ANEXO I

PSI

Índice

1. FINALIDADE

Prover o Tribunal de Justiça do Estado de Sergipe de norma para segurança da informação estabelecendo responsabilidades e diretrizes bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra indisponibilidade, divulgação, acesso e modificação não autorizados de informações e dados.

2. ABRANGÊNCIA

Esta política se aplica, no que couber, às atividades de todos os magistrados, servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito do Tribunal de Justiça do Estado de Sergipe ou quem quer que venha a ter acesso a dados ou informações protegidos por esse documento.

3. FREQUÊNCIA DE REVISÃO

Os instrumentos normativos gerados a partir desta política devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 1(um) ano.

4. PORTAL DE SEGURANÇA DA INFORMAÇÃO

Deverá ser implementado e disponibilizado no portal de segurança da informação a fim de disseminar as políticas aos usuários bem como serviços de monitoração aos gestores. Serão disponibilizados documentos de forma direcionada, conforme o campo de atuação do destinatário, a fim de tratar as peculiaridades de cada atividade.

Este serviço não deverá ser disponibilizado na internet, ou seja, aos usuários externos do TJSE.

5. TERMOS E DEFINIÇÕES

5.1. Segurança da Informação

Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito. A segurança da informação abrange inclusive a segurança das documentações, das áreas e instalações, e das pessoas no que tange ao manuseio das informações que estas possam ter ou fornecer acesso.

5.2. Confidencialidade

Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

5.3. Integridade

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

5.4. Disponibilidade

Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

5.5. Dado

Qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação.

5.6. Informação

Dados organizados e inseridos em um contexto, de maneira a propiciar determinado retorno ao manipulador, permitindo a escolha entre os vários caminhos que possam levar a um resultado.

5.7. Sistema de Informação

Conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção.

5.8. Sistema de Segurança da Informação

Documento que declara o comprometimento da direção e estabelece o enfoque da organização para gerenciar a Segurança da Informação (...) Convém

que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. [ISO/IEC 27002:2005]

5.9. Ativo de Informação

É o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos.

São exemplos de ativos associados com sistemas de informação:

a) bases de informação: base de dados e arquivos, documentação de sistema, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas;

b) ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) ativos físicos: equipamentos computacionais (monitor, computador, notebook, tablet), equipamentos de comunicação (roteador, switch, modem, PABX, fax), mídia de armazenamento computacional (fitas e discos), outros equipamentos técnicos (nobreaks, ar-condicionado), mobília, acomodações, cofres, instalações;

d) serviços: computação e serviços de comunicação, utilidades gerais, por exemplo iluminação, eletricidade e refrigeração.

5.10. Usuário

Indivíduo com acesso autorizado a dados e informações de acordo com as restrições e permissões definidas.

5.11. Colaborador

Todas as pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, incluindo prestadores de serviço, consultores e estagiários.

5.12. Plano de Continuidade

Abrange ações que envolvem respostas a eventos extraordinários, ações relativas à garantia da continuidade de processos e ações de recuperação ou de reposição de sistemas. Tem por objetivo manter em funcionamento os

serviços e processos críticos na eventualidade da ocorrência de desastres, atentados e falhas.

5.13. Incidente de segurança de informação

Conjunto de atividades ou eventos correlacionados entre si, vinculados à confidencialidade, integridade ou disponibilidade da informação.

5.14. Direito de acesso

Faculdade de adentrar em um sistema de informação, respeitada a necessidade de conhecer.

5.15. Necessidade de Conhecer

Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações sigilosos.

6. PRINCÍPIOS DE SEGURANÇA

A Política de Segurança da Informação no Tribunal de Justiça do Estado de Sergipe é guiada pelos seguintes princípios:

6.1. Responsabilidade

As responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

6.2. Conhecimento

Para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

6.3. Ética

Todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança.

6.4. Legalidade

Processos de segurança devem levar em consideração os objetivos e a Missão do Tribunal de Justiça do Estado de Sergipe; bem como as leis, normas e políticas organizacionais, administrativas, contratuais, técnicas e operacionais;

6.5. *Proporcionalidade*

O nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

6.6. Integração

Os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente.

6.7. Celeridade

As ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível.

6.8. Revisão

Os sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo e com a necessidade.

6.9. Liberdade

Um sistema de segurança da informação deve ser alimentado com o legítimo uso e fluxo de informações/dados. Devendo ser observadas as normas de privacidade e de direito de realização de auditorias.

7. SEGURANÇA ORGANIZACIONAL

7.1. Gerenciamento da Segurança da Informação

O controle, a implementação e a manutenção da segurança da informação são de responsabilidade da seguinte infraestrutura de gerenciamento:

a) Autoridade máxima: é responsável pela aprovação da Política de Segurança da Informação representado pelo Presidente em exercício do Tribunal de Justiça do Estado de Sergipe.

b) Comitê Gestor da Segurança da Informação que será composto pelo Secretário de TI (Gestor da Informação), pelo Gerente de segurança da informação, por um integrante da Diretoria de Segurança, um integrante da Consultoria Jurídica, um integrante da Diretoria de Pessoas, um integrante do Departamento de Obras, um Juiz auxiliar da Presidência e um Juiz corregedor, deverá ter como obrigações:

i. ser composto por magistrados e servidores públicos;
ii. garantir que a segurança seja parte do planejamento dos processos de tratamento da informação;
iii. garantir direcionamento claro e suporte de recursos e de gerência aos envolvidos nas atividades de segurança da informação;
iv. deliberar sobre as diretrizes, normas e procedimentos de segurança da informação propostas por iniciativa dos próprios membros ou do Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação - GATI, bem como sobre alterações na Política de Segurança da Informação;
v. analisar criticamente os incidentes de segurança da informação encaminhando sugestões de mitigação;
vi. tratar os casos omissos a esta política encaminhando ao órgão competente quando necessário.

c) Gerente de Segurança da Informação: é função atribuída ao Chefe de Divisão de Redes, servidor efetivo do Tribunal de Justiça do Estado de Sergipe, que será responsável por todas as atividades relacionadas com a Segurança da Informação, o qual, além de possuir formação profissional(especialização ou certificação de entidade reconhecida) e experiência compatíveis com o grau de responsabilidade da função, deverá:

i. dispor de autoridade suficiente para que suas determinações sejam acatadas em todo Tribunal de Justiça do Estado de Sergipe;
ii. ser membro integrante do Comitê Gestor da Segurança da Informação;

iii. reportar-se diretamente ao Comitê Gestor da Segurança da Informação de modo a evitar que as recomendações sobre questões de segurança da informação sejam diluídas ou ignoradas pela gerência intermediária no interesse da eficiência operacional;

iv. gerenciar o Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação;

v. ser responsável pela gestão do conhecimento e pelas experiências internas para garantir consistência e fornecer auxílio nas tomadas de decisão sobre segurança da informação;

vi. orientar e oferecer recursos necessários em processos de investigação decorrentes de suspeitas de incidente ou violação de segurança da informação;

vii. difundir e promover o cumprimento da Política de Segurança da Informação pelas diversas áreas, enfatizando a responsabilidade de cada uma no tratamento da informação e dirimindo dúvidas quando necessário.

d) Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação - GATI, cujos membros devem dedicar-se às atividades relacionadas à Segurança da Informação, sendo responsável por:

i. participar da elaboração de planos de continuidade;

ii. realizar auditorias, monitoração de uso e inspeções para avaliação da conformidade com as normas de segurança da informação em vigor;

iii. revisar e manter atualizadas as normas, instruções e procedimentos para tornar efetiva as diretrizes da Política de Segurança da Informação;

iv. propor as regras e atribuir as responsabilidades específicas para a Segurança da Informação;

v. avaliar a adequação e coordenar a implementação de controles específicos de segurança da informação para sistemas (aplicativos e equipamentos) ou serviços;

vi. definir mecanismos e regras de controle que monitorem o cumprimento da Política de Segurança da Informação, implantando os que estiverem sob sua responsabilidade;

vii. propor as metodologias e processos específicos para a Segurança da Informação, tais como análise e avaliação de riscos e sistema de classificação da informação;

viii. dar suporte de segurança da informação às diversas áreas que manipulem informações;

ix. analisar tecnicamente e monitorar incidentes de segurança da informação;

xi. implementar mecanismos que permitam a quantificação, a classificação e o levantamento de custos dos incidentes de segurança da informação e do mau funcionamento de sistemas.

e) Gestor da Informação: é o dirigente da área a ser mais afetada por uma eventual falha no sistema de informação. Representado pelo Secretário de

Tecnologia da Informação, tem a responsabilidade primária pela segurança do sistema, além de:

i. determinar os requisitos de segurança da informação e autoridade para alocar os recursos necessários para alcançá-los;

ii. definir as regras de liberação, bloqueio e autorização de acesso às informações pelas quais é responsável;

iii. contabilizar e classificar a informação;

iv. participar da definição e implantação dos mecanismos de proteção das informações sob sua gestão, em conjunto com o GATI;

v. conduzir processos formais de análise dos direitos de acesso dos usuários, de forma que tais direitos sejam analisados criticamente em intervalos regulares, não excedendo o período máximo de 1 (um) ano, e que as autorizações para direitos de acesso privilegiado sejam analisadas em intervalos mais freqüentes, não excedendo o período máximo de 6 (seis) meses.

f) Proprietário dos Ativos de Informação: é a pessoa responsável pela gerência da infra-estrutura do ativo, atendendo a especificação de qualidade de serviço e os requisitos de segurança da informação formulados pelo gestor da informação, e que poderá delegar formalmente atribuições relativas à Segurança da Informação. Essa função será atribuída ao Diretor de Produção e Suporte associado à Secretaria de Tecnologia de Informação.

7.2. Segurança no acesso de prestadores de serviços

Onde existir a necessidade de acesso de prestadores de serviços aos recursos de processamento da informação, uma avaliação dos riscos envolvidos deve ser feita para determinar as possíveis implicações na segurança e os controles necessários. Estes devem ser acordados e definidos através de instrumento assinado com os prestadores de serviços.

O acesso de prestadores de serviços à informação e aos recursos de processamento da informação não deve ser permitido até que os controles apropriados sejam implementados e um documento definindo os termos para a conexão ou acesso seja assinado.

Esta política deve ser observada no que concerne à assinatura de tais contratos e na contratação externa para processamento da informação.

8. SEGURANÇA EM PESSOAS

8.1. Novos servidores e prestadores de serviço

As responsabilidades de segurança da informação devem ser atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a permanência de cada colaborador.

Todos os magistrados, servidores e prestadores de serviço que utilizam as instalações de processamento da informação devem obedecer ao regimento interno.

8.2. Treinamento dos usuários

Deve ser elaborada uma política de capacitação em segurança da informação para usuários com o objetivo de assegurar que estejam cientes das ameaças e preocupações de segurança da informação e equipados para apoiar a política de segurança da instituição durante a execução normal do seu trabalho.

Os usuários devem ser treinados nos procedimentos de segurança da informação e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

As informações orientativas aos usuários deverão estar presentes no portal de segurança da informação.

8.3. Notificação de falhas e incidentes de segurança da informação e mau funcionamento

Quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços devem ser registradas e imediatamente notificadas aos superiores. Os usuários, para sua própria proteção, não podem, sob nenhuma circunstância, tentar averiguar uma fragilidade suspeita. A investigação de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema.

Os usuários não devem tentar remover um problema suspeito em um aplicativo ou equipamento a menos que sejam autorizados.

Devem ser estabelecidos procedimentos formais para notificação de falhas e incidentes de segurança da informação e mau funcionamento de equipamentos ou aplicativos, bem como procedimentos de resposta a incidentes.

9. CONFORMIDADE

9.1. Conformidade com os requisitos legais

Os estatutos, regulamentações ou cláusulas contratuais relevantes devem ser explicitamente definidos e documentados para cada sistema de

informação. Os controles e as responsabilidades específicos devem ser, de forma similar, definidos e documentados para atender a estes requisitos.

Devem ser adotados procedimentos apropriados para garantir a conformidade com as restrições legais no uso de materiais protegidos por leis de propriedade intelectual, direitos autorais, patentes ou marcas registradas.

Os sistemas de armazenamento de informações, além de disponibilizar os dados em prazos e formatos aceitáveis, devem proteger os registros contra perda, destruição e falsificação, visando à salvaguarda dos registros organizacionais.

9.2. Prevenção contra uso indevido de recursos de processamento da informação

Os recursos de tecnologia da informação e comunicação são de propriedade do Tribunal de Justiça do Estado de Sergipe e são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração.

É considerada imprópria a utilização destes recursos para propósitos não profissionais ou não autorizados. Os magistrados, servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que tomarem conhecimento dessa prática devem levá-la ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

9.3. Monitoração de uso, inspeção de arquivos e auditoria

O grupo de tratamento e respostas de incidentes de segurança da informação pode, a qualquer tempo, monitorar e registrar dados como acessos à rede mundial de computadores (internet), início e fim de conexões à rede, tempo de CPU, utilização de discos feita por cada usuário, registros de auditoria, carga de rede, dentre outros.

Se houver evidência de atividade que possa comprometer a segurança da rede ou dos computadores, o grupo de tratamento e respostas de incidentes de segurança da informação pode monitorar as atividades de um determinado recurso, além de inspecionar arquivos, a bem do interesse da organização. Neste momento tal área deverá enviar relatório de acessos ao gestor responsável.

As ações de monitoração, auditoria e de inspeção são restritas do grupo de tratamento e respostas de incidentes de segurança da informação.

Durante as auditorias de sistemas devem existir controles para salvaguardar a integridade e prevenir o mau uso dos sistemas operacionais e das ferramentas de auditoria.

Ao utilizar os recursos de informática, o usuário concorda com esta política e autoriza implicitamente as ações de auditoria, monitoração e inspeção eventualmente necessárias.

9.4. Cancelamento de acesso

Ao se desligar do Tribunal de Justiça do Estado de Sergipe o magistrado, servidor, colaborador, consultor externo, estagiário ou prestador de serviço deve ter sua autorização de acesso cancelada e não poderá fazer uso de benefícios, contas, senhas de acesso, direitos especiais ou informações.

9.5. Processo disciplinar

A violação das normas de segurança da informação resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais e, em mais alto grau, em penas e sansões legais impostas através de um procedimento administrativo disciplinar.

9.6. Política de segurança para Usuários(PSU)

As restrições, direitos e deveres associados aos usuários de sistemas de informação do TJSE serão estipulados no documento “Política de Segurança para Usuários” que será disponibilizado no portal de Segurança da Informação.

9.7. Questionários de Segurança da Informação

Inicialmente, os acessos de internet dos usuários do TJSE serão definidos através do documento denominado “Questionário-SI-01” que será disponibilizado no portal de Segurança da Informação.

Sempre que necessário, a gerência de segurança da informação deverá enviar questionários aos gestores para definição de novas permissões de usuários.

Os direitos de acesso somente serão disponibilizados, quando preenchidos os questionários, no prazo máximo de 5(cinco) dias úteis.

10. CONCLUSÃO

As diretrizes de segurança da informação estabelecidas neste documento são aplicáveis tanto às informações armazenadas quanto em trânsito e devem ser seguidas por todos os magistrados, servidores, colaboradores, consultores externos, estagiários e prestadores de serviço, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.