patrimônio da instituição ou que não estejam oficialmente homologados. Exceções deverão ser enviadas a gerência de tecnologia de informação, em caráter de análise.

j) e) Não é permitido aos usuários a instalação de equipamentos de rede, tais como switches, roteadores ou qualquer outo ativo que possa comprometer a integridade da rede lógica.

16 – Do uso da Internet:

a) O acesso à Internet ocorrerá exclusivamente por meio dos recursos providos pela DVTIC, a qual poderá autorizar, excepcionalmente, e em caso de necessidade técnica ou operacional, o uso de conexões externas específicas, após solicitação formal e análise;

b) Todo e qualquer acesso à Internet será franqueado apenas após identificação em ferramenta de registro e controle, respeitando-se o nível de acesso estabelecido para o usuário;

c) Em caso de suspeita de incidente de segurança e/ou abuso capaz de comprometer a utilização dos recursos pelo TJAM, a DVTIC poderá bloquear o acesso à internet de usuários e estações de trabalho da rede;

d) A DVTIC poderá estabelecer lista de sítios acessíveis por todos os usuários da rede;

e) O usuário estará sujeito a penalidades de acordo com a gravidade do acesso indevido.

17 – Do uso do correio eletrônico:

a) As contas do correio eletrônico corporativo do tribunal são classificadas em caixas postais de uso individual ou lotação;

b) A DVTIC manterá cópias atualizadas das contas do correio eletrônico do tribunal;

c) O uso da caixa de correio deverá restringir-se ao uso profissional e o acesso indevido poderá ser penalizado;

d) Outras dúvidas quanto ao uso de e-mail deverão ser encaminhados via e-mail a DVTIC.

18 – Do acesso remoto:

a) O acesso remoto no âmbito do tribunal deverá ser solicitado exclusivamente por e-mail contendo dados e justificativa;

b) É de responsabilidade da DVTIC a homologação de software próprio para conexão, a configuração dos sistemas de controle de acesso, a inclusão, a alteração e a remoção de grupos ou usuários nos sistemas de administração corporativos e qualquer outra atividade correlacionada com o processo de disponibilização e administração da VPN no âmbito do tribunal;

c) O cancelamento do acesso à VPN deve ocorrer por meio da formalização no sistema de atendimento ao usuário, quando por solicitação do próprio usuário ou interesse de seu gestor imediato. A DVTIC, no intuito de conservar e proteger a segurança no âmbito do tribunal poderá efetuar o cancelamento dos serviços sem aviso prévio;

VIII – DO CONTROLE

19 – Do filtro de conteúdo:

a) A DVTIC poderá utilizar software específico de filtro de conteúdo para bloqueio do acesso a sítios e serviços considerados inadequados ao acesso corporativo, de acordo com sua exclusiva avaliação;

b) O download de arquivos poderá ser interrompido ou bloqueado, conforme critérios definidos pela DVTIC;

c) A DVTIC estabelece os níveis de acesso à internet, os quais serão monitorados diariamente, visando minimizar a ocorrência de ameaças e comprometimento de performance da rede lógica e/ ou acesso à internet.

20 – Dos perfis de acesso:

a) A DVTIC irá fazer o gerenciamento dos perfis de acesso conforme o cargo e função exercida por cada grupo de servidores, diretores, coordenadores e magistrados.

21 – Do monitoramento e auditoria de segurança:

a) O uso dos recursos de tecnologia da informação no tribunal serão monitorados e registrados;

b) O monitoramento será por ferramentas de segurança que permitam a identificação do motivo do bloqueio, nos casos de acesso negado, o aviso em tempo real ao administrador de rede, em caso de suspeita de quebra de segurança e a realização de mapeamento automático da topologia de rede, na detecção de equipamentos defeituosos;

c) Sistemas e serviços computacionais vulneráveis ou críticos devem receber nível de proteção adicional, como criptografia e armazenamento seguro, de acordo com sua classificação;

d) Os sistemas e serviços computacionais deverão possuir mecanismos de sincronização de seus relógios para efeito de consistência na correlação de eventos; e) Sistemas que contêm informações sensíveis ou críticas para o tribunal devem ser monitorados e auditados periodicamente.

22 – Da conformidade:

a) Toda e qualquer informação gerada, adquirida, utilizada ou custodiada pelo tribunal é considerado seu patrimônio e só poderá ser divulgada mediante prévia autorização da autoridade competente;

b) O uso de quaisquer recursos ou infraestrutura, física ou lógica, no âmbito do tribunal, terá destinação exclusiva em benefício desta, sendo integralmente proibido o emprego para fins pessoais ou em benefício de terceiros;

c) O conteúdo das comunicações, os arquivos, as bases de dados e as mensagens, armazenados, transitados ou gerados pelo uso de ativos de TI do tribunal é considerado propriedade da administração Pública;

d) As informações corporativas para acesso ou manuseio fora das dependências do tribunal ou entre suas unidades, independentemente do meio ou mídia, devem estar protegidas por senhas de acesso ou por mecanismo de criptografia de forma a garantir integridade e confidencialidade;

e) A DVTIC poderá aplicar, aos usuários, pesquisas sobre segurança em TI, com o objetivo de avaliar o nível de conhecimento e a conformidade com Normas de sistema da informação vigentes;

f) A suspensão dos privilégios de um determinado usuário poderá ocorrer por razões ligadas à segurança física e lógica, ou ainda, por razões disciplinares; estando os envolvidos sujeitos à sanções disciplinares.

g) As estações de trabalho, os computadores portáteis e os servidores deverão estar atualizados e aplicados com todos os patches de correção e de segurança fornecidos pelo fabricante e possuir antivírus homologado pela DVTIC instalado e atualizado.

IX – DAS DISPOSIÇÕES FINAIS

23- Todo e qualquer desenvolvimento, aquisição, manutenção e documentação de sistemas deve ser composto dos requisitos mínimos de segurança da informação e alinhado aos padrões da ISSO/IEC 15408-1:2009 e da ABNT NBR ISO/IEC 27002:2005 e dos normativos internos existentes.

24 – A violação desta e de outras normas correlacionadas poderá resultar na suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais e em penas e sanções legais previstas nas legislações vigentes ou procedimentos administrativos formal pelo tribunal.

25 – Os casos omissos nesta Norma deverão ser tratados pela DVTIC.

26 – Esta Norma entra em vigor na data de sua efetivação.