PRESIDÊNCIA

O Desembargador RÔMULO JOSÉ FERREIRA NUNES, Presidente do Tribunal de Justiça do Estado do Pará, no uso de suas atribuições legais, etc. RESOLVE:

PORTARIA Nº1045/2010-GP. Belém, Pa, 27 de agosto de 2010.

Dispõe sobre normas gerais de utilização de recursos de Tecnologia de Informação e Comunicação deste Poder Judiciário.

CONSIDERANDO as recomendações instituídas através da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO do Poder Judiciário do Pará e as DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO publicadas na Portaria nº 990/2009 - GP, de 06 de maio de 2009;

CONSIDERANDO a necessidade de estabelecer normas que efetivem a adoção da política de segurança.

Art.1º Os equipamentos de informática disponibilizados nas unidades do Poder Judiciário Estadual destinam-se, exclusivamente, ao atendimento das necessidades de serviço do Órgão. Parágrafo único Os arquivos armazenados nos equipamentos de informática são de propriedade deste Tribunal.

Art.2º É proibida a instalação, em qualquer equipamento de informática, de produtos(hardware) ou serviços (software) que não tenham sido homologados pela Secretaria de Informática do Tribunal. Parágrafo único. A Secretaria de Informática poderá proceder a desinstalação sumária dos itens que não se enquadrem nos critérios estabelecidos neste artigo.

Art. 3º Os parâmetros de configuração dos sistemas computacionais (computadores, sistemas operacionais, sistemas corporativos, configurações de usuários, permissões e tudo mais que diga respeito aos recursos de tecnologia da informação e comunicação) serão definidos pela Secretaria de Informática, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do Poder Judiciário.

§1º Incluem-se nas definições do caput os serviços disponíveis por meio da Internet cuja utilização seja permitida no âmbito da rede local, considerados os riscos à segurança do ambiente computacional do Poder Judiciário.

§2º Será considerada não-autorizada qualquer modificação efetuada em parâmetros dissonantes das definições estabelecidas.

Art.4º O servidor que apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, arquivo ou programa de computador; fizer uso, de forma indevida ou não- autorizada, dos equipamentos de informática; bem como agir em desacordo com os termos esta portaria, fica sujeito à aplicação das penalidades previstas na lei.

Art. 5º O acesso aos recursos da rede de computadores é garantido a todos os magistrados e servidores do Poder Judiciário, bem como o uso dos recursos de tais equipamentos.

§1º O credenciamento para uso dos recursos computacionais do Tribunal será feito pela Secretaria de Informática, mediante solicitação por escrito, através de documento modelo, assinada pelo superior hierárquico do servidor, ou funcionário de empresa contratada.

§2º O acesso aos recursos da rede poderá ser garantido aos estagiários e aos funcionários de empresas contratadas pelo Tribunal, mediante solicitação formal dos titulares das unidades onde os estagiários estejam lotados ou dos gestores dos contratos, respectivamente.

§3º Os direitos de acesso a cada recurso serão configurados pela Secretaria de Informática, observadas as necessidades do serviço.

§4º Os direitos de acesso a cada recurso poderão ser retirados mediante solicitação do responsável pela unidade de lotação do servidor ou dos responsáveis pelos estagiários e funcionários de empresas contratadas.

§5º Caberá a cada magistrado, servidor, estagiário ou funcionário de empresa contratada, manter em sigilo sua senha de acesso aos recursos computacionais, bem como proceder à sua atualização dentro dos períodos estabelecidos pela Secretaria de Informática.

§6º A senha de acesso é de uso pessoal e intransferível, ficando vedado seu empréstimo ou cessão a terceiros sob qualquer pretexto.

Art.6º É de responsabilidade da Secretaria de Informática monitorar os acessos aos recursos computacionais efetuados através de suas redes de comunicação a partir de registros de auditoria gerados por sistemas de auditoria, incluindo o acesso à Internet e o uso do correio eletrônico, objetivando verificar sua adequação às normas estabelecidas na Política.

Art.7º A Secretaria de Informática poderá criar listas de correio eletrônico contendo um subconjunto dos servidores e/ou magistrados, de forma a facilitar o processo de comunicação institucional.

§1º As mensagens, imagens, e/ou notas enviadas devem ser compatíveis com as atribuições do servidor, e não devem configurar-se como correntes, propagandas comerciais, políticas ou religiosas.

§2º Cabe à Secretaria de Informática estipular os limites de utilização do correio eletrônico que se façam necessários para o bom funcionamento do serviço, aí incluídos a quantidade de destinatários, o tamanho máximo das mensagens enviadas/recebidas e o tamanho máximo de caixa postal, além dos tipos de arquivo permitidos como anexos às mensagens.

Art.8º É de responsabilidade do Departamento de Gestão de Pessoas informar à Secretaria de Informática sobre todo e qualquer desligamento, exoneração ou afastamento por tempo superior a trinta dias, para que as medidas de segurança referentes à suspensão de direitos de uso sejam tomadas.

Art.9º A Secretaria de Informática fará regularmente cópia de segurança dos arquivos armazenados em seus computadores centrais.

§1º É de responsabilidade de cada usuário realizar cópias de segurança de seus arquivos armazenados nos discos locais de suas estações de trabalho.

§2º A Secretaria de Informática disponibilizará instruções sobre os procedimentos para a execução de cópia de segurança dos arquivos locais.

Art.10. O endereço eletrônico institucional dos servidores e magistrados, criado e armazenado nos servidores de correio eletrônico mantidos pela Secretaria de Informática, é o meio oficial de envio e recebimento de informações, instruções e mensagens no âmbito deste Poder Judiciário, devendo seu uso ser amplamente fomentado e priorizado.

Art.11. Os prejuízos à estabilidade e continuidade dos serviços, causados pela exclusão, destruição, modificação, instalação ou qualquer ação em desacordo com os termos desta portaria ficarão sujeitos a processo administrativo disciplinar.

Art.12 A Secretaria de Informática deverá disponibilizar internamente, através do Portal institucional na Intranet, os documentos que compõem a Política de Segurança da Informação.

Art.13 Esta portaria entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

PORTARIA Nº1046/2010- GP. Belém, Pa, 19 de agosto de 2010.

Dispõe sobre normas específicas de utilização de recursos de Tecnologia de Informação e Comunicação para usuários de informática deste Poder Judiciário.

CONSIDERANDO as recomendações instituídas através da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO do Poder Judiciário do Pará e as DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO publicadas na Portaria nº 990/2009 - GP, de 06 de maio de 2009;

CONSIDERANDO a necessidade de estabelecer normas que efetivem a adoção da política de segurança.

Art.1º. A utilização dos serviços de Tecnologia da Informação e Comunicação disponibilizados por este Tribunal de Justiça deve obedecer as seguintes normas específicas, anexas a esta Portaria, em conformidade com a Política de Segurança da Informação instituída por este Poder:

I. Normas para Utilização da Internet

II. Normas para Utilização de Correio Eletrônico

III. Normas para Gestão de Ativos

IV. Normas para Contas e Senhas de Usuários

V. Definições de termos

Art. 2º. Esta portaria entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

ANEXO 1 - Normas de Utilização da Internet

1. 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. Conceito

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

Considerando que o uso da Internet, no âmbito do Poder Judiciário do Pará, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico. Todos os usuários dos ativos de informação de propriedade ou controlados pelo Poder Judiciário do Pará, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

3. Abrangência

Esta norma deverá ser aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação -TIC para acesso à Internet.

4. Documentos de referência

Diretrizes Básicas de Segurança da Informação, instituídas através da Portaria nº 990/2009 - GP, de 06 de maio de 2009; e Normas Gerais de Utilização de Recursos de TIC, instituídas através da Portaria nº XXXX/2009 - GP, de XX de XXXXXXXXX de 2009.

5. Normas para utilização da INTERNET

a) A 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.

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

c) 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.

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

e) É expressamente proibida a divulgação e/ou o compartilhamento de informações sigilosas em listas de discussão (por exemplo Fóruns) ou bate-papo (por exemplo chat).

f) 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.

g) 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.

h) Haverá possibilidade de geração de relatórios acerca dos sites acessados por usuários num determinado período.

i) 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.

j) 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.

k) 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.

l) É permitido o uso de softwares de comunicação instantânea, tais como ICQ, Microsoft Messenger (MSN), SKYPE e afins, observada sua utilização exclusivamente para fins de trabalho de interesse do Órgão.

m) Não é permitida a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Emule e afins.

n) Não é permitido o acesso a sites de relacionamento tais como Orkut, Facebook, Gazzag e afins.

o) 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.

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

Caso haja bloqueio indevido de algum site, o usuário poderá solicitar o desbloqueio através de e-mail à Secretaria de Informática, bastando informar na mensagem qual a URL bloqueada e a justificativa para o desbloqueio da mesma.

6. Disposições finais

O TJ/PA se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

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

ANEXO 2 - Normas de Utilização de Correio Eletrônico

1. Objetivo

Estabelecer responsabilidades e requisitos básicos para uso dos serviços de Correio Eletrônico, no ambiente de Tecnologia da Informação e Comunicação (TIC) do TJ/PA.

2. Conceito

As redes de comunicação de dados foram concebidas e construídas com um objetivo bem claro: prover comunicação rápida entre dispositivos e pessoas, tornando irrelevante a distância física entre elas. O serviço de correio eletrônico ilustra bem a agilidade, facilidade e rapidez da comunicação tornada possível através das redes, podendo ocasionalmente, ser utilizada para mensagens pessoais curtas e pouco frequentes.

Considerando que o uso dos serviços de Correio Eletrônico, no âmbito do TJ/PA, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Todos os usuários dos ativos de informação (de propriedade ou controlados pelo TJ/PA), ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente por se tratar da utilização do bem público.

3. Abrangência

Esta norma deverá ser aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação -TIC para acesso envio e recebimento de mensagens através do serviço de correio eletrônico.

4. Documentos de referência

Diretrizes Básicas de Segurança da Informação, instituídas através da Portaria nº 990/2009 - GP, de 06 de maio de 2009; e Normas Gerais de Utilização de Recursos de TIC, instituídas através da Portaria nº 1045/2010 - GP, de 19 de agosto de 2010.

5. Regras para utilização do Correio Eletrônico (E-mail)

a) Todas as contas institucionais de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.

b) Os usuários do TJ/PA poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, a critério do titular da unidade, enquanto perdurar o seu vínculo com o órgão.

c) Contas individuais, com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens. Esta regra não se aplica às contas vinculadas aos cargos/funções, por serem inerentes as atribuições desses cargos/funções.

d) O tamanho das caixas postais institucionais será de 150 Mbytes para os usuários ligados à direção da instituição (Presidente, Vice-Presidente, Secretários, Diretores, Coordenadores e Assessores) e Magistrados. Para os demais usuários, 100 Mbytes.

e) As mensagens com arquivos anexados (texto e anexo) ao passarem pelo servidor de correio eletrônico serão encaminhadas conforme os critérios abaixo:

Tamanho	Horário/Obs
Até 5,0 MB	De 06:00 às 00:00 horas
De 5,1 a 10,0 MB	De 00:01 às 05:59 horas
Acima de 10,0 MB	Consultar formas e procedimentos alternativos indicados pela Secretaria de Informática. Sugestões: gravar em pendrive, CD, DVD, etc...

f) O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico.

g) É vedada a utilização do Correio Eletrônico, nas situações abaixo:

i. Acesso não autorizado à caixa postal de outro usuário.

ii. Uso de contas privadas dos usuários, através dos serviços Post Office Protocol - **POP**, Internet Message Access Protocol - **IMAP** e Simple Mail Transfer Protocol - **SMTP** de provedores externos ao domínio tjpa.jus.br. O acesso às contas privadas de correio (Hotmail, Gmail, Yahoo e outras) somente será permitido através do serviço de Webmail (navegadores como Internet Explorer, Mozilla Firefox, Google Chrome e similares).

iii. Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e a

ordem pública.

iv. Envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou 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).

v. Envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, opção sexual ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados.

vi. Envio de mensagens do tipo "corrente" ou "spam".

vii. Envio de mensagens do tipo propaganda político-eleitoral.

viii. Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas.

ix. Envio de mensagens que contenham arquivos com código executável tais como .exe, .com, .bat, .pif, .js, vbs, .hta, .src, .cpl, .reg, .dll, .inf ou qualquer outro tipo que represente risco à segurança, conforme critérios estabelecidos pela Gerência de Segurança da Informação do TJ/PA.

x. Utilização de listas e/ou grupos de contatos do TJ/PA ou de qualquer outra entidade para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou grupos de contatos em questão.

xi. Todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa o andamento dos serviços deste Poder Judiciário.

xii. As mensagens dos usuários deverão conter, no seu final, aviso padronizado quanto a responsabilidade legal do conteúdo da mensagem (*disclaimer*), a ser disponibilizado no portal do TJ/PA na área de Política de Segurança da Informação.

6. Disposições finais

O TJ/PA se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

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

ANEXO 3 - Normas para Gestão de Ativos

Objetivo

Alcançar e manter a proteção adequada dos ativos do ambiente de Tecnologia da Informação e Comunicação (TIC) do TJ/PA, definindo as responsabilidades de seus agentes responsáveis e custodiantes.

Conceitos

Segundo a nova norma ABNT NBR ISO/IEC 17799:2005, convém que todos os ativos sejam inventariados, identificados e mantidos, tendo um agente responsável e/ou um custodiante que deverão adotar procedimentos específicos para controle do uso, manutenção e proteção adequada do ativo.

Desta forma, a presente norma define claramente quais as responsabilidades que os usuários terão ao serem designados como agentes responsáveis ou custodiantes de algum ativo tecnológico.

Abrangência

Esta norma deverá ser aplicada a todos os usuários que sejam agentes responsáveis e/ou custodiantes de ativos tecnológicos em uso no TJ/PA.

Documentos de referência

Diretrizes Básicas de Segurança da Informação, instituídas através da Portaria nº 990/2009 - GP, de 06 de maio de 2009; e Normas Gerais de Utilização de Recursos de TIC, instituídas através da Portaria nº 10452010 - GP, de 19 de agosto de 2010.

Equipamentos do tipo servidor

Todo equipamento do tipo servidor terá designado um **Agente Responsável** e um **Custodiante** , que deverão obedecer as normas seguintes, objetivando garantir a segurança e a funcionalidade desses equipamentos.

Todo ativo tecnológico do tipo servidor terá designado um Agente Responsável, o qual deverá:

Manter as informações cadastrais sobre o ativo atualizadas - hardware, software e serviços disponibilizados através daquele ativo.
Atuar como suporte nível 3 , conforme item 9 (nove) deste documento.
Delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária daquele ativo.
Coordenar as ações de solução nos casos de comprometimento da segurança lógica do ativo (invasões de hackers, pixação de sites, problemas na aplicação, etc).
Coordenar as ações de solução nos casos de comprometimento da segurança física do ativo (danos, furto, roubo ou qualquer ameaça física ou do meio ambiente).
Monitorar a atualização de todos os softwares instalados naquele ativo, desde *upgrade* de versão a aplicação de *patches* de correção, observando a importância e as consequências de t ais implementações.
Ter chave de acesso com privilégio de leitura somente.
Obs.: O agente responsável pelo ativo poderá ter acesso com privilégios de administrador sempre que precisar. Para tal, é necessário solicitar formalmente ao custodiante que conceda este acesso, informando sempre o período desejado e as tarefas que serão executadas, caso seja um servidor em produção. Para maiores informações sobre senhas de administrador, consultar o manual de normas e contas e senhas de administradores publicada na Intranet, seção Política de Segurança.

Realizar estudos de planejamento de capacidade de forma a evitar sobrecarga nos sistemas suportados pelo ativo.
Garantir que sistema operacional e aplicativos estejam sujeitos a rígido controle de gestão de mudanças .
Considerar os seguintes aspectos quando da implementação de qualquer tipo de modificação:
Identificação e registro das mudanças significativas.
Planejamento e testes das mudanças.
Avaliações de impactos potencias, incluindo impactos de segurança.
Procedimento formal de aprovação das mudanças propostas.
Comunicação dos detalhes das mudanças para todos os setores e pessoas envolvidas.
Procedimento de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.
Criar e implantar os procedimentos para a geração de cópias de segurança (backup) e sua recuperação (restore) em um tempo aceitável.
Garantir que registros de auditoria (log) contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
Estar ciente que a não observância aos itens aqui definidos sujeita-o às sanções em vigor.

Todo ativo tecnológico do tipo servidor terá designado um Custodiante, que será responsável por:

Ajudar o agente responsável a manter atualizadas as informações cadastrais sobre o ativo (hardware, software e serviços).
Atuar como suporte nível 2 , conforme item 9 (nove) deste documento.
Cuidar do ativo no dia-a-dia, notificando o agente responsável de qualquer anomalia encontrada.
Comunicar imediatamente ao agente responsável qualquer problema de segurança lógica do ativo (invasões de hackers, pixação de sites, problemas na aplicação, etc) e as ações que foram tomadas para sanar/minimizar o problema.
Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia.
Atualizar, a pedido do agente responsável, os softwares de qualquer natureza que rodem no ativo, desde upgrade de versão a aplicação de patches .
Ter chave de acesso com privilégio de administrador nos ativos sob sua custódia.
Realizar as modificações necessárias nos ativos, de acordo com o planejamento de gestão de mudanças definido pelo agente responsável.
Garantir que as cópias de segurança (backup) estão sendo geradas.
Monitorar os registros de auditoria (log), avisando imediatamente ao agente responsável qualquer problema encontrado.
Evitar o acesso aos ativos por pessoas não autorizadas.
Estar ciente de que a instalação de software de qualquer natureza ou a modificação de qualquer configuração sem a autorização por escrito ou por email do agente responsável pelo ativo não é permitida, exceto em casos de suporte técnico.
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Equipamentos do tipo impressoras de rede e multifuncionais

Todo equipamento do tipo impressora de rede ou multifuncional terá designado um Agente Responsável e um Custodiante, que deverão obedecer às normas seguintes, objetivando garantir a segurança e a funcionalidade desses equipamentos.

Todo ativo tecnológico do tipo impressora de rede ou multifuncional instalado no TJ/PA terá designado um Agente Responsável, o qual deverá:

Manter as informações cadastrais sobre o ativo atualizadas (hardware, local de instalação, configuração de rede, etc).
Atuar como suporte nível 3 , conforme item 9 (nove) deste documento.
Delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária daquele ativo.
Coordenar as ações de solução nos casos de comprometimento da segurança física do ativo (danos, furto, roubo ou qualquer ameaça física ou do meio ambiente).
Monitorar a atualização de todos os softwares instalados naquele ativo, desde *upgrade* de versão a aplicação de *patches* de correção, observando a importância e as consequências de t ais implementações.
Ter chave de acesso com privilégio de administrador, para que possa efetuar as configurações de rede e outras necessárias ao funcionamento adequado do equipamento .
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Todo ativo tecnológico do tipo impressora de rede ou multifuncional instalado no TJ/PA terá designado um Custodiante, que será responsável por:

Ajudar o agente responsável a manter atualizadas as informações cadastrais sobre o ativo.
Atuar como suporte nível 2 , conforme item 9 (nove) deste documento.
Cuidar do ativo no dia-a-dia, notificando o agente responsável de qualquer anomalia encontrada.
Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia.
Evitar o acesso aos ativos por pessoas não autorizadas.
Estar ciente de que a instalação de software de qualquer natureza ou a modificação de qualquer configuração sem a autorização por escrito ou por email do agente responsável pelo ativo não é permitida, exceto em casos de suporte técnico.

Coibir qualquer modificação nos equipamentos e/ou softwares, por quem quer que seja, exceto quando autorizada por escrito ou por email pelo agente responsável pelo ativo.
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Equipamentos do tipo estações de trabalho, impressoras comuns e periféricos em geral

Todo equipamento do tipo estações de trabalho, impressoras comuns (não multifuncionais ou de rede) e periféricos em geral (scanners, câmeras filmadoras, etc) terá designado um Agente Responsável, que exercerá também o papel de Custodiante e deverá obedecer às normas seguintes, objetivando garantir a segurança e a funcionalidade desses equipamentos.

Todo ativo tecnológico do tipo estações de trabalho, impressoras comuns e periféricos em geral instalado no TJ/PA terá designado um Agente Responsável, o qual deverá:

Cuidar do ativo no dia-a-dia, notificando a Secretaria de Informática de qualquer anomalia encontrada, tais como problemas na aplicação ou mau funcionamento do equipamento.
Abrir o chamado técnico na Central de Serviços, prestando as informações solicitadas e executando as ações preliminares indicadas para os testes e resolução dos problemas.
Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia.
Atualizar periodicamente os softwares de qualquer natureza instalados no ativo (sistema operacional, antivírus e dos sistemas corporativos).
Ter chave de acesso com privilégio de administrador nos ativos sob sua custódia.
Realizar as cópias de segurança (backup) dos arquivos de trabalho armazenados localmente .
Evitar o acesso aos ativos por pessoas não autorizadas.
Estar ciente de que a instalação de software de qualquer natureza ou a modificação de qualquer configuração sem a autorização expressa do agente responsável pelo ativo não é permitida.
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Equipamentos ativos de rede

Todo equipamento ativo de rede (*switch* , roteador, *access point* , *appliance* , etc) terá designado um Agente Responsável e um Custodiante, que deverão obedecer às normas seguintes, objetivando garantir a segurança e a funcionalidade desses equipamentos.

Todo equipamento ativo de rede instalado no TJ/PA terá designado um Agente Responsável, o qual deverá:

Manter as informações cadastrais sobre o ativo atualizadas (hardware, software, configurações e serviços disponibilizados através daquele ativo).
Atuar como suporte nível 3 , conforme item 9 (nove) deste documento.
Delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária daquele ativo.
Coordenar as ações em casos de comprometimento da segurança lógica do ativo.
Coordenar as ações em casos de comprometimento da segurança física do ativo (danos, furto, roubo ou qualquer ameaça física ou do meio ambiente).
Manter atualizado todos os softwares que rodem naquele ativo, desde upgrade de versão a aplicação de patches .
Ter chave de acesso com privilégio de Administrador .
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Todo equipamento ativo de rede instalado no TJ/PA terá designado um Custodiante, que será responsável por:

Notificar o agente responsável sobre qualquer anomalia verificada no ativo.
Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia.
Evitar o acesso aos ativos por pessoas não autorizadas.
Estar ciente que a não observância aos itens aqui representados sujeita-o às sanções em vigor.

Suporte

Foram definidos 3 (três) níveis de suporte para os ativos, a saber:

Nível de suporte	Responsável	Atividades
Suporte 1º nível	Técnicos da Central de Serviços	Testes de conectividade: ping, traceroute e similares; Monitoramento de serviços - up/down; Aviso ao custodiante e/ou agente responsável em caso de falha no ativo; Outras atividades, a serem acordadas entre os envolvidos.
Suporte 2º nível	Custodiante do ativo	Realizar todas as atividades de competência do suporte de 1 o nível; *Reboot* após autorização por escrito ou por email do agente responsável ; Quando na impossibilidade de resolução do problema, notificar imediatamente o suporte de 3º nível.
Suporte 3º nível	Agente responsável pelo ativo	Realizar todas as atividades de competência do suporte de 2 o nível; Quando na impossibilidade de resolução do problema, este será responsável em acionar suporte externo.

Disposições finais

O TJ/PA se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

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

Anexo 4 - Normas para Contas e Senhas de Usuários

Objetivo

Estabelecer os procedimentos para fornecimento e uso adequado das contas e definição das senhas de usuários no ambiente de Tecnologia da Informação e Comunicação (TIC) do TJ/PA.

Conceito

Segundo a norma ABNT NBR ISO/IEC 17799:2005, item 11.2, convém que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

Convém ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2) e que a criação de contas e a concessão de senhas seja controlada através de um processo de gerenciamento formal (item 11.2.3).

Desta forma, o TJ/PA elaborou esta norma para fornecimento e utilização de contas e senhas de usuários em geral, que se aplica tanto a usuários comuns como a usuários administradores, objetivando evitar o uso inapropriado e que contribuirá evitar falhas ou violações de sistemas.

Abrangência

Esta norma deverá ser aplicada a todos os usuários de ativos do ambiente de Tecnologia da Informação e Comunicação - TIC do TJ/PA.

Documentos de referência

Diretrizes Básicas de Segurança da Informação, instituídas através da Portaria nº 990/2009 - GP, de 06 de maio de 2009; e Normas Gerais de Utilização de Recursos de TIC, instituídas através da Portaria nº 10452010 - GP, de 19 de agosto de 2010.

Normas para solicitação e fornecimento de contas e senhas

A criação de contas de usuários poderá ser solicitada para todos os magistrados, servidores (inclusive os requisitados) e estagiários do Poder Judiciário do Pará.

A solicitação deverá ser protocolada e encaminhada à Secretaria de Informática, podendo ser utilizado formulário padrão disponibilizado na Intranet do TJ/PA, ou qualquer outro documento que contenha todas as informações requisitadas no respectivo formulário.

Magistrados e Secretários poderão solicitar a criação de suas próprias contas.

A solicitação de criação de contas de servidores deverá ser assinada pelo superior hierárquico nos níveis de Magistrado, Secretário, Diretor e Coordenador.

Depois de cadastrada, a conta do usuário deverá ser incluída na unidade ao qual está vinculado, com as permissões cabíveis ou solicitadas, sendo obrigatório que o usuário troque sua senha no primeiro acesso.

Para o acesso remoto via VPN e para o acesso ao serviço de FTP, as solicitações são feitas pelo superior hierárquico nos níveis de Magistrado, Secretário, Diretor e Coordenador, através de documento formal contendo a devida justificativa.

Deve-se atribuir o menor privilégio possível a uma conta, de forma a permitir a realização das tarefas pertinentes ao seu usuário, e apenas isto.

Os sistemas e aplicações deverão ter mecanismos que impeçam a exibição na tela de login do último usuário a acessá-los.

Os sistemas e aplicações deverão ter mecanismos que impeçam a exibição, na tela de login, da senha referente ao respectivo login em uso, devendo exibir caracteres como asteriscos ou similares.

Normas para utilização de contas e senhas

A senha é de uso pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da mesma, conforme previsto na legislação.

Para o acesso à internet através da rede do TJ/PA será requisitada identificação do usuário (conta e senha) no momento do primeiro acesso de cada sessão de uso, possibilitando a identificação do mesmo e da navegação realizada.

Os acessos bem sucedidos e as falhas nas tentativas de logon serão registrados para efeito de auditoria.

Normas para a formação de contas e senhas

As senhas para usuários comuns deverão conter no mínimo 8 (oito) caracteres, e para usuários administradores no mínimo 14 (quatorze) caracteres, sendo facultado o uso de letras e números. Como recomendação para fortalecimento da segurança, sugere-se a utilização de caracteres em caixa alta (maiúsculas), caixa baixa (minúsculas) e caracteres especiais ($, %, &, #, @, ...). Sugere-se também a elaboração de senhas com o maior número de caracteres possível e confortável para o usuário, de forma a dificultar tentativas indevidas de acesso.

Os sistemas e aplicações deverão prover mecanismos que garantam que somente sejam aceitas senhas com a formação anteriormente citada.

Deverá ser evitada a composição de senhas com sequências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento e palavras contidas em dicionário). Tais restrições deverão ser informadas aos usuários para efeito de formação das suas senhas.

As contas com privilégio de administrador não poderão conter em sua formação algo que as identifique como sendo uma conta de administrador. Por exemplo: admin, adm, administrador, administrator, pradmin ou similares.

Deverá ser criada uma ou mais contas, sem nenhum privilégio, com formação que possa sugerí-la como sendo uma conta de administrador. Essas contas deverão ser constantemente submetidas a auditoria, com o propósito de se verificar as tentativas de utilização das mesmas.

Normas para tempo de vida de contas e senhas

O usuário será obrigado a trocar sua senha no ato do seu primeiro login.

Os sistemas guardarão um histórico de senhas, composto pelas 12 (doze) últimas senhas usadas, para fim de evitar suas reutilizações.

O tempo mínimo, por vontade do usuário, para troca de senhas deverá ser de 2 (dois) dias.

A conta deverá ser bloqueada após a 5ª (quinta) tentativa de login com senha incorreta.

O tempo de vida das senhas deverá ser de, no máximo, 90 (noventa) dias, quando deverá ser forçada a sua troca no primeiro login após esse período.

Com antecedência mínima de 7 dias, o sistema deverá avisar da necessidade de troca da senha pela proximidade do término de sua validade.

Contas que ficarem inativas por 60 (sessenta) dias ou mais deverão ser bloqueadas.

Caso o usuário suspeite do comprometimento de sua senha, esta deverá ser modificada imediatamente, através dos mecanismos disponíveis para tal.

Normas para reinicialização de senhas

As contas só poderão ter suas senhas reinicializadas por solicitação formal (documento escrito ou email institucional) do seu detentor à área responsável pela administração das contas (Serviço de Segurança e Sistemas Básicos).

Apenas nos casos de exceção justificados pela extrema necessidade de reinicialização de senha sem a devida solicitação formal prévia, algumas informações cadastrais do usuário deverão ser confirmadas pelo mesmo (procedimento de positivação). Neste caso, a positivação deverá ser realizada por meio do retorno da ligação ao solicitante, para um telefone funcional de sua unidade de lotação.

Normas para bloqueio e reativação de contas

As contas podem ser bloqueadas a pedido do próprio usuário; por inatividade (não utilização por período igual ou superior a 60 dias); ou por ordem formal devidamente justificada de superior hierárquico nos níveis de Magistrado, Secretário, Diretor e Coordenador.

As contas bloqueadas a pedido do próprio usuário ou por inatividade poderão ser reativadas a pedido do próprio usuário, mediante documento formal ou procedimento de positivação via contato telefônico.

As contas bloqueadas por determinação de superior hierárquico somente poderão ser reativadas mediante documento formal emitido pelo superior hierárquico nos níveis de Magistrado, Secretário, Diretor e Coordenador.

Normas para destruição de contas de usuário

A destruição de uma conta de usuário ocorrerá por determinação da administração do TJ/PA através de documento expedido pelo Departamento de Gestão de Pessoas - DGP, ou por solicitação formal do superior hierárquico do detentor da conta, nos níveis de Magistrado, Secretário, Diretor e Coordenador. Em ambos os casos, o documento deverá estar devidamente justificado.

O Departamento de Gestão de Pessoas - DGP deverá comunicar mensalmente à Secretaria de Informática o desligamento ou remanejamento de qualquer usuário.

Durante o processo de destruição de conta de rede, o conteúdo da pasta do usuário na rede deverá ser resguardado sob a forma de cópia de segurança (backup) por um período de 120 (cento e vinte) dias, após o qual deverá ser destruído definitivamente.

Disposições Gerais

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

ANEXO 5 - Definições de termos

1- Definições

Termo	Definição
Administrador	Conta que permite acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas.
Agente responsável	Identifica uma pessoa que tenha uma responsabilidade autorizada para controlar e fiscalizar o uso e a segurança dos ativos.
Arquivos infectados	Aqueles que sofreram a ação de vírus eletrônico.
Ativo	Qualquer coisa que tenha valor para a organização [ISSO/IEC 13335-1:2004]; Os ativos podem ser de vários tipos, incluindo: ativos de informação; ativos de software; ativos físicos; serviços; ativos intangíveis, tais como reputação e a imagem da organização.
Caixa Postal **Correio eletrônico**	Espaço em disco onde são armazenadas as mensagens de correio eletrônico.
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.
Códigos Maliciosos ou Agressivos	Qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico.
Conta de correio institucional	Conta de correio eletrônico pertencente ao TJ/PA ("tj.pa.gov.br" ou "tjpa.jus.br"), podendo ser individual (um único usuário) ou de um grupo de usuários.
Conta de correio privado	Conta de correio eletrônico externo ao TJ/PA (Hotmail, Gmail, Yahoo, etc...).
Contas	Ver chave de acesso.
Correio Eletrônico	Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.
Criptografia	Tecnologia que consiste na cifragem e decifragem de mensagens, de forma a garantir a segurança, e o sigilo no envio de informações.
Custodiante do ativo	Identifica uma pessoa que usa e/ou cuida do ativo no dia-a-dia [ISO/IEC 13335 1:2004 Item 7.1.2].
Disclaimer	Mensagem de advertência legal, normalmente colocada ao final de uma mensagem eletrônica, informando ao destinatário sobre o sigilo, confidencialidade, responsabilidade e procedimentos a serem tomados em caso de envio incorreto da mensagem.
Download	Baixar um arquivo ou documento de outro computador, através da Internet.
Ferramenta Tecnológica	Sistema (Conjunto de Programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.
FTP (*File Transfer Protocol)*	Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.
IMAP (Internet Message Access Protocol)	Protocolo de acesso a mensagens eletrônicas que se assemelha ao protocolo POP, diferenciando se pela menor quantidade de dados trafegados quando da leitura dos e mails.
Informações Controladas pelo Governo	São aquelas pertencentes a terceiros, sendo da competência dos Órgãos Públicos a responsabilidade sobre a sua guarda, utilização e divulgação.
Informações de Propriedade do Governo	São aquelas geradas nos ambientes dos Órgãos Governamentais.
Internet	Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.
Intranet	Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os magistrados e servidores possam acessar as informações relativas ao TJ/PA.
Licença de Software	Direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes.
Login/Logon	Termo da língua inglesa, consagrado no campo da informática, que designa o processo através do qual um sistema verifica a autenticidade da identidade (formada pelo binômio identificação e senha) de um usuário, garantindo ou não acesso temporário a recursos disponíveis no sistema.
Logoff	Termo da língua inglesa, consagrado no campo da informática, que expressa o processo de desligamento de um usuário do uso de um sistema, definindo assim o fim de seu uso dos recursos garantidos por ocasião do login/logon.

Modem	Equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações, geralmente através da rede de telefonia.
Órgão Público	Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.
Peer-to-Peer (P2P)	É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.
POP (*Post Office Protocol)* .	Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.
Proprietário do ativo	Pessoa ou instituição que detém a propriedade legal do ativo.
Proxy	Sistema de software responsável por compartilhar acesso à recursos disponíveis na Internet podendo registrar e bloquear estes acessos com base em regras e restrições predefinidas.
Reinicialização	Processo através do qual anula-se a informação contido anteriormente em uma identificação ou sistema, levando-o de volta a um estado inicial predeterminado, com valores definidos pelo agente da reincialização
Servidor de Correio Eletrônico	Equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico.
Sistemas Informatizados	Sistema constituído de programas e/ou equipamentos computacionais.
Sitio (Site)	Páginas contendo informações, imagens, fotos, vídeos, sons, etc, que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.
SMTP (*Simple Mail Transfer Protocol)*	Protocolo de comunicação usado para troca de mensagens na Internet, via correio eletrônico.
Software	Programa de Computador.
Spam	Mensagens cujo conteúdo esteja fora do interesse da instituição, enviada para vários destinatários, sem que os mesmos a tenham solicitado.
Upload	Envio de um arquivo de seu computador para outro, através da Internet.
URL	*Universal Resource Locator* endereço de uma pagina Web, como por exemplo http://www.tjpa.jus.br/.
Usuários	Funcionários, magistrados, prestadores de serviços, fornecedores e estagiários.
Vírus Eletrônico	São pequenos programas que, a semelhança dos vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.
VPN (*Virtual Private Network*)	Tecnologia de rede que permite ao usuário acessar uma rede privada, interna à Instituição, a partir de uma rede pública como a Internet.

PORTARIA N°2159/2010-GP. Belém, 14 de setembro de 2010.

CONSIDERANDO o Ofício nº 371/GP, datado de 06 de setembro de 2010, protocolizado sob nº 2010001049411, oriundo do Supremo Tribunal Federal; COLOCAR o MM. Juiz de Direito Dr. LEONARDO DE FARIAS DUARTE À DISPOSIÇÃO do Supremo Tribunal Federal, para atuar como Magistrado Instrutor no Gabinete do Excelentíssimo Senhor Ministro Joaquim Barbosa, a partir do dia 14 de setembro do corrente ano.

PORTARIA Nº2163/2010-GP. Belém, 15 de setembro de 2010.

CONSIDERANDO o expediente protocolizado sob o nº. 2010001035970; EXONERAR, a pedido, o Exmo. Sr. Dr. ANIBAL NERY EMERICK JUNIOR, do cargo de Juiz de Direito Substituto do Estado do Pará, retroagindo seus efeitos ao dia 09 de agosto de 2010.

PORTARIA Nº2164/2010-GP. Belém, 14 de setembro de 2010.

TORNAR SEM EFEITO, nos termos do § 3º do art. 22 da Lei nº. 5.810 de 24.01.1994, a Portaria nº. 0834/2010-GP de 26/04/2010, publicada no D.J.E. de 27/04/2010, que nomeou WALLACE CARNEIRO DE SOUSA, para exercer o cargo de AUXILIAR JUDICIÁRIO, em virtude do candidato não ter tomado posse no prazo legal.

PORTARIA Nº2165/2010-GP. Belém, 14 de setembro de 2010.

CONSIDERANDO o expediente protocolizado neste Tribunal sob o nº 2010001048214; I -EXONERAR, a pedido, a servidora ELAINE CRISTINA LOPES BARROS, matrícula nº 50687, do Cargo em Comissão de Assistente de Desembargador, REF-CJI, junto ao Gabinete da Exma. Sra. Gleide Pereira de Moura, Desembargadora deste Egrégio Tribunal de Justiça, a contar de 01/09/2010. II - NOMEAR a bacharela ELAINE CRISTINA LOPES BARROS, para exercer o Cargo em Comissão de Assessor de Desembargador, REF-CJS-4, junto ao Gabinete da Exma. Sra. Gleide Pereira de Moura, Desembargadora deste Egrégio Tribunal de Justiça, a contar de 01/09/2010.

PORTARIA Nº2166/2010-GP. Belém, 14 de setembro de 2010.

CONSIDERANDO o expediente protocolizado neste Tribunal sob o nº 2010001048214; I -EXONERAR, a pedido, o servidor TÁSSIO FONSECA BARLETA, matrícula nº 77623, do Cargo em Comissão de Assessor de Desembargador, REF-CJS-4, junto ao Gabinete da Exma. Sra. Gleide Pereira de Moura, Desembargadora deste Egrégio Tribunal de Justiça, a contar de 01/09/2010. II - NOMEAR o bacharel TÁSSIO FONSECA BARLETA, para exercer o Cargo em Comissão de Assistente de Desembargador, REF-CJI, junto ao Gabinete da Exma. Sra. Gleide Pereira de Moura, Desembargadora deste Egrégio Tribunal de Justiça, a contar de 01/09/2010.

PORTARIA Nº2167/2010-GP. Belém, 14 de setembro de 2010.