PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
GABINETE DA PRESIDÊNCIA

PORTARIA Nº1107/2014-GP

A Excelentíssima Senhora Desembargadora LUZIA NADJA GUIMARÃES NASCIMENTO, Presidente do Tribunal de Justiça do Estado do Pará, no uso de suas atribuições legais, etc.

CONSIDERANDO o que dispõe a Portaria nº4618/2013-GP (DJ nº.5391-19/11/13) sobre o Normativo 00.01 – Manual de Procedimentos para Elaboração de Normativos Técnicos Administrativos;

CONSIDERANDO o ato decisório da Presidência, proferido nos Expedientes formalizados pela Secretaria de Informática sob o Protocolo – SIGA_DOC nº.PAMEM201402287A, nº.PAMEM201402279A, nº.PAMEM201402284A, nº.PAMEM201402283A, nº.PAMEM201402281A, nº.PAMEM201402282A, nº.PAMEM201402280A, nº.PAMEM201400426A, nº.PAMEM201400320A;

RESOLVE:

Art.1º ATRIBUIR eficácia interna de procedimento padrão aos Manuais a seguir especificados e que constam nos Anexos desta Portaria:

I – Normativo Segurança no Uso da Intranet;
II – Normativo Política de Segurança da Informação;
III – Normativo Estação de Trabalho – Padronização, Segurança e Administração;
IV – Normativo Correio Eletrônico – Padrão e Regras de Utilização;
V – Normativo Antivirus: Instalação, Configuração, Utilização e Atualização;
VI – Normativo Correio Eletrônico – Gestão Tecnológica;
VII – Normativo Utilização da Internet;
VIII – Normativo Publicação (Deploy) de Aplicações;
IX – Normativo Videoconferência.

Art.2º Esta Portaria entra em vigor na data de sua publicação.

Belém, 09 de abril de 2014.

Desembargadora **LUZIA NADJA GUIMARÃES NASCIMENTO**
Presidente

PUBLICAÇÃO
Publicado na Edição nº **5479**
Diário de Justiça de **11/04/2014**

I - SEGURANÇA NO USO DA INTRANET

1. ASSUNTO/OBJETIVO

Estabelecer padrões de segurança que permitam garantir a integridade, confidencialidade e disponibilidade de informações no ambiente Intranet dentro dos sites corporativos.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Garantir a segurança no uso dos recursos disponíveis no ambiente de Intranet do TJPA.

3. UNIDADE GESTORA

Secretaria de Informática – Coordenadoria de Suporte Técnico – Serviço de Segurança e Sistemas Básicos.

4. PÚBLICO ALVO

Todo o Tribunal

5. RELAÇÃO COM OUTROS NORMATIVOS

Política de Segurança da Informação

6. REGULAMENTAÇÃO UTILIZADA

NBR ISO 27002/2006.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

AMBIENTE INTRANET – Face à grande dispersão da Intranet no TJPA e para facilitar a padronização e o seu respectivo entendimento, a presente norma utiliza os termos "ambiente Intranet" e "Intranet" com um significado mais restrito, pois, faz referência apenas aos recursos existentes nos sites institucionais do TJPA;

APLICAÇÃO INTRANET – Conjunto de programas computacionais pelos quais são disponibilizadas informações na Intranet;

ÁREA ADMINISTRADORA DOS SERVIDORES – É o setor que se ocupa da instalação, operação, supervisão e manutenção dos servidores utilizados no ambiente Intranet;

ÁREA GESTORA DA INFORMAÇÃO – É o setor dono da informação ou seu usuário principal, responsável por sua classificação e publicação;

BACKUP – Cópia de segurança de um arquivo ou conjunto de dados, guardada para futura consulta, recuperação ou referência, caso o arquivo ou conjunto de dados original seja corrompido ou destruído;

BIA (Business Impact Analisys) – Metodologia que permite avaliar os impactos de uma interrupção significativa nos processos de negócios do TJPA, por meio da aplicação de questionário;

E-MAIL – Canal de comunicação, fazendo uso de correio-eletrônico, que possibilita a troca de informações entre usuários;

CONFIDENCIALIDADE – Princípio de segurança da informação através do qual é estabelecido o conceito de garantia de acesso à informação somente ao(s) usuário(s) autorizado(s);

CONSOLE DE SERVIDORES – Ferramentas que oferecem recursos para administração remota dos servidores;

CRIPTOGRAFIA – Sistemas matemáticos cujo objetivo é resolver os problemas de segurança da informação que dizem respeito à privacidade e autenticidade;

DISPONIBILIDADE – Princípio de segurança da informação por intermédio do qual é garantido o acesso do usuário à informação, sempre que necessário;

ESTAÇÃO DE TRABALHO INTRANET – Microcomputador conectado à rede do TJPA, por intermédio do qual o usuário pode ter acesso aos diversos serviços e informações disponibilizados na Intranet, respeitando-se os perfis de acesso definidos pela área gestora da informação;

FICUS – FICHA DE CADASTRAMENTO DE USUÁRIO – Formulário destinado a formalizar a solicitação de cadastramento de usuário para acesso aos recursos computacionais do TJPA;

FICUS/E – FICHA DE CADASTRAMENTO DE USUÁRIO EXTERNO – Formulário destinado a formalizar a solicitação de cadastramento de usuário externo para acesso aos recursos computacionais do TJPA;

FUNCIONALIDADE – Conjunto de atributos que demonstram a existência de funções e suas propriedades especificadas, ou seja, características do software que atendem a determinados propósitos;

INTEGRIDADE - Princípio de segurança da informação por intermédio do qual é garantida a informação conforme disponibilizada pelo seu gestor;

INTRANET – Rede privada de computadores que se baseia nos padrões e conceitos de comunicação de dados da rede Internet;

LOGON ou LOGIN – É o processo de identificação e autenticação ao qual um usuário é submetido antes de conseguir acesso ao sistema, software ou aplicativo;

MÍDIA MAGNÉTICA – Qualquer artefato tecnológico que possibilite o armazenamento magnético de dados digitais (por exemplo: PENDRIVE, Memory Cards, IPOD, máquinas fotográficas, dispositivos de armazenamento MP3, entre outros);

PLANO DE CONTINGÊNCIA - Conjunto de medidas que visam manter em funcionamento o ambiente operacional tecnológico sem interrupções em caso de sinistro;

SERVIÇO DE LOG - Registro de eventos cujo objetivo é possibilitar a monitoração dos recursos, bem como a auditoria do ambiente tecnológico do TJPA;

SSSB - SERVIÇO DE SEGURANÇA E SISTEMAS BÁSICOS – Setor responsável pela normatização na área de segurança da informação e pertencente ao organograma da Secretaria de Informática do TJPA, dentro da Coordenadoria de Suporte Técnico.

SESSÃO DE TRABALHO - Intervalo de tempo em que o usuário permanece conectado e apto a interagir com a Rede TJPA;

TCP/IP – TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL – Protocolo padrão de comunicação utilizado pela rede Internet;
USUÁRIO – É o Magistrado ou Servidor do TJPA, prestador de serviços, usuário fábrica, estagiário, menor aprendiz ou usuário externo autorizado a ter acesso aos recursos computacionais do TJPA;
USUÁRIO FÁBRICA – Empregado de empresa terceirizada de TI, na modalidade Fábrica de Software, que acessa o ambiente de Desenvolvimento do TJPA, por meio da EXTRANET TJPA, para elaborar projetos e sistemas contratados pelo TJPA.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

Não se aplica.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

9.1.1 Homologar recursos tecnológicos utilizados no ambiente Intranet.
9.1.2 Estabelecer critérios e indicadores de avaliação de desempenho do ambiente Intranet.
9.1.3 Definir e revisar a configuração padrão das plataformas e ativos utilizados no ambiente Intranet.
9.1.4 Estabelecer critérios e indicadores de avaliação de desempenho do ambiente Intranet.
9.1.5 Garantir a integridade, confidencialidade e disponibilidade da informação contida nos arquivos e diretórios do ambiente Intranet, protegendo-a contra ataques ou invasões internos e externos.
9.1.6 Definir procedimentos a serem executados em situações de contingência.
9.1.7 Definir padrões de monitoração e auditoria do ambiente.
9.1.8 Definir perfil de segurança dos usuários operadores ou administradores para estabelecer o nível de acesso que estes têm aos servidores da Intranet.
9.1.9 Implementar e monitorar a configuração padrão utilizada no ambiente Intranet.
9.1.10 Estabelecer critérios e indicadores de avaliação de desempenho do ambiente Intranet.
9.1.11 Definir padrões de monitoração e auditoria do ambiente, sob a ótica de segurança da informação.
9.1.12 Definir e revisar as recomendações de segurança nos padrões utilizados no ambiente Intranet.
9.1.13 Definir procedimentos padrões e ferramentas que garantam a integridade, confidencialidade e disponibilidade da informação contida nos arquivos e diretórios do ambiente Intranet, protegendo-a contra ataques ou invasões internos e externos.
9.1.14 Homologar soluções de segurança para o ambiente Intranet.
9.1.15 Orientar a área gestora da informação quanto à exigência da trilha de auditoria durante a definição dos requisitos das aplicações Intranet.
9.1.16 Definir rotina de backup para os servidores e serviços sob sua responsabilidade no ambiente Intranet de modo que possam garantir a execução dos planos de contingência em casos de sinistro.
9.1.17 Realizar e armazenar o backup em local adequado e fazer testes de restauração periodicamente.
9.1.18 Realizar backup dos arquivos de configuração e de log.
9.1.19 Realizar tarefa contínua de monitoração do ambiente Intranet quanto à sua operacionalidade em conformidade com padrões e segurança.
9.1.20 Fazer manutenção preventiva dos equipamentos do ambiente Intranet.
9.1.21 Controlar o acesso físico às salas dos servidores.
9.1.22 Excluir do cadastro usuários definitivamente desligados do TJPA.

9.2 CHEFIA DA UNIDADE

9.2.1 Solicitar inclusão e/ou exclusão de permissão de acesso à Intranet aos empregados, estagiários e prestadores de serviço lotados em sua respectiva unidade.
9.2.2 Indicar o perfil de acesso de usuários internos e externos, quando da solicitação de cadastramento.
9.2.3 Solicitar exclusão de usuários definitivamente desligados do TJPA.

9.3 ÁREA GESTORA DA INFORMAÇÃO

9.3.1 Definir perfil de segurança dos usuários para estabelecer o nível de acesso que estes têm à informação sob sua gestão.
9.3.1.1 A definição deve ser conforme descrito no normativo de classificação da informação, por meio da matriz de acesso às informações sob sua gestão, que leva em consideração: cargo e lotação.
9.3.2 Em caso de aplicações WEB, publicar informação via WWW de acordo com o padrão gráfico definido pela Área de Comunicação Social.
9.3.3 Definir a classificação da informação sob sua gestão.
9.3.4 Definir o prazo de validade e de retenção das informações sob sua gestão.
9.3.5 Autorizar o acesso às informações sob sua gestão.

9.4 USUÁRIO

9.4.1 Estar devidamente capacitado para utilizar plenamente a Intranet.
9.4.2 Tratar as informações a que tem acesso conforme o seu nível de classificação.
9.4.3 Comunicar ao SSSB as ocorrências que afetem a integridade, confidencialidade e disponibilidade das informações do ambiente Intranet.
9.4.4 Elaborar a sua senha, cumprindo o padrão estabelecido no Normativo de Concessão de Acesso Lógico aos Recursos Computacionais do TJPA.
9.4.5 Manter o caráter confidencial, pessoal e intransferível da senha fornecida, a qual não deve ser compartilhada com outras pessoas.
9.4.6 Encerrar sua sessão de trabalho ou bloqueá-la ao se afastar da estação de trabalho.

9.4.7 Executar apenas as funções específicas que lhe foram concedidas pela autorização de acesso, de acordo com o perfil que lhe é atribuído.
9.4.8 Dar conhecimento à chefia imediata de qualquer infração verificada aos procedimentos estabelecidos e à normatização vigente.
9.4.9 Utilizar a informação e recursos somente para os fins previstos pelo gestor da informação e em estrita observância às normas estabelecidas.
9.4.10 Utilizar a Intranet segundo os normativos vigentes.

10. PROCEDIMENTOS

10.1. INFORMAÇÃO NA INTRANET DO TJPA

10.1.1 As informações disponibilizadas na Intranet devem ser classificadas de acordo com os níveis de sigilo presentes no Manual Normativo sobre CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO.
10.1.1.1 A área gestora da informação é responsável pela classificação das informações por ela disponibilizadas na Intranet.
10.1.2 A área gestora da informação deve definir o tempo que a informação deve permanecer disponível para acesso na Intranet.
10.1.2.1 Após o prazo definido no item acima, a informação deve ser tratada de acordo com a classificação que lhe foi atribuída, tanto no caso de descarte como armazenamento.
10.1.3 A atualização da informação disponibilizada na Intranet deve ser feita pela área gestora da informação.
10.1.4 As ocorrências detectadas que afetem a disponibilidade, confidencialidade e integridade das informações do ambiente Intranet devem ser comunicadas imediatamente ao Serviço de Segurança e Sistemas Básicos (SSSB) da Secretaria de Informática do TJPA.
10.1.5 O descarte de material que contiver informações não consideradas públicas deve ser feito de modo a impedir a recuperação total ou parcial das informações nele contidas.
10.1.6 Em situações de contingência, devem ser observados os procedimentos definidos pelo SSSB para o atendimento das necessidades tecnológicas e operacionais.
10.1.7 O SSSB, durante o levantamento de requisitos das aplicações Intranet, deve sempre orientar a área gestora da informação quanto à exigência da implementação de trilha de auditoria de acordo com o descrito no Manual Normativo associado a esta atividade.
10.1.8 As informações classificadas como CONFIDENCIAL e CONFIDENCIAL RESTRITA devem possuir rotina de backup.
10.1.8.1 O gestor deve definir o prazo de retenção do backup.

10.2 BACKUP DOS SERVIDORES

10.2.1 A área administradora dos servidores deve realizar o backup dos dados do ambiente Intranet e armazená-los em local adequado.
10.2.2 A área administradora dos servidores deve fazer o backup dos arquivos de log e da configuração do ambiente Intranet com periodicidade e prazo de retenção que garantam a continuidade dos serviços.
10.2.3 As aplicações e bases de dados do ambiente Intranet, classificadas como críticas pela área gestora e que constem com a mesma classificação no Programa de Continuidade de Negócios do TJPA, após a realização do BIA, devem possuir duas cópias backup idênticas armazenadas em localizações geográficas distintas, cuja distância em linha reta seja de no mínimo 6,5 km.
10.2.3.1 Demais aplicações e bases de dados devem manter rotina de backup com uma única fita armazenada em local geográfico distinto do site corporativo, cuja distância em linha reta seja de no mínimo 6,5 km.

10.3 CONFIGURAÇÃO DO AMBIENTE

10.3.1 A configuração dos servidores deve seguir os padrões definidos pelo SSSB, de acordo com a plataforma implementada.
10.3.2 A documentação de configuração do ambiente Intranet deve ser classificada como Confidencial com acesso exclusivo às equipes que necessitam acesso para desempenho de suas tarefas e mantida atualizada e guardada em local seguro.
10.3.3 Devem ser observadas as recomendações de segurança publicadas pelo SSSB.

10.4 INFRA-ESTRUTURA

10.4.1 O ambiente Intranet deve possuir recursos de monitoração de falhas, performance e segurança.
10.4.2 A monitoração do ambiente deve ser feita rotineiramente pela área responsável pelo monitoramento que se reportará à área administradora dos servidores de forma a permitir a identificação, correção e registro imediato dos problemas e ações tomadas para sua solução.
10.4.3 Os critérios e indicadores de avaliação de performance do ambiente Intranet devem ser estabelecidos pela SSSB.
10.4.4 Os servidores devem estar localizados em ambiente seguro, salvaguardados de quaisquer intempéries que venham a afetar a disponibilidade dos serviços da Intranet.
10.4.5 A paralisação para manutenção de serviços da Intranet deve ocorrer mediante notificação aos respectivos usuários, com pelo menos 24 horas de antecedência.
10.4.6 A console dos servidores do ambiente Intranet deve ser de uso exclusivo dos administradores e operadores.
10.4.7 Os empregados que fazem parte da administração, operação e monitoração do ambiente Intranet devem ser plenamente capacitados para execução de suas tarefas.
10.4.8 O ambiente Intranet deve possuir um plano de contingência específico, de forma a garantir a disponibilidade dos serviços.

10.4.8.1 O plano de contingência deverá estar em consonância com o definido no Programa de Continuidade de Negócios do TJPA.
10.4.9 A limpeza da sala dos servidores do ambiente Intranet deve ser feita por pessoal autorizado, devidamente instruído para tal, e deve ocorrer sob a supervisão direta e presencial de um responsável designado e em horários estabelecidos pela área administradora dos servidores.
10.4.9.1 Deve ser registrado o acesso realizado à sala dos servidores para execução dos serviços de limpeza, bem como do responsável designado para acompanhar.
10.4.10 As rotinas de manutenção preventiva dos equipamentos que compõem o ambiente Intranet devem ocorrer periodicamente, de acordo com o tipo, o porte e as recomendações dos fabricantes.
10.4.10.1 A realização da manutenção preventiva dos equipamentos deve ser feita pela área administradora dos servidores, conforme especificado nos contratos firmados com os fabricantes ou fornecedores.
10.4.11 Os servidores do ambiente Intranet considerados críticos devem possuir serviço de log permanentemente ativo.
10.4.11.1 A classificação de um servidor como crítico deve ser atribuída pelo SSSB, levando em consideração as aplicações e dados armazenados e a respectiva classificação de criticidade mapeada pelo Programa de Continuidade de Negócios do TJPA.
10.4.11.2 A classificação dos servidores deve ser reavaliada, no máximo, a cada seis meses ou a cada nova implementação de aplicação ou base de dados.
10.4.12 O ambiente Intranet deve seguir as recomendações e padrões de segurança definidos pelo SSSB visando à proteção contra ações indevidas.
10.4.12.1 A solução de segurança da Intranet deve ser revista, no máximo, de seis em seis meses, pelo SSSB.
10.4.12.2 A solução de segurança da Intranet deve ser atualizada sempre que for detectada alguma vulnerabilidade ou quando for implementada uma nova funcionalidade.
10.4.13 É proibida a saída de informações da sala dos servidores da Intranet em mídia magnética e/ou óptica em situações de manutenção, substituição ou devolução de equipamento.
10.4.14 O manuseio dos equipamentos deve ser feito de forma a preservar sua integridade física e lógica, respeitando-se as recomendações de conservação e uso do fabricante.
10.4.15 Em caso de saída de equipamento dos ambientes do TJPA ou de dispositivos de armazenamentos, em caráter temporário ou definitivo, os dados existentes devem ser eliminados visando minimizar a possibilidade de cópia em seu destino.
10.4.16 O controle de acesso físico às salas dos servidores é administrado pela área responsável pelos servidores da Intranet.
10.4.17 A infraestrutura de rede do ambiente Intranet deve seguir os padrões especificados nas normas do TJPA referentes às instalações físicas.
10.4.18 Os servidores da Intranet devem, de acordo com as especificações do Programa de Continuidade de Negócios da TJPA, ter disponibilidade de 24 horas por dia, sete dias por semana, salvo manutenções programadas, ou contingência.
10.4.19 Em situações de inoperância do ambiente Intranet em que seja necessária a disponibilidade dos serviços, os procedimentos a serem adotados devem estar obedecendo ao definido no Programa de Continuidade de Negócios do TJPA.
10.4.20 Os recursos tecnológicos utilizados no ambiente Intranet devem ser homologados pelo SSSB.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Não se aplica

12. CONSIDERAÇÕES FINAIS

Não se aplica.

II - POLÍTICA DE SEGURANÇA DA INFORMAÇÂO

1. ASSUNTO/OBJETIVO

Definição das diretrizes básicas da política de segurança da Informação do Tribunal de Justiça do Pará (TJPA).

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Este manual tem por objetivo informar e estabelecer as diretrizes, parâmetros e orientações estratégicas de Segurança da Informação e, a partir da sua existência, normas técnicas específicas, normas de utilização de recursos de informática, procedimentos operacionais, instruções de trabalho e padrões de segurança, compondo assim, uma Política de Segurança da Informação para a instituição. Atendendo a necessidade de garantia dos meios legais para que os gestores possam administrar a estrutura de segurança da informação aplicada a todos os ambientes, sistemas, pessoas e processos do Poder Judiciário do Pará.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos (SSSB)

4. PÚBLICO ALVO

Servidores, magistrados, estagiários e os colaboradores em todas as unidades do TJPA.

5. RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica.

6. REGULAMENTAÇÃO UTILIZADA

Portaria nº 990/2009 – GP;
Portaria n° 1045/2010 – GP.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Segurança da informação – prática de defender informações contra acesso não autorizado, uso, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. É um termo geral que pode ser usado independentemente do formato dos dados;
Classificação da informação – indica o nível de disponibilidade, integridade e confidencialidade necessário para cada tipo de informação;
Disponibilidade – garante confiabilidade e acesso tempestivo aos dados e recursos para pessoas autorizadas;
Integridade – assegura a exatidão e confiabilidade das informações e sistemas e que qualquer modificação não autorizada seja impedida. Mecanismos de hardware e software e comunicação devem trabalhar em conjunto para manter e processar os dados corretamente garantindo que os dados cheguem aos seus destinos pretendidos sem alteração inesperada;
Confidencialidade – assevera que o necessário nível de sigilo é aplicado em cada ponto de processamento da informação, impedindo a divulgação não autorizada. O nível de confidencialidade exigido deve ser mantido enquanto os dados residem nos sistemas, transitam na rede e quando chegam ao destino;
Vulnerabilidade – Software, hardware, processo ou fraqueza humana que pode fornecer um atacante a porta aberta que ele está procurando para entrar em um computador ou rede e obter acesso não autorizado aos recursos do ambiente;

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

ANEXO I – ESTRUTURA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TJPA.

9. COMPETÊNCIAS E RESPONSABILIDADES

Competirá à Comissão de Informática e à Secretaria de Informática, a manutenção, atualização e monitoramento periódico destas Diretrizes Básicas, bem como sua complementação por intermédio dos demais instrumentos que compõem a Política de Segurança da Informação do Poder Judiciário do Pará.

A revisão por completo das diretrizes deve ocorrer obrigatoriamente, em período não superior a 1 (um) ano, ou a qualquer tempo, em virtude de demanda importante ou urgente, como por exemplo: incidentes de segurança considerados significativos, novas tecnologias, vulnerabilidades encontradas ou novas necessidades legais ou de mercado.
A aprovação de alterações nas Diretrizes, bem como nas Normas Gerais e específicas, instrumentos que compõem a Política de Segurança da Informação, competirá à Presidência, depois de referendado pela Comissão de Informática.

A Presidência do Tribunal de Justiça do Estado do Pará poderá determinar que eventuais monitoramentos possam ser utilizados em pesquisa para identificação de eventuais tentativas ou mesmo infrações contra a Política de Segurança da Informação do Poder Judiciário do Pará.

10. PROCEDIMENTOS

A Política de Segurança da Informação do Poder Judiciário do Pará será estabelecida por intermédio de Diretrizes Básicas de Segurança da Informação, Normas Gerais para Usuários, Normas Gerais para Técnicos, Normas especificas, Procedimentos Operacionais e Instruções de Trabalho.

10.1 Conteúdo das Diretrizes Básicas de Segurança da Informação:

10.1.1 Propriedade da Informação - Garantir que toda informação gerada, em trânsito e/ou custodiada pelo Poder Judiciário do Pará por meio de tecnologia, procedimentos, pessoas e ambientes é de sua propriedade, e será usada apenas por usuários devidamente autorizados para fins profissionais, no estrito interesse da Instituição.
10.1.2 Proteção de Recursos - Proteger os recursos de Tecnologia da Informação e Comunicações, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada, garantindo sua confidencialidade, integridade e disponibilidade, considerando níveis para a classificação da informação.
10.1.3 Nível de Segurança - Garantir que na criação de novos serviços internos e externos, a seleção de mecanismos de segurança, a aquisição de bens e contratação de serviços levem em consideração o balanceamento de aspectos tais como riscos, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio.
10.1.4 Utilização de Informações e Recursos - Assegurar que informações e recursos tecnológicos sejam tornados disponíveis para magistrados, servidores e terceiros devidamente autorizados e que sejam utilizados apenas para finalidades lícitas, éticas e administrativamente aprovadas, bem como que suas configurações e parâmetros não sejam alterados sem aprovação prévia, devendo os usuários serem adequadamente identificados.
10.1.5 Classificação da Informação - Garantir que todas as informações tenham classificação de segurança, colocadas de maneira clara, permitindo que sejam adequadamente protegidas quanto ao seu acesso e uso. A

informação e/ou a documentação consideradas de acesso restrito devem ter adequada guarda e armazenamento, assim como aquelas sem utilidade, devem ser destruídas no momento do seu descarte.

10.1.6 Sigilo Profissional - Assegurar que informações e recursos estejam sujeitos às regras referentes ao sigilo profissional, garantindo adequada proteção, por meio de termos de responsabilidade e sigilo, aplicados a magistrados e servidores. E de cláusulas contratuais, aplicadas a terceiros.

10.1.7 Conscientização - Tomar medidas para que magistrados, servidores e terceiros com acesso às informações, ambientes e recursos tecnológicos do Poder Judiciário do Pará, sejam devidamente conscientizados quanto à Segurança da Informação, face às suas responsabilidades e atuação.

10.1.8 Monitoramento - Garantir o monitoramento do tráfego de informações efetuado em ambientes e recursos de Tecnologia de Informação e Comunicações, rastreando e identificando possíveis ocorrências de eventos críticos, no estrito interesse da administração do Poder Judiciário do Pará, obedecendo a legislação aplicável.

10.1.9 Gestão de Ativos - Assegurar a análise periódica dos ativos da informação (bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre, pesquisa, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócios, procedimentos de recuperação, trilhas de auditoria e informações armazenadas) de forma que estejam devidamente inventariados, protegidos, tenham um usuário responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

10.1.10 Desenvolvimento, Manutenção e Produção de Sistemas – Assegurar que o desenvolvimento, manutenção, aquisição e adaptação de produtos de mercado e sistemas internos e/ou externos, sejam providos dos requisitos de Segurança necessários para garantir informações confiáveis, íntegras e oportunas.

10.1.11 Documentação de Tecnologia da Informação e Comunicações - Assegurar que os sistemas e procedimentos de Tecnologia da Informação e Comunicações (TIC) do Poder Judiciário do Pará tenham documentação e regras adequadas e suficientes para garantir seu entendimento e recuperação em casos de contingências.

10.1.12 Gerenciamento das Operações e Comunicações - Garantir a operação segura e corrente dos recursos do processamento da informação por intermédio da implementação de controles internos de segurança considerando as pessoas, procedimentos, ambientes e tecnologia.

10.1.13 Terceirização ou Prestação de Serviços - Manter nível de segurança da informação adequado, quanto aos aspectos desta política, naquilo que se refere a responsabilidade pelos procedimentos, sistemas e recursos, terceirizados no todo ou em parte, promovendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

10.1.14 Segurança de Pessoas, Segurança Física e do Ambiente de Tecnologia da Informação e Comunicações - Prover mecanismos para que magistrados, servidores, terceiros e visitantes disponham de segurança adequada no que se refere ao acesso e uso de recursos e ambientes físicos relacionados a Tecnologia da Informação e Comunicações.

10.1.15 Continuidade das Atividades - Garantir a continuidade das atividades do Poder Judiciário do Pará, reduzindo a um período aceitável e factível, a interrupção causada por desastres ou falhas de segurança, por intermédio da combinação de ações de administração de crises, prevenção e recuperação dos serviços.

10.1.16 Prevenção e Resposta a Incidentes - Assegurar que medidas preventivas sejam tomadas com o objetivo de diminuir o risco de ocorrência de fraudes e/ou incidentes que comprometam a segurança da informação, devendo existir canal de comunicação adequado para esse fim.

10.1.17 Administração da Segurança da Informação - Assegurar que a administração da segurança da informação do Poder Judiciário do Pará seja feita pela Presidência, por intermédio de área especifica, com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como avaliar e analisar assuntos a ela pertinentes.

10.1.18 Conformidade - Garantir o cumprimento das leis, regulamentos e normas que regem as atividades do Poder Judiciário do Pará, de forma a obter máxima aderência aos instrumentos legais e normativos, garantindo que os requisitos de segurança sejam cumpridos.

10.1.19 Alegação de Desconhecimento - Esclarecer aos usuários de informações, serviços, ambientes e recursos tecnológicos, que não é dado o direito de alegação de desconhecimento desta Política de Segurança da Informação. Visto que a mesma é amplamente divulgada no âmbito interno da organização.

10.1.20 Sanções - Garantir que a não observância dos preceitos deste documento implicará na aplicação de sanções administrativas previstas nas normas internas do Poder Judiciário do Pará, nas cláusulas de responsabilidade e sigilo, e outros preceitos legais pertinentes, pactuadas em contratos, declarações ou termos de responsabilidade, sem prejuízo de responsabilização pecuniária, quando cabível. Em se tratando de magistrado e servidor o ressarcimento do prejuízo não eximirá da penalidade disciplinar cabível. Tratando-se de crime, serão os fatos levados ao conhecimento da autoridade policial, para instauração do respectivo inquérito, sem prejuízo das medidas de natureza cível.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Não se aplica

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

III - ESTAÇÕES DE TRABALHO – PADRONIZAÇÃO E CONFIGURAÇÃO

1. ASSUNTO/OBJETIVO

Estabelecer padrões para administração e suporte das estações de trabalho do Tribunal de Justiça do Estado do Pará (TJPA).

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Obter um maior controle das Estações de Trabalho visando preservar a segurança de dados e otimizar a produtividade dos usuários.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos.

4. PÚBLICO ALVO

Todas as unidades do Tribunal de Justiça do Estado do Pará.

5. RELAÇÃO COM OUTROS NORMATIVOS

Tratamento da Informação.
Antivírus - Instalação, Configuração, Utilização e Atualização.
Concessão de Acesso Lógico aos Recursos Computacionais do TJPA.

6. REGULAMENTAÇÃO UTILIZADA

Não se aplica

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Acesso Remoto – é o nome atribuído à capacidade de efetuar acesso a um computador ou uma rede a partir de uma localidade remota, dentro da mesma rede ou a partir de redes diferentes;
Active Directory – Serviço de diretório do Windows que armazena contas, senhas e políticas da rede;
Antivírus – programa cuja finalidade é detectar, isolar e, quando possível, remover códigos hostis em computador ou meio de armazenamento;
Backup – cópia de segurança dos arquivos de um computador;
Central de Serviços – Central de Serviços de Tecnologia da Informação e Comunicação;
Chefia da Unidade – Servidor público que responde a função gratificada ou a cargo de confiança, responsável por coordenar as atividades de determinada unidade do TJPA;
CAU – Coordenadoria de Apoio ao Usuário do TJPA.
Compartilhamento – Disponibilização de recursos de um computador, que permite acesso à rede local;
Conta de Serviço – Contas específicas, geralmente com direitos de administrador, utilizadas para iniciar serviços de produtos da Microsoft;
Domínio – agrupamento lógico de servidores de rede e outros recursos.
Endereço IP – é o endereço atribuído a cada equipamento pertencente a uma rede de computadores que utilize como protocolo a interconexão o TCP/IP;
Estação de Trabalho – computador pelo qual é feito o acesso à rede do TJPA;
Hot Fix – Correção liberadas pelo fabricante de um software com o objetivo de corrigir uma vulnerabilidade ou funcionalidade específica de um determinado sistema de software.
Service Pack – Conjunto de correções liberadas pelo fabricante de um software com o objetivo de corrigir alguma vulnerabilidade ou funcionalidade de um determinado sistema de software.
Software – Conjunto de instruções, logicamente organizadas em linguagem natural ou codificada, que capacitam máquinas na automatização e tratamento da informação para a execução de uma determinada tarefa;
SSSB – Serviço de Segurança e Sistemas Básicos;
Usuário – Servidor público, prestador de serviços ou estagiário autorizado a ter acesso aos recursos computacionais do TJPA para desempenho de suas atribuições;
Vírus – são pequenos programas feitos geralmente em linguagem de máquina, e que possuem a característica de se agregarem a outros programas passando a fazer parte deles, e de se replicarem automaticamente, contaminando (através de uma cópia de si mesmo) outros arquivos.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

8.1 Orientações Técnicas

8.1.1 A unidade responsável pela manutenção e instalação das estações de trabalho no TJPA é a CENTRAL DE SERVIÇOS.

8.1.2 Os responsáveis pela manutenção das estações de trabalho têm plenos conhecimentos dos Sistemas Operacionais homologados.

8.1.3 O idioma utilizado no sistema operacional de estações de trabalho é o Português.

8.1.4 Os Service Packs e os Hot Fixes homologados pelo TJPA são aplicados nas estações de trabalho de forma automática.

8.1.5 Não é permitida a utilização de modem interno ou externo nas estações de trabalho conectadas a rede do TJPA, exceto para os microcomputadores portáteis – notebooks.

8.1.6 As estações de trabalho terão apenas os softwares homologados e necessários para a realização das atividades do usuário.

8.1.7 Os arquivos que necessitem ser acessados por vários usuários do TJPA são disponibilizados em servidores de arquivos e ficam sujeitos às regras existentes para compartilhamento e acesso de pastas públicas, e de acordo com a sua classificação de sigilo.
8.1.8 Não é permitido o compartilhamento de arquivos que não sejam exclusivamente de trabalho;
8.1.9 A proteção de tela e papel de parede utilizada nas estações de trabalho segue o padrão definido pelo TJPA.
8.1.10 A homologação de novos produtos ou novas versões deve ser efetuada de forma conjunta entre a Coordenadoria de Suporte Técnico e a Coordenadoria de Atendimento ao Usuário.
8.1.11 Para acessar a estação de trabalho conectada à Rede do TJPA, o usuário deve estar cadastrado.
8.1.12 Não é permitido o compartilhamento de senhas e da sessão de trabalho de rede.
8.1.13 As estações de trabalho estão incluídas dentro do serviço de diretório Active Directory em uma Unidade Organizacional própria, na qual está definida uma Política de Grupo que implemente normas de segurança.
8.1.14 Os computadores portáteis (notebooks) estão também em uma Unidade Organizacional separada, com uma Política de Grupo semelhante, mas que permita o uso de modens e alterações nas configurações da rede.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

9.1.1 Homologar padrões e procedimentos para instalação, configuração, utilização e atualização das Estações de Trabalho.
9.1.2 Prestar suporte e orientar Central de Serviços, sempre que necessário
9.1.3 Elaborar manuais técnicos com padrões e procedimentos para instalação, configuração, utilização das Estações de Trabalho.
9.1.4 Definir a forma de distribuição das atualizações dos Sistemas Operacionais e demais aplicativos através da rede.
9.1.5 Comunicar a Central de Serviços, via correio eletrônico, quando novas alterações surgirem para a configuração das Estações de Trabalho.
9.1.6 Estabelecer e manter contato com o fabricante dos Sistemas Operacionais utilizados no parque tecnológico do TJPA.

9.2 CENTRAL DE SERVIÇOS / CAU

9.2.1 Instalar e configurar as Estações de Trabalho conforme padrão definido nos manuais elaborados pelo SSSB.
9.2.2 Efetivar alterações nas configurações das estações de trabalho.
9.2.3 Auxiliar o SSSB nas especificações e na elaboração e manutenção de padrões referentes à configuração das Estações de Trabalho;
9.2.4 Instalar e manter atualizados o antivírus nos microcomputadores que não estejam conectados à rede.
9.2.5 Repassar e notificar o SSSB, sobre as ocorrências não solucionadas localmente.
9.2.6 Prestar atendimento ao usuário quanto a problemas relacionados à configuração, utilização e atualização de antivírus.
9.2.7 Os responsáveis pela manutenção das estações de trabalho têm plenos conhecimentos dos Sistemas Operacionais homologados.

9.3 USUÁRIO

9.3.1 Encerrar sua sessão de trabalho ao terminar suas tarefas na estação de trabalho;
9.3.2 Encerrar ou bloquear sua sessão de trabalho, sempre que se ausentar de sua estação de trabalho, durante suas atividades;
9.3.3 Utilizar a rede local, respeitando as normas de segurança em vigor, de modo a garantir a sua utilização adequada;
9.3.4 Não tentar acessar quaisquer recursos de rede para os quais não possua autorização;
9.3.5 Utilizar as informações a que tiver acesso somente para o desempenho de suas atribuições;
9.3.6 Usar os recursos e as informações a que tiver acesso em estrita observância às normas estabelecidas.
9.3.7 Utilizar composição de senhas a partir da combinação aleatória de caracteres alfanuméricos.
9.3.8 Elaborar a senha conforme orientações contidas no Normativo Técnico sobre CONCESSÃO DE ACESSO LÓGICO AOS RECURSOS COMPUTACIONAIS DO TJPA e manter o sigilo da senha, respondendo pelo seu uso indevido.
9.3.9 Trocar sua senha de acesso no primeiro logon, quando for solicitado pelo sistema ou quando suspeitar de sua violação;
9.3.10 Não alterar as configurações de sua estação de trabalho nem permitir que sejam alteradas, exceto quando solicitado e autorizado pela Central de Serviços da CAU;
9.3.11 Não remover, desabilitar ou alterar a configuração do programa antivírs das estações de trabalho.
9.3.12 Verificar a existência de vírus nos arquivos recebidos por qualquer meio eletrônico antes de sua utilização.
9.3.13 Remover os vírus encontrados nos arquivos recebidos imediatamente após sua identificação, utilizando o software antivírus homologado pelo TJPA.
9.3.14 Não remover ou desabilitar o programa antivírus das estações de trabalho.
9.3.15 Não instalar quaisquer softwares na estação de trabalho sem a autorização da Central de Serviços da CAU;

9.3.16 Acionar a Central de Serviços em caso de problemas com a instalação e atualização do antivírus na estação;

10. PROCEDIMENTOS
Não se aplica

11. NORMAS
Não se aplica

12. RELATÓRIOS GERENCIAIS E INDICADORES
12.1 Relatórios:
12.1.1 Relatórios a Serem Emitidos pelo SSSB sob demanda:
12.1.2 Relatórios da quantidade de estações de trabalho incluídas no Domínio
12.1.3 Relatório de Atualização das Estações de Trabalho
12.2 Indicadores:
Não se aplica

13. CONSIDERAÇÕES FINAIS
Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

IV - CORREIO ELETRÔNICO - PADRÃO E REGRAS DE UTILIZAÇÃO

1. ASSUNTO/OBJETIVO
O Correio Eletrônico do Tribunal de Justiça do Estado do Pará objetiva facilitar e agilizar o desenvolvimento das atividades do Tribunal de Justiça.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO
Tem como finalidade a comunicação administrativa entre as unidades judiciárias, seus magistrados, servidores, terceirizados e requisitados, além de possibilitar a veiculação de informações de interesse de todo o Egrégio Tribunal de Justiça.

3. UNIDADE GESTORA
Serviço de Segurança e Sistemas Básicos, da Secretaria de Informática, do Tribunal de Justiça.

4. PÚBLICO ALVO
Magistrados, servidores, terceirizados, requisitados e colaboradores de todas as Unidades Judiciais do Tribunal de Justiça.

5. RELAÇÃO COM OUTROS NORMATIVOS
SI-17.01-Tratamento da Informação

6. REGULAMENTAÇÃO UTILIZADA
Não se aplica.

7. DEFINIÇÕES E CONCEITOS BÁSICOS
Agenda eletrônica/calendário – onde são alocados os horários disponíveis para compromissos e agendamento de reuniões, palestras ou cursos;
Administração do Servidor de E-mail - Serviço de Segurança e Sistemas Básicos, setor da Secretaria de Informática, responsável pelo suporte técnico do Servidor de E-mail;
Alias - termo que identifica de forma única uma caixa postal ou lista de distribuição;
Backup – cópia de segurança de arquivos ou dados que venham a servir a referências futuras;
Caixa postal – local, no servidor do Correio Eletrônico do Tribunal de Justiça do Estado do Pará, onde são armazenadas as mensagens, compromissos, tarefas e outros documentos recebidos e enviados;
Caixa postal individual – caixa postal de magistrados, terceirizados e requisitados, caracterizada como ferramenta facilitadora da execução de suas atividades no ambiente do Tribunal de Justiça;
Caixa postal unidade – é caixa postal de uma unidade do Tribunal de Justiça cadastrada no Correio Eletrônico do Tribunal de Justiça do Estado do Pará;
Comunicação administrativa – toda comunicação emitida por meio dos atos administrativos, que visem o repasse de orientações, demandas ou normas relacionadas às atividades do Tribunal de Justiça;
Conceito/slogan – em Publicidade, frase ou expressão que resume o posicionamento desejado perante o público, objetivando a construção de determinada imagem;
Conta de rede - Identificação pessoal do usuário que permite acesso à rede local;
Diretório – é a lista de endereços/usuários cadastrados no correio eletrônico;
Display Name- nome completo da caixa postal;
Domínio – termo utilizado para representar um grupo de dispositivos, servidores e computadores agrupados dentro de uma rede;

Gestor chefe de unidade – servidor público cadastrado no Sistema de RH como responsável pela gerência da unidade judicial;
Listas de distribuição – são caixas postais agrupadas sob um mesmo nome, onde uma mensagem enviada à lista é remetida a todos que a compõem;
Lista de distribuição particular – é uma relação de caixas postais definidas pelo usuário, sendo utilizada somente pelo criador da lista;
Lista de distribuição pública – é uma relação composta de, no mínimo, 10 caixas postais individuais ou de unidades, com a mesma afinidade e abrangência restrita, utilizada por mais de uma unidade judicial;
Lista de distribuição pública corporativa – são listas de distribuição pública definidas pelo Serviço de Segurança e Sistemas Básicos, composta de, no mínimo, 10 caixas postais individuais ou de unidades, com a mesma afinidade e abrangência corporativa, utilizada por mais de uma unidade;
MB-megabyte - termo utilizado para expressar capacidade de armazenamento transmissão em computadores, correspondente a um milhão de bytes;
Marca – é o símbolo gráfico que personaliza a Instituição e ocupa local de destaque no conjunto dos elementos formadores da sua imagem institucional, pois sintetiza a comunicação do nome e suas características, conferindo-lhes identidade e tangibilidade;
Notícia - informação de interesse dos empregados, divulgada em linguagem coloquial típica do texto jornalístico;
OTRS - Sistema de abertura de chamado técnico (e-mail: central.servico@tjpa.jus.br / Telefone: 08002807005 / Web:
https://deskotrs.i.tj.pa.gov.br/otrs/customer.pl).
Redirecionamento de mensagens – recurso do serviço de correio eletrônico no qual uma mensagem é transferida automaticamente para outro endereço;
Restrição de recebimento de mensagens – recurso do serviço de correio eletrônico no qual se define permissão de envio de mensagens a uma caixa postal;
SSSB - Serviço de Segurança e Sistemas Básicos - setor responsável pela administração do servidor de e-mail.
SMTP – Simple Mail Transfer Protocol – protocolo para envio de mensagens;
Spam – mensagem comercial enviado ao destinatário sem a sua solicitação;
TJEPA – Tribunal de Justiça do Estado do Pará;
Usuário - é o magistrado, servidor, estagiário ou terceirizado autorizado a ter acesso ao Correio Eletrônico do TJEPA;
Usuário responsável pela caixa postal unidade - é o gestor chefe de uma unidade judicial, no caso de caixa postal principal, ou servidor público indicado por este, para administrar a documentação recebida e expedida, por meio da Caixa Postal Unidade Judicial;
Usuário secundário - é o indicado pelo usuário responsável pela Caixa Postal da Unidade Judicial para ajudá-lo a administrar a documentação recebida e expedida.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

A conta de correio eletrônico é uma ferramenta de trabalho de propriedade do Tribunal de Justiça do Estado do Pará para a realização das atividades laborais.

8.1 Orientações Técnicas

8.1.1 O Tribunal de Justiça do Estado do Pará se reserva o direito de monitorar através da rede, aplicativos e sistemas de monitoramento, a circulação e o conteúdo das mensagens de caixas postais individuais e de unidades, a qualquer tempo e independente de aviso prévio.

8.1.2 O tamanho máximo do e-mail obedece o padrão de limites do Tribunal de Justiça do Estado do Pará de 10 megabytes (MB), incluindo arquivos anexos, para envio e recebimento em caixa postal.

8.1.3 O monitoramento, o bloqueio e o rastreamento de mensagens enviadas e recebidas nas caixas postais do Correio Eletrônico são efetuados sob demanda do Serviço de Segurança e Sistemas Básicos, a fim de garantir sua utilização como instrumento de comunicação administrativa e o cumprimento deste normativo.

8.1.4 O Correio Eletrônico veicula a comunicação administrativa do Tribunal de Justiça do Estado do Pará sobre produtos, serviços e processos.

8.1.5 Conteúdos de caráter noticioso ou promocional, não restritos a assuntos administrativos ou operacionais, são submetidos à análise da Serviço de Segurança e Sistemas Básicos.

8.1.6 Não é permitido o uso do Correio Eletrônico para os seguintes fins:

a) particulares;
b) promoção pessoal;
c) divulgação político-partidária/eletiva;
d) veiculação de mensagens que impliquem discriminação de idade, raça, religião, gênero, orientação sexual, nacionalidade ou desabilitação física
e) divulgação de mensagens que solicitem o reenvio a outros usuários, correntes, anedotas, entretenimento, esoterismo, bolões, mensagens não solicitadas, mensagens religiosas, pedido de ajuda financeira, aviso sobre supostos vírus, ou que caracterize ofensa ou agressão;
f) veiculação de mensagens de cunho pornográfico ou pedofílico;
g) veiculação de mensagens de oferta de produtos ou serviços de terceiros;
h) veiculação de mensagens em desacordo com as demais normas do Tribunal de Justiça;
i) divulgação da lista de endereços eletrônicos dos usuários do Correio Eletrônico para fora do Tribunal de Justiça.

8.1.7 Toda comunicação enviada por meio do Correio Eletrônico deve estar de acordo com as políticas do Tribunal de Justiça do Estado do Pará e deve seguir o normativo vigente sobre Tratamento da Informação (normativo SI-17.01-Tratamento da Informação).
8.1.8 A comunicação eletrônica (CE) é o ato emitido por meio eletrônico para solicitar ou divulgar orientações de caráter geral ou restrito, dar andamento ou solução a assuntos administrativos ou operacionais. Caracteriza-se por texto curto, objetivo e direto, visando agilizar a comunicação no âmbito do Tribunal de Justiça do Estado do Pará.
8.1.9 Toda mensagem encaminhada via correio eletrônico constitui-se no ato administrativo de comunicação eletrônica e obedece as regras gerais da comunicação administrativa do Tribunal de Justiça do Estado do Pará.
8.1.10 Na elaboração de comunicação eletrônica é proibida a utilização de papel de parede, animação, imagem ilustrativa, conceito/slogan, exceto quando se tratar de ação de comunicação publicitária interna promovida pelo Cerimonial.
8.1.11 O texto da CE é objetivo, direto, sem preâmbulos e o assunto é introduzido no primeiro parágrafo.
8.1.12 O corpo da CE não contém tabelas, planilhas, listas ou gráficos, devendo utilizar-se de anexos para transmitir as referidas informações.
8.1.13 O assunto tratado na CE é inserido, de forma sucinta e específica, no campo "Assunto" do formulário do correio eletrônico.
8.1.14 Cabe ao emitente do ato atribuir o grau de sigilo da informação, no campo “Assunto”.
8.1.15 O uso de arquivos anexos à CE deve se restringir ao estritamente necessário de modo a não sobrecarregar a caixa postal do destinatário.
8.1.16 As sugestões, elogios, reclamações e denúncias devem ser encaminhadas por meio do canal de relacionamento Interno.
8.1.17 Os casos não previstos neste normativo devem ser encaminhados à caixa postal noc@tjpa.jus.br, para avaliação.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 Serviço de Segurança e Sistemas Básicos – SSSB:
9.1.1 O SSSB é a unidade gestora da política de utilização do Correio Eletrônico.
9.1.2 São atribuições do SSSB:
a) definir a política de utilização do Correio Eletrônico;
b) definir normas, padrões e procedimentos referentes à utilização do Correio Eletrônico;
c) orientar os usuários quanto à correta utilização do Correio Eletrônico;
d) solicitar bloqueio e autorizar desbloqueio de caixa postal por uso indevido do Correio Eletrônico;
e) autorizar o acesso a Caixa Postal de Unidade para fins de auditoria;
f) autorizar a criação e exclusão de Listas de Distribuição Pública e Pública Corporativa;
g) analisar e deliberar sobre situações não previstas neste Normativo.
9.1.3 O SSSB é o gestor tecnológico do Correio Eletrônico e as suas atribuições estão especificadas neste Normativo
9.1.4 O SSSB é responsável por criar, manter e excluir caixas postais e listas de distribuição pública.
9.1.5 As caixas postais de servidores, estagiários, terceirizados e requisitados são criadas por solicitação através de abertura de chamado via OTRS.

9.2 USUÁRIO
9.2.1 É responsabilidade do usuário do Correio Eletrônico:
a) manter em sigilo sua senha de acesso ao correio eletrônico;
b) obedecer às regras de utilização do correio eletrônico;
c) fechar o aplicativo de correio toda vez que se ausentar, evitando acesso indevido;
d) usar a informação e os recursos a ela relacionados em estrita observância à Política de Segurança da Informação.
e) efetuar manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo seu funcionamento contínuo;
f) manter atualizados os dados de sua caixa postal, através de chamado via OTRS;
g) comunicar ao SSSB o uso indevido do Correio Eletrônico;
h) comunicar ao SSSB o recebimento de mensagens suspeitas de vírus/spam ou tentativa de fraude;
i) encaminhar solicitação de alteração de conta de rede através de chamado via OTRS, em caso de transferência para outra unidade judicial;
j) efetuar “backup” das mensagens de sua caixa postal individual arquivadas em pastas particulares no disco do microcomputador ou servidor de arquivos da unidade judicial;
k) efetuar “backup” das mensagens contidas na caixa postal, evitando com que a mesma não fique cheia;
l) habilitar o aviso de ausência temporária da Caixa Postal Individual, conforme disposto no subitem 10.3., nos casos de afastamento temporário do Servidor ou Estagiário de sua Unidade de lotação, no exercício de suas atividades, quando não for possível o acesso ao Correio Eletrônico.

9.2.2 A responsabilidade do usuário abrange o conteúdo de textos, áudio e imagens, veiculados em suas mensagens.

9.3 GESTOR CHEFE DA UNIDADE

9.3.1 O gestor chefe da Unidade é responsável por:

a) toda correspondência emitida e recebida na Caixa Postal Unidade, tanto da principal quanto da(s) secundária(s);

b) atualizar os dados da Caixa Postal da Unidade;

c) solicitar o cadastramento de Caixa Postal da Unidade, principal e secundária;

d) designar os usuários para acesso à Caixa Postal Unidade, principal e secundária;

e) controlar o limite de armazenamento da Caixa Postal Unidade e garantir seu funcionamento contínuo;

f) verificar e controlar periodicamente os usuários autorizados a ter acesso à Caixa Postal Unidade, principal e secundária, por meio do formulário Propriedades de Caixa Postal;

g) orientar os usuários subordinados sobre o uso correto do Correio Eletrônico;

h) solicitar o desbloqueio de Caixa Postal individual de usuário subordinado suspenso por uso indevido, orientando o usuário para o uso correto do canal;

i) dar início ao processo de apuração pertinente, para aplicação de penalidades disciplinares por uso indevido do Correio Eletrônico;

j) solicitar a exclusão de acesso à Caixa Postal da Unidade dos usuários subordinados em caso de transferência para outra unidade judicial, licença, cessão para outro órgão, demissão ou aposentadoria.

k) efetuar backup das mensagens arquivadas em pastas particulares no disco do microcomputador ou servidor de arquivos da Unidade Judicial, como rotina de segurança;

l) efetuar backup das mensagens contidas na Caixa Postal da Unidade Judicial, principal e secundária, em caso de extinção da Unidade Judicial;

m) solicitar a exclusão da Caixa Postal da Unidade Judicial, principal e secundária, após execução do backup;

n) comunicar à SSSB o uso indevido do Correio Eletrônico por parte de usuário subordinado.

10. PROCEDIMENTOS

10.1 Criação, Alteração e Exclusão de Caixa Postal

10.1.1 CAIXA POSTAL DE UNIDADE JUDICIAL

10.1.1.1 Destina-se ao envio e recebimento de mensagens relacionadas às atividades da Unidade Judicial, constituindo-se canal oficial para a comunicação administrativa.

10.1.1.2 A caixa postal unidade judicial é identificada por meio do "ALIAS" e do nome da unidade.

10.1.1.3 As caixas postais de unidades judiciais podem ser principal ou secundária.

10.1.1.4 Todas as unidades judiciais devem possuir caixa postal principal.

10.1.1.5 Para solicitar a criação, alteração ou exclusão de uma caixa postal de unidade, faz-se necessário a abertura de chamado pelo OTRS, sugerindo qual a nomenclatura do endereço de e-mail, bem como, indicando quem será a pessoa responsável pela manutenção da referida caixa postal.

10.1.1.6 O gestor chefe da unidade judicial tem acesso às caixas postais de sua unidade, principal e secundárias, além de designar outros empregados como usuário responsável.

10.1.1.7 O usuário responsável pela caixa postal unidade judicial designa usuários secundários a fim de auxiliá-lo na administração das correspondências ou substituí-lo em sua ausência.

10.1.1.8 Os estagiários não tem permissão de acesso às caixas postais de unidades judicias, principais ou secundárias.

10.1.1.9 A solicitação de acesso àscaixas postais judiciais principais ou secundárias para requisitados é responsabilidade do gestor da unidade em questão, que deve analisar os riscos advindos da utilização indevida de informações do Tribunal de Justiça do Estado do Pará.

10.1.1.10 É de inteira responsabilidade do gestor chefe da Unidade Judicial efetuar backup do conteúdo da caixa postal respectiva.

10.1.1.11 É permitido ainda, o redirecionamento de mensagens entre caixas postais de unidades judiciais distintas.

10.1.1.12 Para que seja efetuado o redirecionamento das mensagens, o usuário responsável pela caixa postal da unidade deverá solicitar através de chamado via sistema de chamado técnico (OTRS).

10.1.1.13 A solicitação para configuração de restrição é efetuada por chamado via OTRS.

10.1.1.14 A composição do "ALIAS" de Caixa Postal Unidade Judicial obedece aos padrões estabelecidos pelo SSSB.

10.1.1.15 A composição do "DISPLAY NAME" da Caixa Postal Unidade Judicial obedece à designação da unidade junto ao organograma geral do Tribunal de Justiça do Estado do Pará.

10.1.1.16 Caixa Postal Unidade Judicial, cuja estrutura foi extinta e a exclusão não solicitada num prazo de 45 dias da data da extinção da Unidade Judicial, é excluída automaticamente, com todas as mensagens nela existentes, não sendo possível a sua recuperação.

10.1.1.17 No caso da caixa postal de unidade judicial excluída, o gestor chefe da Unidade encaminha o "backup" à(s) Unidade(s) que absorveram as atividades da Unidade extinta.

10.1.2 CAIXA POSTAL INDIVIDUAL

10.1.2.1 É utilizada por magistrados, servidores, estagiários, terceirizados e requisitados no exercício das atividades desenvolvidas na Unidade de lotação.

10.1.2.2 A avaliação quanto à necessidade de acesso ao Correio Eletrônico por servidores, estagiários, terceirizados e requisitados deve considerar as atividades que lhes são atribuídas, com foco na racionalização do uso do canal.

10.1.2.3 É de inteira responsabilidade do usuário, o conteúdo da caixa postal extinta.
10.1.2.4 Os empregados envolvidos em processos de apuração sumária, sindicância, apuração de responsabilidade, processo administrativo, civil ou penal, os demissíveis, podem ter sua caixa postal suspensa e extinta, a critério do gestor chefe de sua Unidade de lotação.
10.1.2.5 Neste caso, a manutenção do acesso ao Correio Eletrônico é de inteira responsabilidade do gestor chefe da Unidade de lotação do servidor, terceirizado e requisitado.
10.1.2.6 A criação da caixa postal individual de magistrado, servidor e cedidos deve ser efetuada no momento em que for criado o usuário de rede.
10.1.2.7 Caso o usuário necessite efetuar qualquer alteração em sua caixa postal, faz necessária a abertura de chamado pelo OTRS para posterior análise e viabilidade se houver.
10.1.2.8 É de responsabilidade do usuário, o backup de sua caixa postal, e nos casos em que for comunicado o término do vínculo do usuário com este Egrégio Tribunal de Justiça, será dado um prazo de 15 (quinze) dias para a exclusão total de sua caixa postal.
10.1.2.9 É permitido o cadastramento de caixa postal para:
a) todo servidor em exercício efetivo de suas atividades no Tribunal de Justiça do Pará;
b) estagiários regularizados perante o sistema de Recursos Humanos do Tribunal de Justiça;
c) terceirizados e requisitados para execução de suas atividades no Tribunal de Justiça do Pará.

10.1.2.10 É proibido o cadastramento de usuário sem a devida solicitação preenchida e assinada através de formulário padrão, e encaminhada através de chamado via OTRS.

10.2 Lista de Distribuição
10.2.1 CRIAÇÃO DE LISTA DE DISTRIBUIÇÃO PARTICULAR
10.2.1.1 O usuário cria Lista de Distribuição Particular seguindo os passos: seleciona no “outlook” o item Ferramentas; Catálogo de Endereços; Arquivo – Nova entrada; seleciona Nova Lista; nomeia a lista a ser criada; seleciona o membros que deseja incluir.

10.2.2 CRIAÇÃO E MANUTENÇÃO DE LISTA DE DISTRIBUIÇÃO PÚBLICA E PÚBLICA CORPORATIVA
10.2.2.1 O servidor chefe de qualquer Unidade deverá abrir um chamado via OTRS para solicitar a criação de lista de distribuição pública e lista de distribuição pública corporativa.
A Central de Serviços recebe a solicitação e verifica se contém todas as informações necessárias. Caso a solicitação não contenha as informações necessárias para análise, solicita ao usuário a complementação das informações. Após a conferência, a Central de Serviços designa o chamado ao SSSB.
10.2.2.2 O SSSB analisa a solicitação e, em caso de deferimento, efetua a criação da referida lista. Caso seja indeferida a solicitação, o SSSB fecha o chamado justificando ao usuário o motivo.
10.2.2.3 O SSSB providencia a criação de Lista Pública e Lista Pública Corporativa, incluindo as seguintes informações no campo Observações de Propriedades da lista: Unidade solicitante; Data da criação; Data da atualização (se for o caso); Expiração (indeterminada ou data, no caso de lista provisória). O SSSB fecha o chamado, informando a criação da lista.

10.2.3 EXCLUSÃO DE LISTA DE DISTRIBUIÇÃO PÚBLICA E PÚBLICA CORPORATIVA
10.2.3.1 O servidor público chefe de qualquer Unidade deverá abrir um chamado via OTRS para solicitar a exclusão de lista de distribuição pública e lista de distribuição pública corporativa da sua Unidade.
10.2.3.2 A Central de Serviços recebe a solicitação, verifica se a Unidade Judicial solicitante corresponde à Unidade Judicial responsável pela lista e encaminha a solicitação ao SSSB.
10.2.3.3 O SSSB analisa a solicitação e, em caso de deferimento, efetua a exclusão.

10.3 AVISO DE AUSÊNCIA TEMPORÁRIA
10.3.1 Acessar o Outlook Web Access, escolher Opções, Assistente de Aviso de Ausência Temporária.

10.4 UTILIZAÇÃO INDEVIDA
10.4.1 O usuário detecta a utilização indevida do Correio Eletrônico e envia a mensagem à caixa postal central.servicos@tjpa.jus.br para que seja aberto um chamado via OTRS.
10.4.2 A Central de Serviços recebe a mensagem, encaminha ao SSSB para análise e bloqueio da(s) caixa(s) postal(is) de origem e retransmissoras, por tempo indeterminado, se for o caso.
10.4.3 Concomitantemente à suspensão, o SSSB encaminha mensagem à Unidade de lotação do usuário suspenso, com cópia à Secretaria de Informática, informando a efetivação do bloqueio.
10.4.4 O chefe da Unidade de lotação do usuário ou autoridade imediatamente superior, quando o usuário bloqueado for gestor chefe de Unidade, recebe a comunicação de bloqueio e efetua análise quanto a necessidade de abertura de Processo de Administrativo Disciplinar por uso indevido do Correio Eletrônico.
10.4.5 No caso de desbloqueio da caixa postal, o gestor chefe da Unidade orienta o usuário suspenso quanto à utilização do Correio Eletrônico, conforme normas vigentes e envia solicitação à Central de Serviços, por meio da Caixa Postal Principal da Unidade, contendo a confirmação de que o usuário foi devidamente orientado.
10.4.6 A Central de Serviços recebe a solicitação e encaminha para o SSSB para análise e restabelecimento do acesso.

10.4.7 No caso de uso indevido de caixa postal de Unidade, o SSSB encaminha à unidade infratora mensagem de orientação com cópia à caixa postal individual do chefe da unidade e à unidade de vinculação hierarquicamente superior.
10.4.8 O SSSB informa mensalmente à caixa postal da Secretaria de Informática, até o 2º dia útil do mês subsequente ao mês de referência, as ocorrências consolidadas de uso indevido, contendo nome e matrícula do usuário bloqueado, data da ocorrência, número da ocorrência (1ª, 2ª, etc) e Unidade de lotação com código.

11. NORMAS
Não se aplica.

12. RELATÓRIOS GERENCIAIS E INDICADORES
Não se aplica.

13. CONSIDERAÇÕES FINAIS
Este normativo aborda as melhores práticas de utilização do serviço de Correio Eletrônico para o Tribunal de Justiça do Estado do Pará e o mesmo sofrerá atualizações periódicas, no intuito de implementar melhorias. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

V - ANTIVÍRUS - INSTALAÇÃO, CONFIGURAÇÃO, UTILIZAÇÃO E ATUALIZAÇÃO

1. ASSUNTO/OBJETIVO
Orientar a instalação, a configuração a utilização e a atualização dos antivírus deste Tribunal de Justiça.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO
Garantir segurança aos sistemas e informações do TJPA, contra a execução de código hostil. Todas as Estações e Servidores ligados à rede do TJPA.

3. UNIDADE GESTORA
Serviço de Segurança e Sistemas Básicos (SSSB)

4. PÚBLICO ALVO
Magistrados, servidores, estagiários e os colaboradores em todas as unidades do TJPA.

5. RELAÇÃO COM OUTROS NORMATIVOS
SI-02.01- Política de Segurança da Informação

6. REGULAMENTAÇÃO UTILIZADA
NBR ISO 27002/2006.

7. DEFINIÇÕES E CONCEITOS BÁSICOS
Agente – é o módulo cliente instalado em todas as estações/servidores em uma organização e tem a função de prover uma comunicação segura entre o servidor de gerência e os softwares do servidor institucional de antivírus (atualmente Kaspersky) instalados em cada máquina;
Antivírus – programa cuja finalidade é detectar, isolar e, quando possível, remover códigos hostis em computador ou meio de armazenamento;
Arquivos de Atualização – arquivos utilizados pelo antivírus para atualização das definições de códigos hostis e do engine;
Central de Serviços – Central de Serviços de Tecnologia da Informação e Comunicação;
Chefia da Unidade – Servidor público que responde a função gratificada ou a cargo de confiança, responsável por coordenar as atividades de determinada unidade do TJPA;
Código Hostil – conjunto de instruções que tem como objetivo destruir, alterar, danificar ou se apropriar de informações não autorizadas. A ação do sistema de proteção objetiva que nenhum código hostil seja capaz de se auto-executar, sendo sempre necessário para tal a intervenção, intencional ou não, do usuário;
Download – processo de transferência de dados de um servidor para uma estação cliente;
Engine – nome dado pelos fabricantes de software antivírus para o conjunto de bibliotecas (.DLL) que contem os mecanismos de varredura e recuperação de arquivos infectados por vírus;
SSSB – Serviço de Segurança e Sistemas Básicos;
Software – Conjunto de instruções, logicamente organizadas em linguagem natural ou codificada, que capacitam máquinas na automatização e tratamento da informação para a execução de uma determinada tarefa;
Usuário – Magistrado, servidor, estagiário ou prestador de serviços autorizado a ter acesso aos recursos computacionais do TJPA para desempenho de suas atribuições;
Vírus – são pequenos programas, feitos geralmente em linguagem de máquina, que possuem a característica de se inserirem em outros programas passando a fazer parte deles, e de se replicarem automaticamente, contaminando (através de uma cópia de si mesmo) outros arquivos.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS
Não se aplica.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

9.1.1 Homologar padrões e procedimentos para instalação, configuração, utilização e atualização de antivírus.

9.1.2 Divulgar informações institucionais relacionadas à incidência de códigos hostis.

9.1.3 Prestar suporte e orientar Central de Serviços, sempre que necessário

9.1.4 Elaborar manuais técnicos com padrões e procedimentos para instalação, configuração, utilização e instalação de antivírus.

9.1.5 Definir a forma de distribuição dos arquivos de atualização do antivírus através da rede.

9.1.6 Efetuar captura, testes e disponibilização dos arquivos de atualização da plataforma antivírus para novos códigos hostis, sempre que houver liberação de novas versões pelo fabricante.

9.1.7 Comunicar a Central de Serviços, via correio eletrônico, quando da liberação de novas versões do antivírus.

9.1.8 Estabelecer e manter contato com o fabricante do antivírus para fins de suporte.

9.2 Central de Serviços

9.2.1 Instalar a versão mais atual do antivírus e dos arquivos de atualização conforme padrão definido nos manuais elaborados pelo SSSB.

9.2.2 Configurar os servidores e estações das redes locais para que seja efetuada atualização automática a partir da estação/servidor de atualização designado para a localidade.

9.2.3 Manter atualizados o antivírus e os arquivos de atualização nos servidores e estações de trabalho, utilizando para isso, somente os arquivos distribuídos pelo SSSB.

9.2.4 Instalar e manter atualizados o antivírus nos microcomputadores que não estejam conectados à rede.

9.2.5 Repassar e notificar o SSSB, sobre as ocorrências não solucionadas localmente.

9.2.6 Prestar atendimento ao usuário quanto a problemas relacionados à configuração, utilização e atualização de antivírus.

9.3 Usuário

9.3.1 Manter o antivírus instalado e ativo, nos equipamentos utilizados para desempenho de suas atribuições.

9.3.2 Acionar a Central de Serviços em caso de detecção de códigos hostis que não tenham sido removidos pelo antivírus.

9.3.3 Acionar a Central de Serviços em caso de problemas com a instalação e atualização do antivírus na estação.

9.4 Chefia da Unidade

9.4.1 Assegurar-se da existência de antivírus instalado atualizado e ativo, em todos os equipamentos da unidade sob sua responsabilidade.

10. PROCEDIMENTOS

10.1 PROCEDIMENTOS ASSOCIADOS AO ANTIVIRUS INSTITUCIONAL

10.1.1 A instalação inicial do antivírus e do agente Kaspersky Network nas estações está inclusa na imagem das máquinas

10.1.2 A atualização para novas versões do antivírus nas Estações de Trabalho e servidores será feita de forma automática e centralizada pelo SSSB.

10.1.3 Caso a instalação centralizada da nova versão apresente problemas a atualização do antivírus nas Estações de Trabalho e Servidores deve ser feita manualmente pela Central de Serviços de acordo com manual elaborado para esta finalidade.

10.1.4 Aplicativos de uso institucional que forem afetados (funcionamento inadequado/não funcionamento) após a instalação do antivírus, devem ser levados ao conhecimento da SSSB para sua análise, tratamento e liberação de suas funções em conjunto com a referida ferramenta.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Relatórios de Infecção por Vírus

Relatório de Atualização de Base de Dados

Relatório de Versão do Kaspersky

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

VI - CORREIO ELETRÔNICO - GESTÃO TECNOLÓGICA

1. ASSUNTO/OBJETIVO

O Correio Eletrônico do Tribunal de Justiça do Estado do Pará objetiva facilitar e agilizar o desenvolvimento das atividades deste Tribunal.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Normatizar e padronizar rotinas para disponibilidade e manutenção do serviço do Correio Eletrônico do Tribunal de Justiça do Estado do Pará.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos, da Secretaria de Informática, deste Egrégio Tribunal de Justiça.

4. PÚBLICO ALVO

Magistrados, servidores, estagiários, terceirizados, requisitados e colaborado-res de todas as unidades do Tribunal de Justiça do Estado do Pará.

5. RELAÇÃO COM OUTROS NORMATIVOS

Normativo: Correio Eletrônico - Padrão e Regras de Utilização

6. REGULAMENTAÇÃO UTILIZADA

Não se aplica.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Alias – Significa o segundo nome ou apelido. Pode referenciar um endereço eletrônico alternativo de uma pessoa ou grupo de pessoas;
Caixa Postal – É o local, no servidor do Correio Eletrônico, onde são armazenadas as mensagens, compromissos, tarefas e outros documentos recebidos e enviados;
Conta de Rede Windows – É a identificação do usuário que, juntamente com a senha, o habilita a acessar os recursos do ambiente de rede Windows;
Exchange – Serviço de correio eletrônico utilizado pelo Tribunal de Justiça do Estado do Pará;
LOG – Arquivo de registro de eventos;
MAPI – Messaging Application Programming Interface – Interface de programação de aplicativos de mensagens;
SSSB – Serviço de Segurança e Sistemas Básicos;
SMTP – Simple Mail Transfer Protocol – Protocolo para envio de mensagens;
Usuário – É o servidor público, estagiário, terceirizado ou cedido autorizado a acessar o Correio Eletrônico do Tribunal de Justiça do Estado do Pará.
Usuário Responsável pela Caixa Postal – É o dirigente de uma unidade judicial ou usuário indicado por este para administrar a documentação recebida e expedida, por meio da Caixa Postal Unidade Judicial;
Usuário Secundário – É o indicado pelo usuário responsável pela Caixa Postal para ajudá-lo a administrar a documentação recebida e expedida;
Windows – Sistema operacional utilizado nos servidores do Correio Eletrônico do Tribunal de Justiça do Estado do Pará.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

8.1 Orientações Técnicas

8.1.1 Toda caixa postal deve possuir o endereço SMTP no formato alias@tjpa.jus.br.

8.1.2 Toda caixa postal de servidores, estagiários, terceirizados e cedidos, e de todas as unidades judiciárias, deve ter também endereço SMTP, com domínio "@tjepa.jus.br" configurado.

8.1.3 Este endereço deve ser o primário.

8.1.4 O envio de mensagens através do correio interno, por aplicativos ou por sistemas de monitoramento de aplicações e serviços, é permitido, desde que o público alvo seja o de usuários do Correio Eletrônico deste Tribunal de Justiça.

8.1.5 Alguns destinatários podem ser de correio internet, desde que relacionados à aplicação, como jurisdicionados.

8.1.6 As aplicações que necessitem enviar mensagens devem fazê-lo utilizando o protocolo SMTP, seguindo os parâmetros de desenvolvimento especificados pelo S3B.

8.1.7 O endereço de origem das mensagens enviadas por aplicações deve ser um endereço SMTP associado a uma caixa postal específica da aplicação.

8.1.8 As demandas para envio de mensagens por aplicativos devem ser encaminhadas ao S3B para avaliação, conforme o caso.

8.1.9 Os procedimentos para criação, manutenção de caixas postais, manuais e guias específicos são elaborados pelo S3B

8.1.10 Os procedimentos para instalação, manutenção, produção e suporte dos servidores de correio eletrônico interno, bem como dos serviços inerentes ao produto e do plano de contingência, são elaborados e atualizados pelo S3B em manuais e guias para uso por esta unidade judicial centralizadora estadual de tecnologia da informação.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

Intermediar as demandas de aplicativos que necessitem enviar mensagens eletrônicas, avaliando a destinação das mensagens enviadas pelo aplicativo, e executar os procedimentos para efetivação da conexão, quando relativa a envio de mensagens ao público interno ou externo.

9.2 Atribuições do SSSB relacionadas aos servidores do Correio Eletrônico

9.2.1 Suporte ao atendimento em 2º nível;

9.2.2 Orientar e resolver problemas não solucionados pelo 1º nível;

9.2.3 Ler, analisar, responder e encaminhar mensagens recebidas pela caixa postal de suporte ao noc@tjpa.jus.br;
9.2.4 Cadastrar e manter os analistas do S3B como sub-administradores do Exchange, para viabilizar a execução de suas atividades de cadastramento e manutenção de caixas postais e listas de distribuição pública.
9.2.5 Definir e manter padrões e configurações do ambiente de correio;
9.2.6 Definir padrões de hardware e software dos servidores;
9.2.7 Definir a quantidade e localização dos servidores do Correio Eletrônico;
9.2.8 Manter as configurações de TCP/IP do servidor (Endereços IP, DNS, WINS), de acordo com a estrutura de rede onde este está localizado;
9.2.9 Manter a padronização de software definida para o ambiente de correio;
9.2.10 Manter a padronização de hierarquia para pastas públicas;
9.2.11 Manter as listas de distribuição públicas corporativas;
9.2.12 Manter a distribuição de caixas postais entre os servidores;
9.2.13 Configurar conexões de aplicações para envio de mensagens via SMTP;
9.2.14 Programar backup automático;
9.2.15 Restaurar backup;
9.2.16 Testar em laboratório, novas versões lançadas no mercado (Windows, Exchange e correções de software);
9.2.17 Instalar aplicativos nos servidores necessários ao funcionamento do Correio Eletrônico, inclusive na aplicação de atualizações de versões;
9.2.18 Configurar produtos instalados, inclusive antivírus.
9.2.19 Monitorar a atualizar automaticamente, versões dos arquivos de definição de vírus, nos antivírus do Exchange e do Windows;
9.2.20 Impedir contaminações e proliferações, evitando prejuízos ao serviço de correio eletrônico, inclusive com a configuração de bloqueio de mensagens por assunto.
9.2.21 Monitorar os serviços Exchange e antivírus;
9.2.22 Monitorar as filas de mensagens;
9.2.23 Monitorar os recursos (CPU, Memória e discos);
9.2.24 Monitorar a conexão com o ambiente de correio externo, verificar o desempenho na troca de mensagens entre os ambientes, adotar ações tempestivas em caso de problemas;
9.2.25 Pesquisar soluções para os problemas relativos ao serviço de correio eletrônico e acionar suporte de terceiros, sempre que necessário;
9.2.26 Monitorar atividades de backup das bases de dados do correio e efetuar backup manual em caso de falhas no processo automatizado.
9.2.27 A restauração de backup tem por objetivo a recuperação de toda a base de informação do correio nos casos de pane do sistema (hardware ou software) ou recuperação de logs para atividades de auditoria;
9.2.28 Não há recuperação de mensagens ou pastas removidas de caixas postais do sistema de correio eletrônico;
9.2.29 Não há recuperação de caixas postais excluídas;
9.2.30 Rastrear as mensagens enviadas e recebidas por caixas postais do Correio Eletrônico, mediante solicitação;
9.2.31 Bloquear/desbloquear caixas postais por uso indevido, conforme previsto no Normativo.
9.2.32 Definir e homologar novos serviços/soluções disponibilizadas no Correio Eletrônico;
9.2.33 Definir padrões e diretrizes para o Correio Eletrônico;
9.2.34 Obter em conjunto ao NIC a definição da arquitetura tecnológica sempre que necessário.
9.2.35 Acionar fornecedores/assistência técnica em caso de necessidade de manutenção do hardware;

As atribuições acima são referentes ao conjunto de servidores Exchange e ao serviço de correio eletrônico interno independentemente da localização física.
As atualizações nos servidores ou instalações de produtos são demandadas exclusivamente pela S3B, de acordo com a necessidade e disponibilidade de recursos.
Apenas a equipe de suporte da S3B tem acesso físico aos servidores.

10. PROCEDIMENTOS
10.1 Rastreamento de Mensagens
10.1.1 O rastreamento de mensagens pode ser solicitado pelo S3B.
10.1.2 É efetuado com base nos últimos 30(trinta) dias corridos, contados a partir da data de recebimento da solicitação.

10.2 Manutenção Preventiva
10.2.1 Cabe ao S3B, acompanhar localmente o servidor instalado na unidade e acionar fornecedor do equipamento em caso de problemas.
10.2.2 Paralisações de servidores para manutenção, devem ser agendadas para após 20h00m, em dias úteis, ou final de semana, salvo em casos onde o serviço esteja prejudicado, inoperante ou com indicação de colapso iminente, necessitando uma parada emergencial antes das 19:00h.
10.2.3 Não é permitida a paralisação de servidor para manutenção da base de dados correção de software ou correções de segurança, nos finais de semana, sem aviso prévio.

10.2.4 Dependendo da urgência da correção, é permitida a parada durante o período de expediente, mediante aviso prévio aos usuários do servidor, em até meia hora antes da paralisação, desde que ocorra por período inferior a 2 horas.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Não se aplica.

12. CONSIDERAÇÕES FINAIS

Este normativo aborda as melhores práticas para manutenção dos servidores de Correio Eletrônico deste Tribunal de Justiça do Estado do Pará, e o mesmo sofrerá atualizações periódicas, no intuito de implementar melhorias.

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

VII - UTILIZAÇÃO DA INTERNET

1. ASSUNTO/OBJETIVO

Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Pará.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

A Internet é o maior conglomerado de redes de comunicações em escala mundial, ou seja, vários computadores e dispositivos conectados em uma rede mundial e dispõe milhões de dispositivos interligados pelo protocolo de comunicação TCP/IP que permite o acesso a informações e todo tipo de transferência de dados. Ela carrega uma ampla variedade de recursos e serviços, incluindo os documentos interligados por meio de hiperligações da World Wide Web (Rede de Alcance Mundial), e a infraestrutura para suportar correio eletrônico e serviços como comunicação instantânea e compartilhamento de arquivos.

Sua utilização no Tribunal visa a disponibilização de serviços aos jurisdicionados e advogados, ao acesso a sistemas externos, à comunicação entre unidades judiciárias geograficamente espalhadas, à prestação de serviço e à comunicação por meio de correio eletrônico, serviços de mensageria entre si e com demais órgãos e entidades.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos (SSSB).

4. PÚBLICO ALVO

Magistrados, servidores, estagiários e os colaboradores em todas as unidades do TJPA.

5. RELAÇÃO COM OUTROS NORMATIVOS

SI-02.01-Política de Segurança da Informação

6. REGULAMENTAÇÃO UTILIZADA

NBR ISO 27002/2006.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Chave de Acesso - Código de acesso atribuído a cada usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis.

Contas - Ver chave de acesso.

Download - Baixar um arquivo ou documento de outro computador, através da Internet.

FTP (File Transfer Protocol) - Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

Internet - o maior conglomerado de redes de comunicações em escala mundial, ou seja, vários computadores e dispositivos conectados em uma rede mundial e dispõe milhões de dispositivos interligados pelo protocolo de comunicação TCP/IP que permite o acesso a informações e todo tipo de transferência de dados.

Modem - Equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações, geralmente através da rede de telefonia.

Mensageria - Aportuguesamento do termo da língua inglesa “messaging”. Representa os sistemas destinados à troca de mensagens entre usuários de sistemas computacionais. A troca de mensagens pode ser síncrona quanto os interlocutores recebem imediatamente as mensagens enviadas entre si ou podem ser assíncronas quando as mensagens podem ser armazenadas pelo sistema para posterior leitura e resposta. Estes sistemas podem ser públicos e disponíveis na Internet ou podem ser privados e disponíveis apenas para os membros de uma instituição dentro de sua infraestrutura de comunicação interna (rede local). Exemplos clássicos de sistemas de mensageria são o MSN, Google Talk, Yahoo Messenger.

Peer-to-Peer (P2P) - É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.

SIR – Serviço de Infraestrutura de Rede

SSSB - Serviço de Sergurança e Sistemas Básicos

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

Não se aplica.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

9.1.1 Definir controles lógicos no sentido de garantir o cumprimento deste normativo e resguardar a utilização da banda para o uso institucional.

9.2 SIR

9.2.1 Monitorar a disponibilidade e funcionamento dos Links de Comunicação com a Internet e entre as comarcas.

9.3 Usuário

9.3.1 É de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente Norma.

10. PROCEDIMENTOS

10.1 PROCEDIMENTOS RELACIONADOS AO USO DA INTERNET

10.1.1 Internet, no âmbito do Poder Judiciário do Pará, é uma concessão e não um direito. Portanto, seu uso deve estar relacionado às necessidades de trabalho do Órgão, de forma a garantir a segurança e a boa performance deste instrumento de trabalho.

10.1.2 O usuário deve utilizar a Internet observando a conformidade com a lei, a moral e a ordem pública.

10.1.3 O acesso à Internet se dará por meio de mecanismos de autenticação (usuário/senha), que determinarão tanto a titularidade dos acessos feitos por seus usuários como registros para fins de auditoria.

10.1.4 O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso (usuário/senha).

10.1.5 É expressamente proibida a divulgação e/ou o compartilhamento de informações sigilosas em listas de discussão (ex.: Fóruns), bate-papo (ex.: chat) ou quaisquer outros meios.

10.1.6 Usuários com acesso à Internet não podem enviar para terceiros softwares adquiridos e/ou licenciados ou dados de propriedade do Poder Judiciário do Pará, sem a autorização expressa do responsável pelo mesmo.

10.1.7 Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades, desde que respeitados os termos de licença de uso e registro desses programas.

10.1.8 Haverá possibilidade de geração de relatórios acerca dos sites acessados por usuários em um determinado período.

10.1.9 O usuário não deve utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

10.1.10 É vedada a utilização de modem em máquinas que já estejam conectadas via cabo ou redes sem fio (wireless), ao ambiente interno da rede do Poder Judiciário do Pará.

10.1.11 Os usuários que desejarem utilizar outras conexões de rede, além daquelas já estabelecidas, deverão obrigatoriamente solicitar autorização à Secretaria de Informática, de forma a não comprometer a segurança da rede.

10.1.12 É permitido o uso de softwares de comunicação instantânea (mensageria), tais como, Google Talk, Skype e afins, observada sua utilização exclusivamente para fins de trabalho de interesse do Órgão.

10.1.13 Não é permitida a utilização de softwares do tipo peer-to-peer (P2P) para atividades de download ou compartilhamento de arquivos, tais como Kazaa, Emule e afins.

10.1.14 Devido à questões associadas à falta de garantia da segurança da informação, o uso de softwares de armazenamento em nuvem, tais como DropBox, iCloud, Google Drive e afins é permitido apenas em casos especiais, no interesse de atividades de trabalho do TJPA e após análise e parecer do Serviço de Segurança e Sistemas Básicos. Para estes serviços, quando liberados, não há garantia de segurança.

10.1.15 Não é permitido o acesso a sites externos de Proxy ou uso de softwares tais como UltraSurf e afins, com o intuito de burlar restrições internas aqui normatizadas. Ação contrária a esta norma caracteriza transgressão das regras de segurança da informação e coloca o transgressor sujeito às sansões e medidas previstas em lei.

10.1.16 Haverá monitoramento contínuo e bloqueio automático de sites conhecidos de jogos, pornografia, pedofilia e outros em desacordo com a lei. O acesso a sites do tipo é terminantemente proibido, mesmo quando ainda não estiverem bloqueados pelo sistema de segurança.

10.1.17 Caso haja bloqueio de algum site e este bloqueio seja considerado inválido, o usuário poderá solicitar o desbloqueio através da abertura de um chamado técnico no sistema disponível no portal interno do TJPA, sendo necessário informar na mensagem qual a URL bloqueada e a justificativa para o desbloqueio da mesma.

10.1.18 Considerando o horário do expediente forense se estende ao longo do horário entre 8:00 e 14:00, fica liberado após o termino do horário de expediente, a partir das 15:00, o acesso à Internet aos recursos de redes sociais do tipo Facebook, Google Plus, Twitter e assemelhados, assim como o acesso a vídeos sob demanda (YouTube).

11. RELATÓRIOS GERENCIAIS E INDICADORES

Relatórios a Serem Emitidos pelo SSSB sob demanda

Relatórios de Utilização do Serviço de Internet

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

VIII - PUBLICAÇÃO (DEPLOY) DE APLICAÇÕES

1. ASSUNTO/OBJETIVO

Definição e descrição do processo para deploy de aplicações em servidores de produção, compreendendo desde abertura do chamado até o seu fechamento.

2. FINALIDADE E AMBITO DA APLICAÇÃO

Possui finalidade de normatizar e padronizar o processo de deploy executado pelo Serviço de Segurança e Sistemas Básicos, de tal modo que os diversos clientes que requisitam este serviço tenham total conhecimento do mesmo. Esta norma aplica-se a todas as aplicações de produção, sejam elas existentes ou novas.

3. UNIDADE GESTORA

Secretaria de Informática.

4. PUBLICO ALVO

Secretária de Informática e Coordenadora de Estatística.

5. RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica.

6. REGULAMENTAÇÃO UTILIZADA

Não se aplica.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

7.1. Deploy

Termo utilizado para a implantação ou instalação de um sistema ou aplicação em um servidor (recurso computacional)

7.2. ANS ou SLA:

Acordo de Nivel de Serviço são os níveis e tempos esperados para a entrega do serviço especificado.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

- Fluxo I: Fluxo do Processo.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1. SECRETARIA DE INFORMATICA

A secretaria de informática tem a responsabilidade de solicitar e executar os deploys para a implantação de sistemas existentes ou novos. Acrescido ela também tem a competência de solicitar os deploys (procedimento interno).

9.2. COORDENADORIA DE ESTATÍSTICA

Possui a competência de solicitar os deploys de suas aplicações.

10. PROCEDIMENTOS

10.1. ABERTURA DO CHAMADO

A abertura do chamado deverá ser realizada na ferramenta OTRS, acessível pela URL https://deskotrs/otrs/index.pl (Módulo Atendente) ou pelo e-mail noc.deploy@tjpa.jus.br, sendo o método preferível a interface via Web. O chamado deverá ser obrigatoriamente aberto na sub-fila “DEPLOY” da fila “SERVIDORES DE APLICAÇÃO”.

10.1.1. APLICAÇÕES EXISTENTES

No caso do deploy ser atualização de uma aplicação existente, o chamado deverá conter, pelo menos, as seguintes informações:

a) Nome da aplicação;
b) Servidor hospedeiro (nome ou IP);
c) Pasta/arquivos de origem e destino dos arquivos de deploy;
d) Script para execução, caso aplicável;
e) Horário para execução (imediato ou agendado, conforme SLA);
f) Observações adicionais, caso necessário.

10.1.2. APLICAÇÕES NOVAS

No caso do deploy ser atualização de uma aplicação nova, o chamado deverá conter, pelo menos, as seguintes informações:

a) Nome da aplicação (completo e sigla);
b) Qual o público-alvo que acessará a aplicação (interno/externo/comarcas/etc);

c) Se a aplicação deverá ser acessível via Internet;
d) Qual o volume de acessos esperado;
e) Quais os requisitos de recursos computacionais estimados;
f) Sinopse do funcionamento da aplicação, inclusive o funcionamento interno (bancos, webservices, etc);
g) Quais as tecnologias na qual a aplicação foi desenvolvida;
h) Quais as dependências que a aplicação precisa para funcionar, caso aplicável;
i) Quem são os desenvolvedores responsáveis pela aplicação.

10.1.3. CASOS EMERGENCIAIS

Em casos excepcionais onde a aplicação necessita de deploy imediato e a execução do processo padrão não seja possível ou comprometa o Égregio, será aceito a solicitação de deploy através de contato telefônico do Coordenador de Aplicações. O chefe do Serviço de Segurança e Sistemas Básicos deverá receber este contato telefônico.

Nesta situação, ainda assim será necessário abrir o chamado posteriormente, somente para efeito de registro.

10.2. EXECUÇÃO DO DEPLOY

Na fase de execução do deploy, todas as interações serão realizadas pela ferramenta OTRS e o operador responsável pelo chamado assentará todas as informações pertinentes.

Será de inteira responsabilidade do proprietário a transferência de todos os arquivos necessários para a execução do deploy até o horário previsto informado na abertura do chamado.

Caso esteja pendente ou faltando alguma informação, o chamado poderá ser encerrado por informações insuficientes para execução, sendo que o operador tentará quando possível sanar estes problemas. Sendo que nesta situação não será possível garantir a execução no horário solicitado.

Após a execução, serão informadas todas as informações pertinentes, sejam elas de sucesso ou falha. Em caso de falha o chamado permanecerá aberto até que sejam solucionadas as falhas de modo que a aplicação fique disponível novamente. Caso isto não seja possível, o proprietário do chamado deverá informar a situação para cancelar, abortar execução ou restaurar versão anterior.

No caso de restaurar a versão anterior da aplicação, o responsável/proprietário será o responsável por disponibilizar o(s) arquivo(s) correto(s), não sendo de responsabilidade de quem executa o deploy salvaguardar a versão anterior.

10.3. ACORDO DE NIVEL DE SERVIÇO

O prazo padrão para atendimento de deploy será de até 1 (uma) hora após a solicitação, sendo este caracterizado como “imediato”. Este deverá respeitar o horário de abertura do chamado que compreende das 08h00 às 15h00. No caso do deploy “agendado”, compreenderá qualquer horário solicitado que seja superior ao SLA padrão.

Os horários para deploy deverão preferencialmente ocorrer após as 14h00, sendo este o horário onde o fluxo de acesso aos sistemas apresenta uma diminuição em sua utilização, visando desta forma o menor impacto possível ao Egrégio, bem como disponibilidade nos serviços disponibilizados.

Nos casos esporádicos onde o deploy necessita ser realizado fora do de expediente, isto é, após as 16h00, o mesmo deverá possuir, no mínimo, 48 (quarenta e oito) horas de antecedência a fim de viabilizar os recursos necessários para realizar a operação solicitada.

10.4. FECHAMENTO DO CHAMADO

O chamado será fechado somente após a homologação do proprietário atestando o perfeito funcionamento da aplicação. O prazo para homologação será de até 24 (vinte e quatro) horas após a execução do deploy. Decorrido o prazo sem resposta, este será automaticamente encerrado como solucionado.

Caso o proprietário do chamado informe para cancelar, abortar execução ou restaurar versão anterior, o chamado será encerrado como não solucionado ou falha.

11. RELATORIOS GERENCIAIS E INDICADORES

Caso necessário, poderá ser gerado relatório a partir da ferramenta de chamados, sendo este contendo as solicitações de deploy em um determinado intervalo de tempo, bem como se houve descumprimento do tempo estabelecido no ANS.

12. CONSIDERAÇÕES FINAIS

Esclarecimentos adicionais sobre a norma poderão ser obtidos junto a Secretaria de Informática, no Serviço de Segurança e Sistemas Básicos.

13. APROVAÇÃO

Este normativo entra em vigor a partir da data de publicação.

IX - VIDEOCONFERÊNCIA

1. ASSUNTO/OBJETIVO

Definição de procedimentos para videoconferência entre as unidades organizacionais do Tribunal de Justiça do Pará (TJPA).

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Este manual tem por objetivo informar e viabilizar a realização de reuniões administrativas utilizando a tecnologia de videoconferência. A adoção desse recurso propicia maior segurança, redução de custos com deslocamentos, possibilitando reuniões online entre as unidades organizacionais deste Tribunal de Justiça, de acordo com a disponibilidade de agenda individual de cada unidade.

Caberá aos interessados o agendamento prévio, via Portal Interno do TJPA, de acordo com a disponibilidade das salas/equipamentos de videoconferência do TJPA.

A Secretaria de Informática ficará responsável pela viabilização técnica da infraestrutura necessária para a realização da videoconferência, previamente agendada, ficando sob a responsabilidade dos gestores das unidades a disponibilização de agenda e confirmação dos participantes.

3. UNIDADE GESTORA

Secretaria de Informática.

4. PÚBLICO ALVO

Servidores, magistrados e Superintendência do Sistema Penal do Estado (SUSIPE).

5. RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica

6. REGULAMENTAÇÃO UTILIZADA

Portaria 4.618/2013 de 19/11/2013

7. DEFINIÇÕES E CONCEITOS BÁSICOS

7.1. Videoconferência

Tecnologia que proporciona a pessoas situadas geograficamente distantes a participarem de uma mesma reunião simultaneamente, de forma que todos os participantes possam se encontrar através da comunicação audiovisual em tempo real, e possam dialogar entre si. Basicamente define-se Videoconferência como a transmissão e recepção sincronizada de imagens (vídeo) e fala (áudio) entre duas ou mais pessoas/grupos de pessoas utilizando equipamentos específicos e conexões de rede/Internet.

7.2. Infraestrutura de Videoconferência

Os equipamentos de videoconferência (terminais ou CODECs) possuem capacidade de estabelecer uma comunicação ponto a ponto e ponto-multiponto.

Para comunicação entre vários pontos simultaneamente é necessária a utilização de um equipamento denominado MCU (Multipoint Control Unit). O funcionamento da MCU, assim como de outros componentes necessários à videoconferência são especificados pelo protocolo H.323 ou SIP.

7.2.1. MCU

Unidade de Controle Multiponto (em inglês: Multipoint Control Unit) é um dispositivo normalmente utilizado para conectar diversos pontos de videoconferência.

7.2.2. CMS

Aplicativo disponível no Portal Interno do TJ, responsável pelo gerenciamento da agenda de videoconferência. Esta ferramenta viabilizará a disponibilização de horários e controle dos participantes, que posteriormente serão notificados via e-mail acerca da confirmação para participação na videoconferência agendada.

7.2.3. Ambiente de Videoconferência

- Ambiente coletivo: Sala de videoconferência é composta basicamente por um endpoint hardware, câmera, microfone multidirecional e TV;
- Ambiente individual: Estação de trabalho (computador desktop ou notebook) equipada com webcam, microfone e software Polycom (CMA desktop) ou telefone multimídia – Polycom VVX.

7.3. ENDPOINT

7.3.1. Endpoint Hardware

7.3.1.1. Codec (HDX)

Dispositivo que oferece vídeo em alta definição e áudio superior para
aplicações empresariais permitindo a realização de videoconferência ponto a ponto e multiponto.

7.3.1.2. Telefone multimídia Polycom VVX
Telefone IP multimídia que unifica as capacidades de voz, vídeo e aplicações em um único equipamento permite a realização de videoconferências ponto a ponto e ponto multiponto.

7.3.2. Endpoint Software
7.3.2.1. Software Converged Management Application (CMA) Desktop
Aplicativo de vídeo que permite comunicação em tempo real em sistemas e sistemas operacionais distintos com recursos para ambientes PC com suporte

a SIP. O software CMA Desktop é implantado e gerido pelo Polycom CMA do sistema 5000/4000.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS
ANEXO I – Fluxo de agendamentamento de videoconferência;
ANEXO II – Manual de utilização de agendamento via portal;
ANEXO III – Manual de utilização do endpoint software CMA Desktop;
ANEXO IV-A – Manual de utilização do endpoint hardware HDX;
ANEXO IV-B – Manual de utilização do endpoint hardware HDX – Dicas rápidas;
ANEXO V – Manual de utilização do endpoint hardware VVX.

9. COMPETÊNCIAS E RESPONSABILIDADES
- A Secretaria de Informática: responsável pela viabilização técnica de infraestrutura necessária para a realização da videoconferência.
- A Unidade gestora: responsável por administrar determinada agenda: Criar, alterar, cancelar e excluir compromissos da agenda.
- Unidade participante: Pessoa ou unidade habilitada a solicitar videoconferência em determinada agenda disponível no portal interno.

10. PROCEDIMENTOS
- O gestor da agenda (unidade) disponibiliza horário, via portal interno, para realização da videoconferência;
- O servidor ou magistrado seleciona o horário disponibilizado;
- O sistema de agendamento (CMS) envia e-mail para validação pelo gestor da disponibilização do agendamento e para o solicitante notificando-o do pedido de agendamento;
- O gestor valida o pedido de agendamento;
- O solicitante recebe e-mail com as informações necessárias para a realização da videoconferência.

11. RELATÓRIOS GERENCIAIS E INDICADORES
Não se aplica

12. CONSIDERAÇÕES FINAIS
Este normativo define os procedimentos necessários para a realização de videoconferência entre as unidades organizacionais do TJPA via portal interno.