SEGURANÇA NO USO DA INTRANET

Sumário

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.