DECRETO N. 1792/2017, DE 19 DE JUNHO DE 2017.

"DISPÕE SOBRE A IMPLANTAÇÃO E REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI – NO ÂMBITO DA PREFEITURA MUNICIPAL DE TARUMÃ, E DÁ OUTRAS PROVIDÊNCIAS".

OSCAR GOZZI, PREFEITO MUNICIPAL DE TARUMÃ, ESTADO DE SÃO PAULO, NO USO DE SUAS ATRIBUIÇÕES LEGAIS,

CONSIDERANDO os projetos desenvolvidos pela equipe de Tecnologia da Informação por meio dos servidores habilitados para esta finalidade que apontaram os riscos possíveis para as informações geridas pelo Município de Tarumã em todas as suas unidades;
CONSIDERANDO que a gestão de informações tanto eletrônicas quanto físicas são relevantes também para os munícipes e todos aqueles que de qualquer forma relacionam-se com o Município de Tarumã;
CONSIDERANDO finalmente o deveres dos servidores públicos municipais previstos no Estatuto dos Servidores Públicos do Município de Tarumã, da Lei municipal nº. 101/94.

D E C R E T A:

Art. 1º. – Fica instituída no âmbito do Município de Tarumã a Política de Segurança da Informação – PSI em conformidade com o Anexo I deste Decreto.

Art. 2º – A Política de Segurança da Informação – PSI é de obrigatório cumprimento por todos os servidores, efetivos ou não, que mantenham relação com o Município de Tarumã, assim como prestadores de serviços e quaisquer envolvidos, mesmo que transitoriamente, com informações sensíveis que são protegidas pela Política de Segurança da Informação – PSI.

Art. 3º – As infrações à Política de Segurança da Informação – PSI sujeitará o responsável às punições previstas na legislação vigente, especialmente aquelas constantes do Estatuto dos Servidores Públicos Municipais, Lei Municipal nº 101/94 e suas posteriores alterações.

Art. 4º – As despesas decorrentes da execução do presente Decreto, correrão por conta de verbas próprias já consignadas no orçamento vigente, suplementadas se necessário.

Art. 5º – Este Decreto entrará em vigor na data de sua Publicação.

Art. 6º – Revogam-se as disposições em contrário.

Paço Municipal "Waldemar Schwarz", 19 de junho de 2017, 27º. Ano da Emancipação Política e 25º. Ano da Instalação.

Oscar Gozzi
PREFEITO MUNICIPAL

Fernandes Baratela
SECRETÁRIO MUNICIPAL DE GOVERNO

Publicado na Secretaria Municipal de Governo, em 19 de junho de 2017.

Fernandes Baratela
SECRETÁRIO MUNICIPAL DE GOVERNO

ANEXO I

Política de Segurança da Informação - PSI

1. Definição da segurança da informação

Diariamente, todas as secretarias e UGBs da Prefeitura Municipal de Tarumã, coletam, processam, armazenam e transmitem informações, não somente pelo meio físico e verbal, mas, também pelo meio digital. Todas essas informações são como Ativos para a organização, e como qualquer outro ativo importante, elas são essenciais para o funcionamento dos serviços públicos, portanto, elas tem valor para a organização e, consequentemente, precisam ser protegidas contra diversos tipos de riscos.

Ativos são objeto de ameaças, sejam elas acidentais ou de forma deliberada, além do mais, os processos, sistemas, redes e pessoas possuem vulnerabilidades inerentes. Ambientes de mudanças, internas ou externas à organização (novas leis ou regulamentações, por exemplo), podem criar novas ameaças a estes ativos de tal modo que, inevitavelmente, sempre haverão riscos à segurança da informação. Desta forma, uma boa segurança da informação reduz estes riscos, protege a instituição pública contra essas ameaças e vulnerabilidades e mitiga qualquer impacto aos ativos de maneira eficaz.

2. Objetivo

Estabelecer os conceitos e diretrizes de segurança da informação, visando proteger as informações da instituição pública e dos cidadãos quanto à:

- Confidencialidade: garantia de que a informação seja acessada somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados possam acessar a informação e aos ativos correspondentes sempre que necessário;
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

3. Abrangência

Esta Política aplica-se a todos os funcionários, estagiários, prestadores de serviços, consultores, auditores, fornecedores, parceiros diversos, temporários, prefeito, vice-prefeito e secretários.

4. Atribuição de responsabilidades para o gerenciamento da segurança da informação

4.1. Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada por concurso ou seleção ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Cabe a todos os colaboradores cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Prefeitura Municipal de Tarumã; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas incluindo a emissão de comentários e opiniões em blogs e redes sociais; não compartilhar informações confidenciais de qualquer tipo; e comunicar imediatamente a **Área de Tecnologia da Informação** quando do descumprimento ou violação desta política.

4.2. Dos Gestores

Entende-se por gestores o Prefeito Municipal, o Vice-Prefeito Municipal e todos os Secretários Municipais.

Todos os gestores devem ser um modelo de conduta e manter postura exemplar em relação à segurança da informação para os colaboradores sob a sua gestão; Atribuir aos colaboradores a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Tarumã; Assegurar que todos os colaboradores possuam acesso e conhecimento desta PSI; Identificar os desvios praticados e adotar as medidas corretivas apropriadas; Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI; Avaliar e aprovar os termos e controles desta Política, bem como os ajustes, melhorias, aprimoramentos e modificações desta Política, propostos pelos Custodiantes da Informação.

4.3. Dos Custodiantes da Informação

Entende-se por Custodiantes da Informação toda e qualquer pessoa física, contratada por concurso ou seleção ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade na área de Tecnologia da Informação.

4.3.1. Da Área de Tecnologia da Informação

Cabe à área de Tecnologia da Informação:

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador;
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

Propor ajustes, melhorias, aprimoramentos e modificações desta Política.

Publicar e promover a PSI aprovada pelos gestores.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para as atividades da Prefeitura Municipal de Tarumã, mediante campanhas, palestras, treinamentos e outros meios de marketing.

Manter comunicação efetiva com os Gestores sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Prefeitura Municipal de Tarumã.

Buscar alinhamento com as diretrizes de governo da instituição.

5. Conformidade

Aos colaboradores não é dado o direito de alegar desconhecimento da Política de Segurança da Informação, devendo seguir rigorosamente o disposto nos Controles de Segurança.

Esta política é comunicada para todo o pessoal envolvido e largamente divulgada, garantindo que todos a conheçam e a pratiquem.

A inobservância das políticas e normas de segurança sujeita o usuário a sanções internas e, nos casos cabíveis, às leis vigentes.

Verificações de cumprimento da política devem ser efetuadas, para verificar o nível de segurança das áreas e elaborar projetos para melhoria dos índices de conformidade.

6. Controles de Segurança

6.1. Segurança da informação no gerenciamento de projetos

A segurança da informação deve ser integrada nos métodos de gerenciamento de projeto da organização para assegurar que os riscos de segurança da informação estão identificados e considerados como parte de um projeto. Isto se aplica de um modo geral, para qualquer projeto independentemente do seu propósito, por exemplo, se é um projeto

para um processo crítico do negócio, um processo de TI, de gerenciamento de recursos ou outro processo de apoio.

Os métodos de gerenciamento de projetos usados devem requerer que:

a) Os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;
b) Uma avaliação dos riscos de segurança da informação seja conduzida em estágios iniciais do projeto para identificar os controles que são necessários;
c) a segurança da informação seja parte integrante de todas as fases da metodologia do projeto.

As questões de segurança da informação devem ser consideradas e analisadas criticamente a intervalos planejados, em todos os projetos. Convém que as responsabilidades pela segurança da informação sejam definidas e alocadas para papéis específicos definidos dos métodos de gerenciamento de projeto.

6.2. Inventário dos ativos

A organização deve identificar os ativos relevantes no ciclo de vida da informação e documentar a sua importância. Convém que o ciclo de vida da informação inclua a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição. A documentação deve ser mantida em um inventário existente ou exclusivo, conforme apropriado.

O inventário de ativos deve ser completo, atualizado e consistente.

Convém que para cada um dos ativos identificados, seja indicado um responsável.

6.3. Tratamento de mídias

6.3.1. Gerenciamento de mídias removíveis

O gerenciamento de mídias removíveis deve seguir as seguintes diretrizes:

a) O conteúdo de qualquer meio magnético reutilizável deve ser destruído antes do seu descarte.
b) Toda mídia deve ser guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante.
c) Para mitigar o risco de degradar a mídia enquanto os dados armazenados ainda são necessários, os dados devem ser transferidos para uma mídia nova antes de se tornar ilegíveis;

d) Cópias múltiplas de dados valiosos devem ser armazenadas em mídias separadas para reduzir riscos futuros de perda ou dano, que ocorram por coincidência nessas mídias;

e) As unidades de mídia removíveis devem ser habilitadas somente se houver uma necessidade do negócio.

6.3.2. Descarte de mídias

Mídias contendo informações confidenciais devem ser guardadas e destruídas de forma segura e protegida, como por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização.

6.4. Acesso às redes administrativas e aos serviços de rede

Os Colaboradores em Geral podem acessar e utilizar apenas os seguintes serviços de rede:

- Sistemas de gestão próprios ou de terceiros, softwares para processamento de textos, planilhas, apresentações, imagens, áudios, vídeos, projetos em 3D e quaisquer outros softwares previamente instalados nos computadores;
- Unidade temporária de transferência arquivos (intercâmbio), unidades de armazenamento permanente de arquivos (exemplo: G) e unidade de armazenamento de imagens (exemplo: M);
- Internet, webmail e sistemas on-line cujo a URL foi previamente liberada;
- Vídeo monitoramento.

Serviços como: sistemas de gestão, unidades de armazenamento temporária, permanente e de imagens, webmail, sistemas on-line e vídeo monitoramento requerem usuário e senha para serem acessados. Tais usuários e senhas serão criados e fornecidos aos colaboradores em geral apenas após a ciência e consentimento dos respectivos responsáveis pelos serviços.

Todos os serviços de rede, inclusive aqueles que requerem o uso de internet, devem ser acessados apenas por meio da rede cabeada disponibilizada para todos os computadores da organização. Uso de VPN deve ser autorizado pelos gestores e somente VPN's confiáveis ou geridas pela própria instituição são permitidas. O uso de redes sem fio para acessar os serviços de rede acima citados é vedado em toda a organização.

É vedada a qualquer usuário externo à instituição o acesso à rede administrativa ou qualquer serviço por ela acessível. Se necessário for, usuários externos devem utilizar

usuários e senhas temporários e todos os seus atos devem ser autorizados e monitorados pelo responsável do serviço.

6.5. Registro e cancelamento de usuário

O identificador de usuário (ID de usuário ou usuário e senha) deve ser único, de uso pessoal e intransferível para permitir relacionar os usuários com suas responsabilidades e ações.

O identificador de usuário deve ser removido ou desabilitado após sua saída da instituição.

É vedada a criação identificadores de usuários redundantes.

6.6. Provisionamento para acesso de usuário

Antes de atribuir ou revogar os direitos de acesso concedidos ao ID de usuário é necessário:

a) Obter autorização do proprietário do sistema ou do ativo de informação para o uso destes; Aprovações separadas para os direitos de acesso da direção também pode ser recomendada;
b) Manter um registro central de direitos de acesso concedido ao ID de usuário para acessar serviços e sistemas de informação;
c) Adaptar dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram a organização;
d) Analisar mensalmente e de maneira critica os direitos de acesso com os proprietários dos serviços ou sistemas de informação (ver 6.8).

6.7. Gerenciamento de direitos de acesso privilegiados

A alocação de direitos de acesso privilegiado deve seguir os seguintes passos:

a) Os direitos de acesso privilegiado devem ser concedidos a usuários conforme a necessidade de uso, baseado nos requisitos mínimos para sua função;
b) Um processo de autorização e um registro de todos os privilégios concedidos devem ser mantidos. Direitos de acesso privilegiados não sejam concedidos até que todo o processo de autorização esteja finalizado;
c) Requisitos para expirar os direitos de acesso privilegiado devem ser definidos;

d) As competências dos usuários com direitos de acesso privilegiado devem ser analisadas criticamente sempre que houver mudanças no quadro de pessoal, para verificar se eles estão alinhados com as suas obrigações;

e) Procedimentos específicos sejam estabelecidos e mantidos para evitar o uso não autorizado de ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas;

f) Para o ID de usuário de administrador genérico, a confidencialidade da informação de autenticação secreta deve ser mantida quando for compartilhada (por exemplo, mudanças de senhas com frequência e tão logo quanto possível, quando um usuário privilegiado deixa a organização ou muda de função, comunicação entre os usuários privilegiados por meio de mecanismos apropriados).

6.8. Gerenciamento da informação de autenticação secreta de usuários

Os colaboradores em geral devem manter a confidencialidade da suas senhas e manter as senhas de grupos de trabalho exclusivamente com os membros do grupo.

É necessário verificar a identidade de um usuário antes de fornecer uma senha, temporária, de substituição ou nova.

É vetado o uso de mensagens de correio eletrônico de terceiros ou desprotegido (texto claro) para o envio de senhas. Elas tem que ser fornecidas por meio seguro.

Senhas temporárias devem ser únicas para cada pessoa e não devem ser fáceis de serem descobertas.

As senhas padrão devem ser alteradas logo após a instalação de sistemas ou software.

6.9. Análise crítica dos direitos de acesso de usuário

Os responsáveis pelos programas ou serviços da rede administrativa devem seguir as seguintes orientações:

a) Os direitos de acesso de usuários devem ser revisados em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou encerramento do contrato;

b) Autorizações para direitos de acesso privilegiado especial devem ser revisadas mensalmente;

c) As alocações de privilégios devem ser verificadas mensalmente para garantir que privilégios não autorizados não foram obtidos.

6.10. Uso da informação de autenticação secreta

Todos os colaboradores em geral devem:

a) Manter a confidencialidade das senhas, garantindo que elas não sejam divulgadas para quaisquer outras partes, incluindo autoridades e lideranças;
b) Evitar manter anotadas as senhas (por exemplo: papel, arquivos ou dispositivos móveis), a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado;
c) Alterar a senha, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
d) Selecionar senhas de qualidade com um tamanho mínimo que sejam:
    1) fortes, porém, fáceis de lembrar;
    2) não baseadas em nada que alguém facilmente possa descobrir ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;
    3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário);
    4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
e) Caso a senha seja temporária, ela deve ser mudada no primeiro acesso (log-on);
f) Não compartilhar a senha de usuários individuais com outros colaboradores;
g) Não utilizar a mesma senha para uso com finalidades profissionais e pessoais.

6.11. Uso de programas utilitários privilegiados

O uso de programas utilitários que são capazes de sobrepor os controles dos sistemas e aplicações devem seguir as seguintes diretrizes:

a) Uso de procedimentos de identificação, autenticação e autorização para programas utilitários de sistema;
b) Segregação de programas utilitários dos softwares de aplicação;
c) Limitação do uso de programas utilitários a um número mínimo de usuários confiáveis e autorizados (ver 6.6);
d) Limitação da disponibilidade dos programas utilitários, por exemplo para a duração de uma modificação autorizada;
e) Remoção ou desabilitação de todos os programas utilitários desnecessários.

6.12. Controle de acesso ao código-fonte de programas

O acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) devem ser estritamente controlados, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais, bem como para manter a confidencialidade de propriedade intelectual valiosa.

6.13. Perímetro de segurança física

Áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis devem permanecer com a porta trancada e somente pessoal autorizado deve ter acesso às chaves. O acesso às estas áreas deve ser monitorado por câmeras de segurança e alarmes ou vigias e guardas.

6.14. Controles de entrada física

Áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido:

a) Todos os visitantes devem ser supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; as permissões de acesso só devem ser concedidas para finalidades específicas e autorizadas;
b) O acesso às áreas em que são processadas ou armazenadas informações sensíveis deve ser restrito apenas ao pessoal autorizado;
c) Deve ser exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação, e que eles avisem imediatamente ao pessoal de segurança, caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;
d) Às partes externas que realizam serviços de suporte, deve ser concedido acesso restrito às áreas seguras ou as instalações de processamento da informação sensíveis, somente quando necessário; este acesso deve ser monitorado.

6.15. Manutenção dos equipamentos

Para assegurar a disponibilidade e integridade permanente dos equipamentos, os mesmos devem ter uma manutenção correta, conforme diretrizes a seguir:

- A manutenção dos equipamentos deve ser realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

- A manutenção e os consertos dos equipamentos devem ser realizados por pessoal de manutenção autorizado;
- Devem ser mantidos registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;
- Informações sensíveis devem ser eliminadas do equipamento caso a manutenção seja realizada por pessoal externo à Prefeitura;
- Antes de colocar o equipamento em operação, após a sua manutenção, ele deve ser inspecionado para garantir que não foi alterado indevidamente e que não está em mau funcionamento.

6.16. Separação dos ambientes de desenvolvimento, teste e de produção

Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

O software em desenvolvimento e o software em produção devem ser, sempre que possível, executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios.

As mudanças nas aplicações e nos sistemas operacionais devem ser testadas em um ambiente de teste ou projeto piloto, antes de ser aplicado aos sistemas operacionais.

6.17. Controles contra códigos maliciosos

A prevenção contra códigos maliciosos deve seguir as seguintes diretrizes:

a) É vetado o uso de softwares não autorizados pela área de tecnologia da informação. Somente os softwares disponíveis nos repositórios ou utilitários e os adquiridos pela organização podem ser instalados, além daqueles provenientes de fontes confiáveis, como por exemplo, softwares da Receita Federal ou Ministério da Saúde ou, ainda, softwares bancários;

b) Prevenir ou detectar o uso de websites maliciosos, suspeitos ou conhecidos (por exemplo: blacklisting);

c) Arquivos e softwares armazenados em dispositivos removíveis devem ser colocados na rede apenas pela área de tecnologia da informação, após procedimento de inspeção de segurança para prevenir a entrada de códigos maliciosos na rede;

d) Instalar e atualizar regularmente softwares de detecção e remoção de códigos maliciosos (antivírus e outros) para o exame de computadores e mídias

magnéticas, de forma preventiva ou de forma rotineira; As verificações realizadas devem incluir:

1) varredura, antes do uso, da existência de códigos maliciosos nos arquivos recebidos por meio de redes ou em qualquer mídia de armazenamento;
2) verificação, antes do uso, da existência de software malicioso em qualquer arquivo recebido através de correio eletrônico ou importado (download). Essa avaliação pode ser feita em diversos locais, como, por exemplo, nos servidores de correio eletrônico, nos computadores pessoais ou quando da sua entrada na rede da organização;
3) verificação da existência de códigos maliciosos em páginas web;

e) Colaboradores em geral devem comunicar a área de tecnologia da informação sempre que suspeitar ou notar algo estranho, por exemplo: um e-mail de uma fonte desconhecida com um link encurtado para fazer o download de uma nota fiscal;
f) Isolar os ambientes onde impactos catastróficos possam ser gerados.

6.18. Cópias de segurança

Os gestores e os custodiantes da informação devem prover:

a) Os recursos adequados para a geração de cópias de segurança para garantir que toda informação e software essenciais possam ser recuperados após um desastre ou a falha de uma mídia.

Os custodiantes da informação devem seguir as seguintes diretrizes:

a) Manter registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação;
b) As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
c) Deve ser dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver 6.14), consistentes com as normas aplicadas na instalação principal;
d) As mídias de backup devem ser mensalmente testadas para garantir que elas são confiáveis no caso do uso emergencial; Isto deve ser combinado com um teste de restauração e checado contra o tempo de restauração requerido. Os testes da capacidade para restaurar os dados copiados devem ser realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o

processo de restauração ou backup falhe e cause irreparável dano ou perda dos dados.

6.19. Registros de eventos

Registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, em intervalos regulares. Convém que os registros (log) de eventos incluam, quando relevante:

a) Identificação dos usuários (ID);
b) Atividades do sistema;
c) Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;
d) Identidade do dispositivo ou sua localização quando possível e o identificador do sistema;
e) Alterações na configuração do sistema;
f) Arquivos acessados e o tipo de acesso;
g) Endereços e protocolos de rede;
h) Alarmes provocados pelo sistema de controle de acesso;
i) Ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos;
j) Registros de transações executadas pelos usuários nas aplicações.

6.20. Proteção das informações dos registros de eventos (logs)

As informações dos registros de eventos (log) e seus recursos devem ser protegidas contra acesso não autorizado e adulteração. Com este objetivo, as seguintes diretrizes devem ser seguidas para proteger os registros de eventos:

a) Impedir alterações dos tipos de mensagens que são gravadas;
b) Impedir que arquivos de registros (log) sejam editados ou excluídos;
c) Garantir que a capacidade de armazenamento da mídia magnética do arquivo de registros (log) nunca seja excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

6.21. Sincronização dos relógios

Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização, devem ser sincronizados com uma única fonte de tempo precisa.

6.22. Controle de software operacional

Procedimentos para controlar a instalação de software em sistemas operacionais:

a) Atualizações do software operacional, aplicativos e bibliotecas de programas devem ser executadas por administradores treinados e com autorização gerencial apropriada;
b) Os sistemas operacionais somente devem conter código executável e aprovado, e não devem conter códigos em desenvolvimento ou compiladores;
c) Sistemas operacionais e aplicativos somente devem ser implementados após testes extensivos e bem sucedidos; é recomendável que os testes incluam testes sobre uso, segurança, efeitos sobre outros sistemas como também sobre uso amigável, e sejam realizados em sistemas separados (ver 6.16); Convém que seja assegurado que todas as bibliotecas de código fonte dos programas correspondentes tenham sido atualizadas;
d) Uma estratégia de retorno às condições anteriores deve ser disponibilizada antes que mudanças sejam implementadas no sistema;
e) Um registro de auditoria deve ser mantido para todas as atualizações das bibliotecas dos programas operacionais;
f) Versões anteriores dos softwares aplicativos devem ser mantidas como medida de contingência;
g) Versões antigas de software devem ser arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações, e software de suporte durante um prazo igual ao prazo de retenção dos dados.

6.23. Restrições quanto à instalação de software

Os perfis de usuários dos colaboradores devem ser configurados com privilégios mínimos para evitar a instalação de softwares no sistema operacional.

São proibidas as instalações de softwares que são usados somente para fins pessoais e softwares cuja possibilidade de serem potencialmente maliciosos é desconhecida ou suspeita.

6.24. Controles de redes

A gestão dos equipamentos de rede é de responsabilidade da equipe de rede que integra a área de tecnologia da informação.

A gestão dos recursos de rede é de responsabilidade da equipe de sistemas e servidores que integra a área de tecnologia da informação.

A equipe de rede deve garantir a disponibilidade dos serviços e computadores conectados à rede, além disso, deve proteger a confidencialidade e integridade dos dados que trafegam sobre essas redes e dos sistemas e aplicações a ela conectados.

Softwares com elevado grau de importância e que requerem cópias de segurança devem ser ser instalados nos servidores e o acesso deve ser disponibilizado aos colaboradores em geral por meio de VPN ou acesso remoto.

Mecanismos apropriados de registro e monitoração podem ser aplicados para habilitar a gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação.

Todo sistema que trabalha sobre a rede deve possuir uma área para autenticação.

6.25. Política de desenvolvimento seguro

Desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema seguro. Dentro de uma política de desenvolvimento seguro, os seguintes aspectos devem ser considerados:

a) Segurança do ambiente de desenvolvimento;
b) Requisitos de segurança na fase do projeto;
c) Pontos de verificação de segurança no cronograma do projeto;
d) Repositórios seguros;
e) Segurança no controle de versões;
f) Necessários conhecimentos de segurança de aplicações;
g) Capacidade dos desenvolvedores de evitar, encontrar e corrigir vulnerabilidades.

As técnicas de programação seguras devem ser usadas tanto para novos desenvolvimentos como para cenários de reuso de código, onde as normas aplicadas ao desenvolvimento podem não ser conhecidas ou não estarem consistentes com as melhores práticas atuais.

6.26. Procedimentos para controle de mudanças de sistemas

A introdução de novos sistemas e mudanças maiores em sistemas existentes deve seguir um processo formal de documentação, especificação, teste, controle da qualidade e gestão da implementação.

Os procedimentos de controle de mudanças devem incluir, porém não se limitar a:

a) A garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada ou descartada;
b) A manutenção de um controle de versão para todas as atualizações de software;

c) A manutenção de uma trilha de auditoria de todas as mudanças solicitadas;
d) A garantia de que toda a documentação operacional, e procedimentos dos usuários sejam alterados conforme necessário para se manter adequado;
e) A garantia de que as mudanças sejam implementadas em horários apropriados e não perturbe os processos de negócio envolvidos.

6.27. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

Quando plataformas operacionais forem modificadas, as aplicações críticas de negócio devem ser analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.

Este processo deve compreender:

a) A análise crítica dos controles da aplicação e dos procedimentos de integridade para assegurar que eles não foram comprometidos pelas mudanças na plataforma operacional;
b) A garantia de que as mudanças previstas na plataforma operacional sejam comunicadas em tempo hábil para permitir os testes e análises críticas antes da implementação.

Informações adicionais

Plataformas operacionais incluem sistemas operacionais, banco de dados e plataformas intermediárias. Convém que os controles também sejam aplicados para mudanças em aplicações.

6.28. Princípios para projetar sistemas seguros

Projetos de software para processar informações importantes devem incluir os seguintes mecanismos:

a) Autenticação segura. Caso a senha seja transmitida por uma rede, ela deve ser criptografada;
b) Controle de sessão;
c) Privilégios de acesso a recursos do sistema;
d) Registro de rastros (logs).

Aplicações web devem usar protocolos de comunicação seguros, como HTTPS. Mensagens de e-mail enviadas por estas aplicações devem ser assinadas antes do envio (TLS).

As APIs e bibliotecas do softwares devem ser atualizada frequentemente com o intuito de incorporar novas correções de falhas de segurança.

Trechos de código, bibliotecas, APIs, frameworks, entre outros, devem ser utilizados apenas quando a fonte destes for reconhecidamente segura e confiável.

Novas tecnologias devem ser analisadas e testadas com antecedência quanto aos riscos de segurança.

6.29. Teste de segurança do sistema

Os testes de funcionalidades de segurança devem ser realizados durante o desenvolvimento de softwares tanto para softwares novos quanto para os que são atualizados.

Os testes devem incluir a verificação das entradas e saídas esperadas do softwares, por exemplo, o software não deve permitir a entrada de comandos de linguagens de programação em campos de texto não apropriados para essa finalidade (SQL injection ou Javascript injection).

Após erros ou falhas do softwares, não devem ser exibidos senhas, nome de arquivo ou conteúdo parcial ou total de arquivos de configuração, caminhos e diretórios do servidor, endereços de IP interno da rede, entre outros. Quando essas falhas precisam ser capturadas, é necessário que isso seja feito em ambiente de testes ou por meio de registros de log apropriados.

6.30. Teste de aceitação de sistemas

Testes de aceitação para novos sistemas de informação, atualizações e novas versões devem estar aderentes às práticas de desenvolvimento seguro de sistemas (ver 6.25). Testes também devem ser realizados nos componentes recebidos e nos sistemas integrados.

Convém que os testes sejam realizados em um ambiente de teste realístico para assegurar que o sistema não introduzirá vulnerabilidades ao ambiente da prefeitura e que os testes são confiáveis.

6.31. Proteção dos dados para teste

Dados de teste devem ser selecionados com cuidado, protegidos e controlados. Deve ser evitado, para propósitos de teste, o uso de bancos de dados operacionais. Caso informações de identificação pessoal ou outras informações sensíveis sejam utilizadas com

o propósito de teste, todos os detalhes e conteúdos devem ser protegidos contra remoção ou modificação.

As seguintes orientações devem ser aplicadas para a proteção de dados operacionais, quando utilizados para fins de teste:

a) Os procedimentos de controle de acesso, aplicáveis aos sistemas de aplicações operacionais, devem ser também aplicados aos sistemas de aplicações em teste;
b) Deve ser obtida autorização cada vez que for utilizada uma cópia da informação operacional para uso em ambiente de teste;
c) A informação operacional deve ser apagada do ambiente de teste, imediatamente após finalizar os testes.

6.32. Proteção de registros

Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

Cuidados devem ser tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros. Os procedimentos de armazenamento e manuseio devem ser implementados de acordo com as recomendações dos fabricantes.

No que diz respeito a mídias eletrônicas, é necessário assegurar a capacidade de acesso aos dados (leitura tanto na mídia como no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia.

Sistemas de armazenamento de dados devem ser escolhidos de modo que o dado solicitado possa ser recuperado de forma aceitável, dependendo dos requisitos a serem atendidos.

O sistema de armazenamento e manuseio deve assegurar a clara identificação dos registros e dos seus períodos de retenção, conforme definido pela legislação nacional ou regional ou por regulamentações, se aplicável. Convém que este sistema permita a destruição apropriada dos registros após esse período, caso não sejam mais necessários à organização.

7. Tratamento dos desvios e exceções

As condutas violadoras das diretrizes desta PSI serão verificadas em conformidade com a legislação vigente, especialmente o Estatuto dos Servidores Públicos do Município de Tarumã (Lei Municipal nº 104/94 e suas posteriores alterações), sujeitando os infratores às

penalidades estatutárias previstas por violações dos deveres funcionais, mediante sindicância ou processo administrativo.

Aos colaboradores não regidos pelo Estatuto serão aplicadas as penalidades contratuais e também aquelas previstas na legislação vigente, inclusive com a possibilidade de declaração de inidoneidade e impedimento de contratar com o Poder Público.

8. Vigência e validade

A presente política passa a vigorar a partir da data de sua aprovação e publicação, sendo válida por tempo indeterminado.

9. Documentos de referência

ABNT NBR ISO/IEC 27002:2013