GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE FAZENDA E PLANEJAMENTO
SUBSECRETARIA ADJUNTA DE TECNOLOGIA DA INFORMAÇÃO

Política de Segurança da Informação

Norma 001-N1: Diretrizes Gerais

Disposições Preliminares

A Política de Segurança da Informação – PSI, no âmbito da SEFAZ-RJ, tem como pressuposto a garantia de Confidencialidade, Integridade e Disponibilidade dos Ativos de Informação. A PSI deve estar disponível a qualquer tempo a todos os servidores para consulta, devendo ser protegida contra alterações indevidas.

Termos e Definições

Ativos de Informação: patrimônio composto por todos os dados e informações gerados e manipulados nos processos da SEFAZ-RJ.

Ambiente Informatizado: o conjunto de recursos que utiliza ou disponibiliza serviços de processamento de dados e sistemas de informação de uso da SEFAZ-RJ.

Confidencialidade: princípio da segurança que trata da garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: princípio da segurança que trata da salvaguarda da exatidão da informação e dos métodos de processamento.

Disponibilidade: princípio da segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário.

Análise de Risco de Vulnerabilidades: avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação.

Controle de Acesso: conjunto de recursos que efetivam as autorizações e as restrições de acesso aos ativos de informação.

Software Homologado: software desenvolvido, adquirido ou alterado pela SEFAZ-RJ.

Ciclo de Vida da Informação: tempo transcorrido entre a geração, manuseio, armazenamento, transporte e descarte de um ativo da informação.

Segregação de Funções: ato pelo qual o colaborador não pode exercer mais que uma função no processo.

Gestão dos Ativos de Informação

Os ativos da informação da SEFAZ-RJ e seu ambiente informatizado devem estar de acordo com esta PSI e suas normas internas relacionadas à segurança da informação.

Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela SEFAZ/RJ é considerada de sua propriedade e deve ser protegida, de acordo com as diretrizes de que trata este documento, a legislação em vigor e ainda com as normas e procedimentos relacionados.

Toda a informação deve ter um responsável pela sua criação, aquisição, manutenção, atualização e segurança.

A Política de Segurança da Informação, bem como o seu cumprimento, deve ser objeto de auditorias periódicas realizadas pela Auditoria Interna.

Os ativos de informação devem estar disponíveis para utilização apenas por necessidade de trabalho, garantindo-se a segregação de função e o princípio do menor privilégio.

Os ativos de informação desta SEFAZ-RJ devem ser protegidos contra ações indevidas intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, extração, alteração, uso e exposição indevidos, em conformidade com os princípios da confidencialidade, integridade e disponibilidade.

Os ativos de informação devem ser mantidos com o mesmo nível de proteção, independente do meio no qual estejam armazenados, em que trafeguem, ou ainda do ambiente em que estejam sendo processados.

Recursos de criptografia deverão, sempre que possíveis, ser disponibilizados para proteger o tráfego de dados e seu armazenamento.

Monitoração deverá ocorrer em tempo real com vistas a prover mecanismos de prevenção, detecção, identificação e combate a invasão (intrusão) de atividade maliciosa e/ou virótica.

Os ativos de informação devem ser inventariados periodicamente por servidores em exercício na área de tecnologia da informação, em especial no tocante aos aspectos atinentes a hardware, software e configurações.

Mecanismos de prevenção, detecção, e eliminação de vírus de computador e de outros programas maliciosos devem ser utilizados de forma preventiva e reativa.

Gestão de Ativos Físicos

Todos os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos.

Todos os usuários devem estar cientes de suas responsabilidades para a manutenção efetiva dos controles de acesso, considerando o uso e a confidencialidade de suas senhas e a segurança de seus equipamentos.

Ao utilizar equipamentos de computação móveis (notebooks, computadores de mão, telefones celulares, etc.), os usuários devem ter cuidados especiais a fim de garantir que as informações do negócio não sejam comprometidas.

Todos os recursos de tecnologia da informação da SEFAZ-RJ devem ser utilizados de acordo com os contratos, normas e legislação em vigor.

Todos os recursos de tecnologia da informação da SEFAZ-RJ devem ser inventariados e submetidos a um processo de homologação.

Classificação da Informação

Os ativos de informação da SEFAZ-RJ devem ser classificados em função de sua importância e confidencialidade.

Gestão dos Acessos

O acesso aos ativos de informação e recursos deverá ser autorizado previamente, sempre obedecendo ao critério do menor privilégio possível.

A senha de acesso de cada servidor utilizada como assinatura eletrônica deverá ser mantida secreta, vetado o seu compartilhamento.

A identificação de acesso (usuário de rede) deverá ser única, pessoal e intransferível, não devendo ser utilizado *login* genérico, salvo em casos a serem aprovados pela Superintendência de Infraestrutura.

As permissões de acesso devem ser concedidas de acordo com as atribuições dos usuários, sempre por necessidade de trabalho.

O acesso ao ativo da informação não gera direito real sobre o mesmo e nem sobre os frutos de sua utilização.

Todos os acessos devem ser rastreáveis para que o usuário seja identificado individualmente.

Gestão de Riscos

As medidas de segurança devem ser adotadas de forma proporcional aos riscos existentes e a magnitude dos potenciais danos, considerando o ambiente, o valor e a criticidade da informação.

Os cenários de riscos de segurança da informação deveram ser avaliados por fórum apropriado para decisão.

Conscientização em Segurança da Informação

Os servidores da SEFAZ-RJ devem ser treinados e capacitados a exercerem as atividades inerentes ao negócio com a visão de segurança da informação.

Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhados com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

Segurança Física do Ambiente

O processo de segurança física deve estabelecer controles de acesso somente às pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas, devendo ser igualmente respeitadas as normas de segurança de acesso definidas pela Administração Predial.

Segurança no Desenvolvimento de Sistemas de Aplicações

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas e às boas práticas de segurança da informação - SI.

O desenvolvimento de software em todas as fases do processo, a prospecção de produtos e serviços e os procedimentos de homologação deverão contar com a participação de servidores em exercícios na área de SI.

Plano de Continuidade de Negócio

Plano de contingência que assegure a operação e a recuperação de ativos de informação em situações de emergência, de acordo com as necessidades e prazos específicos, a serem definidos pela alta gestão da Secretaria.

Recuperação de Dados

Deverão ser providos recursos para a geração de cópias de segurança (backup) e de recuperação de informações (restore), devidamente documentadas, abrangendo periodicidade de cópias, forma e local de armazenamento, autorização de uso, prazo de retenção e plano de simulação e testes.

Auditoria (LOGs)

Deverão ser providos recursos para o registro de informações do tipo trilha de auditoria com prazos de retenção e formas de acesso definidas, com vistas a permitir auditoria, identificação de situações de violação e contabilização individual do uso dos sistemas.

Segurança do Ambiente Computacional

Os ambientes de produção, treinamento, testes, homologação e desenvolvimento dos sistemas informatizados, localizados nas unidades da SEFAZ-RJ ou de seus prestadores de serviços, devem ser distintos e de uso exclusivo da SEFAZ-RJ, respeitados acordos e convênios de cooperação tecnológica.

No ambiente informatizado da SEFAZ-RJ, devem ser utilizados e instalados somente softwares homologados e originais.

Os softwares instalados nos equipamentos servidores, nos equipamentos de rede e comunicação e nas estações de trabalho devem ser permanentemente atualizados, visando incrementar aspectos de segurança e correção de falhas.

A eliminação da informação protegida por sigilo fiscal, ou de uso exclusivo da SEFAZ-RJ e de softwares instalados, constantes em dispositivos de armazenamento, deve ser precedida da utilização de ferramentas adequadas à eliminação segura dos dados.

Devem ser adotadas medidas adicionais de proteção, visando garantir o mesmo nível de segurança das instalações internas da SEFAZ-RJ no caso de:

1 – uso de computação móvel, dispositivos móveis, mídias removíveis e quando o usuário utilizar o seu próprio equipamento (este último quando sua utilização for expressamente autorizada);

2 – uso de acesso remoto ou de rede instalada em ambiente informatizado diferente da SEFAZ-RJ e

3 - comunicação sem fio.

O tráfego de informações em redes locais e de longa distância deve ser protegido contra danos, perdas, indisponibilidades, uso ou exposição indevida, de acordo com seu valor, criticidade e confidencialidade.

As redes de dados devem possuir, sempre que possíveis rotas alternativas, além de contar com mecanismos de redundância.

É vedada a alteração dos mecanismos e configurações definidos pela área de segurança da informação da SEFAZ-RJ.

Das responsabilidades institucionais e funcionais

A responsabilidade quanto à segurança da informação é de todos os servidores e deve ser amplamente divulgada.

É de responsabilidade de todos os servidores cuidar da integridade, confidencialidade e disponibilidade dos ativos de informação da SEFAZ-RJ, devendo ser comunicadas quaisquer irregularidades, falhas ou desvios identificados à sua chefia imediata, assim como a área responsável pela segurança da informação.

É proibida a exploração de falhas ou vulnerabilidades que, por ventura, possam existir nos ativos de informação da SEFAZ-RJ.

A SEFAZ-RJ poderá autorizar testes controlados para identificar a existência de falhas ou vulnerabilidades em seus ativos de informação.

Cabe à SEFAZ-RJ

Gerenciar o processo de implantação e aplicação das diretrizes constantes nesta PSI;

Regulamentar o acesso aos ativos de informação desta SEFAZ-RJ;

Dirimir eventuais dúvidas relativas aos procedimentos regulamentados e

Expedir normas complementares.

Das disposições finais

Os funcionários e terceiros da SEFAZ-RJ devem declarar o seu conhecimento e comprometimento com a Política de Segurança da Informação, através da assinatura de um TERMO DE SIGILO, CONFIDENCIALIDADE E NÃO DIVULGAÇÃO.

O descumprimento das disposições constantes nesta PSI e demais diretrizes de segurança da informação caracteriza infração funcional.

A revisão deste documento, assim como de toda a Política de Segurança, deve ser executada pela Área de Segurança da Informação, anualmente, ou quando necessário.