SECRETARIA DE FINANÇAS

Prefeitura Municipal de Osasco
Secretaria de Finanças

PORTARIA N° 002/2021.

Disciplina Política de Segurança da Informação no âmbito da Administração
Pública Direta.

BRUNO MANCINI, Secretário de Finanças do Município de Osasco, uso de uma de suas atribuições legais e,

Considerando a necessidade de aprimorar Política de Segurança da Informação - PSI no âmbito da Administração Pública Direta;

Considerando a Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pela Administração Municipal, aplicando-se a todos os órgãos e entidades do Poder Executivo Municipal.

Considerando necessidade de uniformizar e dinamizar os procedimentos administrativos que tramitam junto a Subsecretaria de Tecnologia da Informação – STI.

RESOLVE

Art. 1º Fica instituída um conjunto de normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodias pela Administração Municipal, conforme disposto no § 1º art. 1° do Decreto n° 11.078, de 05 de março de 2015, na forma de Anexo a esta Portaria.

Parágrafo único. As Normas serão publicadas no website e Imprensa Oficial do Município de Osasco.

Art. 2º Caberá aos órgãos da Administração Direta do Munícipio de Osasco, no

âmbito de suas competências, as gestões que possibilitem à implementação das ações

estratégicas das normas.

Art. 3° - Esta portaria entra em vigor na data de sua publicação.

Osasco, 05 de março de 2021.

Bruno Mancini
Secretário de Finanças

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

ANEXO

Normas de Segurança da Informação

Política da Segurança da Informação

Norma	01	Data 25/02/21	Email	sti.sf@osasco.sp.gov.br
Version	1.0			

PROPÓSITO

Convém que a política de segurança da informação seja definida pela Subsecretaria de Tecnologia da Informação, publicada e comunicada para todos os funcionários da Prefeitura do Município de Osasco e terceiros, através website e na Imprensa Oficial do Município de Osasco – IOMO.

ESCOPO E APLICAÇÃO

Aplicação – Para conhecimento dos funcionários e terceiros sobre as seguintes Diretrizes da Política de Segurança da Informação da Prefeitura do Município de Osasco.

Norma 01 – Política da Segurança da Informação.

Propósito: Convém que um documento da política de segurança da informação seja aprovado pela Subsecretaria de Tecnologia da Informação e Direção, publicado e comunicado para todos os funcionários e partes externas relevantes, através website e na Imprensa Oficial do Município de Osasco – IOMO.

Norma 02 – Revisão da Política de Segurança da Informação.

Propósito: Revisar periodicamente a política de segurança da informação, a intervalos de tempo planejado ou se mudanças significativas ocorrerem para assegurar a sua adequabilidade e eficácia.

Norma 03 – Comprometimento da Subsecretaria de Tecnologia da Informação Com a Segurança da Informação.

Propósito: Demonstrar o comprometimento da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco com a segurança da informação.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Norma 04 – Coordenação da Segurança da Informação.

Propósito: Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.

Norma 05 – Atribuição de Responsabilidades Pela Segurança da Informação.

Propósito: Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas.

Norma 06 – Processo de Autorização Para os Recursos de Processamento da Informação.

Propósito: Convém que seja definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.

Norma 07 – Acordos de Confidencialidade e Propriedade Intelectual.

Propósito: Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular.

Norma 08 – Contatos Com Autoridades.

Propósito: Convém que contatos com autoridades relevantes sejam mantidos.

Norma 09 – Contatos Com Grupos Especiais.

Propósito: Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais.

Norma 10 – Revisão Independente da Segurança da Informação.

Propósito: Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

Norma 11 – Segurança da Informação com Terceiros.

Propósito: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.

Norma 12 – Gerenciamento de Ativos.

Propósito: Alcançar e manter a proteção adequada dos ativos da organização.

Norma 13 – Classificação da Informação.

Propósito: O sistema de classificação da informação da Prefeitura do Município de Osasco, como definido por este documento, é baseado no conceito necessidade de conhecimento. Este termo significa que a informação não pode ser disponibilizada para ninguém que não tenha uma necessidade legítima e demonstrável, face às atividades da Prefeitura do Município de Osasco, para ter acesso à informação. Este conceito, quando combinado com as políticas definidas neste documento, protegerá a Prefeitura do Município de Osasco contra o uso não autorizado da informação, sua modificação e deleção.

Norma 14 – Gerenciamento de Segurança em Recursos Humanos.

Propósito: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mal-uso de recursos.

Norma 15 – Segurança Física e do Ambiente.

Propósito: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

Norma 16 – Comunicações e Gestão de Operações.

Propósito: Garantir a operação segura e correta dos recursos de processamento das informações.

Norma 17 – Controle de Acessos.

Propósito: Controlar acesso à informação.

Norma 18 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

Propósito: Garantir que a segurança é parte integrante de sistemas de informação.

Norma 19 – Gestão de Incidentes de Segurança da Informação.

Propósito: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Norma 20 – Gestão da Continuidade do Negócio.

Propósito: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

Norma 21 – Conformidade.

Propósito: Evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação a definição e divulgação da Política para funcionários e terceiros, utilizando como recurso, inclusive, a publicação na Imprensa Oficial do Município de Osasco e no website da Subsecretaria de Tecnologia da Informação.

DECLARAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- A Subsecretaria de Tecnologia da Informação deve regulamentar os mecanismos de segurança da informação mais apropriados considerando riscos, tecnologia e custo no âmbito da Administração Direta do Município de Osasco;
- A Subsecretaria de Tecnologia da Informação deverá garantir a continuidade do processamento da informação considerada crítica;
- Todos os funcionários e demais terceiros que prestam serviços na Prefeitura do Município de Osasco devem proteger as informações sensíveis e confidenciais contra acesso, modificação, destruição ou divulgação não autorizada;
- Todo funcionário e demais terceiros devem assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Prefeitura do Município de Osasco;
- Todo funcionário e demais terceiros devem garantir que os sistemas, recursos e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Todos os funcionários e demais terceiros devem cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Todos os funcionários e demais terceiros devem atender a legislação que regulamenta as atividades da Prefeitura do Município de Osasco;
- Cabe a todos os funcionários e demais terceiros comunicar imediatamente à Subsecretaria de Tecnologia da Informação qualquer descumprimento da Política.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Politica de Segurança da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Politica de Segurança da Informação	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Revisão da Política de Segurança da Informação

Norma	02	Data:25/02/21	Email	sti.sf@osasco.sp.gov.br
Version	1.0			

PROPÓSITO

Revisar periodicamente a política de segurança da informação, a intervalos de tempo planejado ou se mudanças significativas ocorrerem para assegurar a sua adequabilidade e eficácia.

ESCOPO E APLICAÇÃO

Aplicação – Esta Norma se aplica à Subsecretaria de Tecnologia da Informação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação a revisão periódica das Políticas de Segurança da Informação.

REVISÃO DA POLÍTICA

Todos os documentos da política de segurança da informação devem ser revistos pelo menos anualmente pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco, que poderá convidar as demais partes interessadas.

Caberá à Subsecretaria de Tecnologia da Informação determinar um plano de revisão da política.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

PROPRIETÁRIOS DOS DOCUMENTOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Todos os documentos do Sistema de Gerenciamento da Segurança da Informação da Prefeitura do Município de Osasco tais como: políticas, padrões e documentos, têm que ter um proprietário do documento.

A Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco deverá designar funções responsáveis pela criação e manutenção das políticas de segurança da informação e documentos relacionados.

CONTROLE DE VERSÃO DAS POLÍTICAS

Todos os documentos do Sistema de Gerenciamento da Segurança da Informação, políticas, padrões e procedimentos devem ser mantidos em um sistema de gerenciamento de versão, preservando o histórico dos vários documentos por um período de pelo menos 3 anos.

PROCESSO DE SUBMISSÃO DE EXCEÇÃO

Todos os funcionários da Prefeitura do Município de Osasco envolvidos com a segurança da informação devem submeter uma solicitação de exceção para estar em conformidade com a política. As exceções de aplicação da política devem ser aprovadas pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco.

REVISÃO DAS EXCEÇÕES

Todas as exceções às políticas aprovadas devem ser revistas pelo menos a cada 6 meses.

REVISÃO DAS POLÍTICAS PELOS FUNCIONÁRIOS

Todos os funcionários e contratados devem rever e dar ciência formalmente das políticas de segurança da informação que se aplicam em seu trabalho e responsabilidade do seu cargo ou função pelo menos numa base anual.

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação deve determinar exceções a esta Política.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

VIOLAÇÕES

O funcionário da Prefeitura do Município de Osasco que violar deliberadamente esta política ficará sujeito a ações disciplinares.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Revisão da Política de Segurança da Informa	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Revisão da Política de Segurança da Informa	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Revisão da Política de Segurança da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Comprometimento da Subsecretaria de Tecnologia da Informação Com a Segurança da Informação

Norma 03 Data:25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Demonstrar o comprometimento da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco com a segurança da informação.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica às Responsabilidades da Subsecretaria de Tecnologia da Informação da Prefeitura de Osasco em relação à Segurança da Informação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – A Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco possui responsabilidades definidas pela presente Norma, no que tange à Segurança da Informação.

SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

A Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco deve, periodicamente, rever o status do sistema de gerenciamento da segurança da informação, aprovar políticas e projetos de segurança da informação.

RISCOS SIGNIFICANTES DE SEGURANÇA DA INFORMAÇÃO

A Subsecretaria de Tecnologia da Informação deve estar ciente dos principais riscos de segurança da informação que possam afetar o funcionamento da organização e, por isso, deve tomar decisões para mitigar ou contingenciar o risco.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

ALOCAÇÃO DE RECURSOS PARA A SEGURANÇA DA INFORMAÇÃO

A Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco deve assegurar os recursos humanos, materiais, assim como serviços e produtos e recursos orçamentários adequados para tratar da segurança da informação.

SEGURANÇA DA INFORMAÇÃO COMO RESPONSABILIDADE GERENCIAL

A segurança da informação é uma responsabilidade gerencial de cada um dos Secretários (as), Diretores (as) e Gerentes da Prefeitura do Município de Osasco, os quais devem garantir o comprometimento e seguimento das políticas de segurança da informação, assim como comunicar qualquer incidente correspondente à Subsecretaria de Tecnologia da Informação.

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Comprometimento da Subsecretaria de Tecnologia da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Comprometimento da Subsecretaria de Tecnologia da Informação	25/02/21	

HISTÓRICO DE REVISÃO

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Comprometimento da Direção com a Segurança da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Coordenação da Segurança da Informação

Norma 04 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br
Version **1.0**

PROPÓSITO

Convém que as atividades de segurança da informação sejam coordenadas pela Subsecretaria de Tecnologia da Informação e aplicadas pelos representantes de diferentes partes da organização, com funções e papéis relevantes.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica às atividades da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco a centralização das atividades relacionadas à segurança da informação, também é responsabilidade de representantes das demais áreas da organização exercer atividades inerentes em sua área de atuação.

CENTRALIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

A direção, orientação e autoridade para todas as atividades de segurança da informação são centralizadas para toda a organização pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco.

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Secretários (as), Diretores (as) e Gerentes devem assegurar que a segurança da informação dentro de suas unidades seja tratada como uma atividade constante de sua atribuição do dia a dia. Secretários (as), Diretores (as) e Gerentes têm a responsabilidade de promover e comunicar a aplicação das Normas de segurança da informação em suas unidades, tornando os funcionários e terceiros cientes de sua responsabilidade do sistema de gerenciamento da segurança da informação.

REPRESENTANTE DA SEGURANÇA DA INFORMAÇÃO

Cada Órgão da Administração Direta do Município de Osasco deverá designar um representante para a segurança da informação junto ao Comitê de Tecnologia da Informação, o qual deve ser treinado para exercer a função, assim como receber o suporte e materiais necessários para desempenhar as atividades.

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Coordenação da Segurança da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Coordenação da Segurança da Informação	25/02/21	

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Coordenação da Segurança da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Atribuição de Responsabilidades Pela Segurança da Informação

Norma 05 Data:25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica às responsabilidades pelas atividades de Segurança da Informação no âmbito da Prefeitura do Município de Osasco.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação determinar formalmente os proprietários das informações, indicar o responsável pelas atividades de cópias de segurança, designar os Administradores de Segurança, aprovar mudanças em sistemas e realizar revisões nos mesmos.
É de responsabilidade da Diretoria de Administração de Recursos Humanos e Diretoria de Gestão de Pessoas informar mudanças na situação do servidor.
É de responsabilidade das Secretarias informar mudanças na situação de estagiários, prestadores de serviços e demais parceiros.
É de responsabilidade de todos os funcionários da Prefeitura do Município de Osasco, estagiários, prestadores de serviços e demais cumprirem as Políticas de Segurança da Informação.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

ATRIBUIÇÃO DO PROPRIETÁRIO DA INFORMAÇÃO

A Subsecretaria de Tecnologia da Informação deve determinar formal e claramente as responsabilidades dos proprietários das informações em termos de criação e manutenção de coleções de informações do negócio da Prefeitura do Município de Osasco, independente da forma de armazenamento.

MUDANÇA DA SITUAÇÃO DO TRABALHO

Qualquer mudança na situação de trabalho de funcionários e terceiros da Prefeitura do Município de Osasco deverá ser informada pela Secretaria de Administração a qual deverá informar imediatamente ao Administrador de Segurança da Informação, responsável pelo controle de acesso aos sistemas de informação da organização.

O mesmo ocorre quanto a fornecedores. Neste caso cada Secretaria deverá informar diretamente ao Administrador de Segurança da Informação.

ADMINISTRADOR DE SEGURANÇA DA INFORMAÇÃO

A Subsecretaria de Tecnologia da Informação deve designar um Administrador da Segurança da Informação com responsabilidades no tocante a definição de privilégios para usuários, controle de senhas e acessos à rede da Prefeitura do Município de Osasco, monitoração e log dos acessos e o desempenho de atividades similares.

ADMINISTRADOR DE CÓPIAS DE SEGURANÇA

A Subsecretaria de Tecnologia da Informação deve designar formalmente um funcionário responsável por executar a política de back-up da Prefeitura do município de Osasco, providenciar o treinamento necessário para as suas atividades, assim como capacitá-lo nas atividades do Administrador de Segurança da Informação.

APROVAÇÃO DE MUDANÇAS EM SISTEMAS DE INFORMAÇÃO

Todos os projetos antes de iniciar, assinar contratos ou realizar promessas que culminem em mudanças no ambiente de hardware, software e comunicações da Prefeitura do Município de Osasco, deverão ter aprovação formal da Subsecretaria de Tecnologia da Informação.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

OUTRAS RESPONSABILIDADES DA SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

As responsabilidades da Subsecretaria de Tecnologia da Informação, no âmbito da Segurança da Informação da Prefeitura do Município de Osasco são:

- ✓ Elaborar, coordenar a implantação, manter e realizar avaliações de conformidade da Política de Segurança da Informação da Prefeitura do Município de Osasco;
- ✓ Definir, implantar e revisar controles;
- ✓ Identificar riscos inerentes e residuais de segurança da informação;
- ✓ Definir os critérios e procedimentos para a classificação e rotulação da informação;
- ✓ Desenvolver e implantar programas de conscientização no âmbito da Prefeitura do Município de Osasco;
- ✓ Analisar a eficácia dos controles implantados e propor melhorias no sistema de gerenciamento de segurança da informação;
- ✓ Implantação dos projetos e iniciativas em segurança da informação;
- ✓ Definir medidas e soluções em segurança de informação, operacionais;
- ✓ Elaborar programas de treinamento em segurança da informação;
- ✓ Implantar novos controles de segurança para a melhoria contínua das medidas de proteção;
- ✓ Identificar riscos inerentes e residuais de segurança da informação;
- ✓ Apoio à implantação de soluções para a minimização dos riscos;
- ✓ Gerir ocorrência dos incidentes em segurança da informação e seu impacto na organização e seu público-alvo;
- ✓ Elaborar e manter Planos de Desastre e Recuperação e Planos de Continuidade de Serviços de TI;
- ✓ Gerenciar crises em segurança da informação, como indisponibilidade de serviços críticos, perda de dados, etc.;

- ✓ Apoiara Procuradoria Geral do Munícipio da Prefeitura do Município de Osasco quanto a questões legais relativas à segurança da informação;
- ✓ Definir as responsabilidades operacionais em segurança da informação a serem seguidas pelas Diretorias da Subsecretaria de Tecnologia da Informação;
- ✓ Apoiar as pastas responsáveis da Prefeitura do Município de Osasco em processos disciplinares como sindicâncias relativos a violações críticas em segurança da informação realizadas por fornecedores e funcionários;
- ✓ Garantir que o Sistema de Gerenciamento de Segurança da Informação seja seguido no âmbito da Prefeitura do Município de Osasco;
- ✓ Aprovação de políticas, normas e procedimentos de segurança da informação;
- ✓ Designação, definição ou alteração das responsabilidades da área de Segurança da Informação;

Responsabilidades Dos Funcionários e Terceiros

Todo funcionário prestador de serviço e demais prestadores de serviços da Prefeitura do Município de Osasco deve seguir a Política de Segurança da Informação em suas atividades do dia a dia. No caso dos funcionários da Prefeitura do Município de Osasco deverão ser atribuídas formalmente em suas atribuições, responsabilidades relativas à Segurança da Informação. No caso de fornecedores e demais terceiros, cláusulas específicas nos respectivos contratos de fornecimento de serviços.

Exceções

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

Referências

NBR ISO/IEC 27002:2013

Documentos Relacionados

Nenhum

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Atribuição de Responsabilidades Pela Segurança da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Atribuição de Responsabilidades Pela Segurança da Informação	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Atribuição de responsabilidades para a segurança da informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Processo de Autorização Para os Recursos de Processamento da Informação

Norma 06 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Convém que seja definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica ao uso de recursos de processamento de informação no âmbito da Prefeitura do Município de Osasco.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação autorizar novos recursos de processamento da informação e participar na aprovação de mudanças no ambiente de hardware e software.

AUTORIZAÇÃO PARA USO DE NOVOS SERVIÇOS DE PROCESSAMENTO DA INFORMAÇÃO

O uso de novos serviços de Internet e de mensagens instantâneas deve ser aprovado pela Subsecretaria de Tecnologia da Informação, a qual analisará e revisará o novo serviço quanto ao risco à segurança da informação da Prefeitura do Município de Osasco.

USO DE NOVAS TECNOLOGIAS

Os controles de segurança da informação devem ser restritos a novas tecnologias no ambiente de produção de forma a garantir que sejam confiáveis e apoiem efetivamente o negócio da Prefeitura do Município de Osasco.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Desabilitação de Componentes de Segurança da Informação

Componentes críticos de segurança da informação da Prefeitura do Município de Osasco não podem ser desconectados, desligados, desabilitados e nem suprimidos sem a aprovação formal da Subsecretaria de Tecnologia da Informação.

Exceções

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

Referências

NBR ISO/IEC 27002:2013

Documentos Relacionados

Nenhum

Aprovação

Criado por	Título	Data	Assinatura
STI	Processo de Autorização Para os Recursos de Processamento da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Processo de Autorização Para os Recursos de Processamento da Informação	25/02/21	

Histórico de Revisão

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Processo de Autorização Para Recursos de Processamento da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Termo de Confidencialidade e Propriedade Intelectual

Norma 07 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica à proteção legal de informações secretas e confidencias da Prefeitura do Município de Osasco e se aplicam a todos os funcionários e terceiros (estagiários, prestadores de serviços e demais).

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade de cada Secretaria Municipal garantir a aplicação da política.

DIREITOS DE PROPRIEDADE

- Toda a documentação, programas de computador, estudos e pesquisas produzidos por funcionários da organização é de propriedade legal da Prefeitura do Município de Osasco;
- Todos os programas de computador, os estudos, as documentações e as pesquisas produzidos por terceiros em função da execução de um contrato estabelecido com a Prefeitura do Município de Osasco são de propriedade legal da Prefeitura do Município de Osasco;
- Todos os terceiros em contrato com a Prefeitura do Município de Osasco, devem assinar um Termo de Confidencialidade antes do início dos trabalhos;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Acordos de Confidencialidade e Propriedade Intelectual	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Acordos de Confidencialidade e Propriedade Intelectual	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Acordos de Confidencialidade e Propriedade Intelectual

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Contatos Com Autoridades

Norma 08 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Convém que contatos com autoridades relevantes sejam mantidos.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica ao contato com autoridades relevantes no caso da necessidade de informá-los, em tempo hábil, sobre a ocorrência de incidentes em segurança da informação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação realizar o contato com autoridades relevantes no caso da ocorrência de incidentes de Segurança da Informação, contatos com bombeiros e concessionárias de serviços públicos e, por fim, acionar o Gabinete do Chefe do Executivo e a Procuradoria Geral para que avaliem a necessidade de comunicarem a Polícia e o Judiciário.

COMUNICAÇÃO DE VIOLAÇÃO EXTERNA

- Violações a segurança da informação na Prefeitura do Município de Osasco somente serão comunicadas às autoridades relevantes se existir dispositivo legal que estipule essa obrigação. Tais violações quando forem comunicadas devem ser informadas à Subsecretaria de Tecnologia da Informação.

- A Subsecretaria de Tecnologia da Informação deve comunicar às demais autoridades relevantes.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

COMUNICAÇÃO COM BOMBEIROS E OUTROS CONCESSIONÁRIOS DE SERVIÇOS PÚBLICOS

A Subsecretaria de Tecnologia da Informação deverá manter uma lista com os telefones dos Bombeiros e demais Concessionários de Serviços Públicos como Água, Energia e Telefonia para o caso de ser necessário seu acionamento face a ocorrência de incidentes que afetam o funcionamento dos serviços de TI fornecidos a Prefeitura do Município de Osasco.

COMUNICAÇÃO A POLÍCIA E JUDICIÁRIO

No caso de violação da segurança da informação que afete o funcionamento dos serviços da Prefeitura do Município de Osasco e cuja fonte de violação seja identificada, a Subsecretaria de Tecnologia da Informação deve acionar a Procuradoria Geral da Prefeitura do Município de Osasco para avaliar a necessidade de procedimentos investigativos e/ou legais contra a fonte. A decisão de se realizar contato com a Polícia ou o Judiciário é da Procuradoria Geral da Prefeitura do Município de Osasco.

EXCEÇÕES

O responsável pela Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Contatos Com Autoridades	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Contatos Com Autoridades	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Contato com Autoridades

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Contatos Com Grupos Especiais

Norma	09	Data:25/02/21		Email	sti.sf@osasco.sp.gov.br
Version	1.0				

PROPÓSITO

Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica aos membros da Subsecretaria de Tecnologia da Informação, visando o seu contínuo aprimoramento.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação manter contatos com associações profissionais e instituições públicas e privadas de ensino e treinamento em segurança da informação.

TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

- Para assegurar que os funcionários envolvidos em segurança da informação na Prefeitura do Município de Osasco fiquem cientes de novos desenvolvimentos na área, a Subsecretaria de Tecnologia da Informação deve promover um plano de desenvolvimento técnico anual para cada funcionário, assim como promover o engajamento desses funcionários em fóruns especializados e participar de associações profissionais na área;

- A Subsecretaria de Tecnologia da Informação deve incentivar seus funcionários a participarem de fóruns e associações especializadas em segurança da informação, apoiando, inclusive a obtenção de certificações profissionais específicas em segurança da informação;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Contatos Com Grupos Especiais	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Contatos Com Grupos Especiais	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Contatos com Grupos Especiais

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Revisão Independente da Segurança da Informação

Norma	10	Data: 25/02/21		Email	sti.sf@osasco.sp.gov.br
Version	1.0				

PROPÓSITO

Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política se aplica a testes de intrusão, assim como a verificação de compliance com as políticas de segurança da informação, por meio de terceiras partes independentes.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação programar e acompanhar as revisões independentes do sistema de segurança da informação da Prefeitura do Município de Osasco.

TESTES DE INTRUSÃO

A Subsecretaria de Tecnologia da Informação deve contratar, a intervalos planejados, a realização de serviços de testes de intrusão por empresa conceituada, visando a verificação das vulnerabilidades internas e externas de acesso à rede da Prefeitura do Município de Osasco.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

VERIFICAÇÕES DE COMPLIANCE

A Subsecretaria de Tecnologia da Informação deve contratar, a intervalos planejados, serviços de auditoria independente para verificar a conformidade das atividades de segurança da informação na Prefeitura do Município de Osasco com os controles e políticas determinadas pelo Sistema de Gerenciamento da Segurança da Informação, assim como a padrões reconhecidos de melhores práticas na área.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Revisão Independente da Segurança da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Revisão Independente da Segurança da Informação	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Revisão Independente da Segurança da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Segurança da Informação com Terceiros

Norma 11 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por terceiros.

ESCOPO E APLICAÇÃO

Aplicação – Para o gerenciamento da segurança da informação relacionado com partes externas ao da Prefeitura do Município de Osasco.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade de terceiros seguir a Política de Segurança da Informação, a Subsecretaria de Tecnologia da Informação deve autorizar acesso interno e externo aos recursos de processamento de informação e avaliar a Política de Segurança da Informação de fornecedores de serviços, além de aprovar terceirização de serviços de processamento de informação e de segurança da informação e aprovar a aceitação de requisitos de segurança da informação de clientes externos, o proprietário da informação deve aprovar acesso às informações sensíveis e confidenciais sob sua responsabilidade.

RISCOS RELACIONADOS COM TERCEIROS

- Todo terceiro, fornecedor, consultor e prestador de serviços deverá cumprir a Política de Segurança da Informação da Prefeitura do Município de Osasco;
- Pessoas que não tem relação de trabalho com a Prefeitura do Município de Osasco sejam funcionários ou terceiros não poderão ter acesso aos recursos de processamento da informação da organização, com exceção ao acesso a informações consideradas públicas;

- Acesso externo ou interno aos recursos de processamento da informação da organização somente poderá ser permitido se houver a necessidade da terceira parte em ter acesso por força de contrato e deverá ter a autorização da Subsecretaria de Tecnologia da Informação;

- Toda terceira parte deverá assinar um Termo de Confidencialidade no acesso a informações da Prefeitura do Município de Osasco;

- Acesso a informações sensíveis por terceiros somente poderá ocorrer com a autorização do proprietário da informação;

- A terceirização de parte de serviços de processamento de informações e de segurança da informação deverá ser precedida de uma análise de risco e aprovada pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco;

- A Subsecretaria de Tecnologia da Informação deve, quando apropriado, avaliar objetivamente a Política de Segurança da Informação de fornecedores de serviços.

SEGURANÇA DA INFORMAÇÃO RELACIONADA COM CLIENTES

- Os requisitos de segurança da informação de clientes dos serviços da Prefeitura do Município de Osasco ou em relação àqueles que desejam hospedar seus sistemas no Data Center da Prefeitura do Município de Osasco deverão ser avaliados e cotejados com a Política de Segurança da Informação da Prefeitura do Município de Osasco e caso aumentem os custos de gestão e a criação de vulnerabilidades, a aceitação desses requisitos deverá ser dada formalmente pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Segurança da Informação com Terceiros	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Segurança da Informação com Terceiros	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Gerenciamento de Ativos

Norma	12	Data:25/02/21		Email	sti.sf@osasco.sp.gov.br
Version	1.0				

PROPÓSITO

Alcançar e manter a proteção adequada dos ativos da organização.

ESCOPO E APLICAÇÃO

Aplicação – A todos os ativos de processamento de informação da Prefeitura do Município de Osasco e aos seus usuários.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação a identificação de sistemas críticos e a aprovação de trabalho remoto, a preparação de inventário de todos os ativos de informação, o uso das normas internas para aquisição de ativos, o proprietário da informação é responsável por determinar a classificação da informação, sobre direitos de acesso à informação e por assegurar que controles adequados estão sendo empregados sobre os ativos de informação sob sua responsabilidade, os funcionários da Prefeitura do Município de Osasco devem seguir as normas sobre uso de ativos de informação.

INVENTÁRIO DE ATIVOS

- Anualmente a Subsecretaria de Tecnologia da Informação deve identificar os serviços e sistemas críticos para a Prefeitura do Município de Osasco;

- Anualmente a Subsecretaria de Tecnologia da Informação deve preparar um inventário de todos os ativos de tecnologia da informação, como sistemas, software, hardware e links de comunicação;

- Os responsáveis pelos equipamentos devem manter os registros do inventário de equipamentos sob a sua responsabilidade assim como controlar a sua movimentação;

- Todos os hardwares, softwares e dispositivos de comunicação devem ser adquiridos seguindo as normas internas e conforme a legislação vigente de aquisições;

- Todos os equipamentos computacionais e de comunicação devem ter um identificador de patrimônio ou um identificador próprio caso não seja item patrimonial da Prefeitura do Município de Osasco;

PROPRIEDADE DOS ATIVOS

- Toda informação processada por ou usada por uma unidade da Prefeitura do Município de Osasco deve designar, junto a Subsecretaria de Tecnologia da Informação, o proprietário da informação responsável por: (1) determinar a classificação da informação; (2) decidir que pode ter acesso às informações; (3) e assegurar que controles adequados estão implantados para armazenamento, distribuição e uso das informações;

- O proprietário da informação, juntamente com a Subsecretaria de Tecnologia da Informação, deve definir os controles requeridos sobre os ativos de informação;

- A Prefeitura do Município de Osasco tem a propriedade legal do conteúdo de todas as mensagens e arquivos armazenados em seus computadores e redes e se reserva o direito de acessar essas informações sem notificação quando for necessário por razões de suas atividades e serviços;

- Com exceção dos sistemas operacionais e de gerenciamento da rede, a Subsecretaria de Tecnologia da Informação não pode ser designada como proprietários da informação;

- Se o proprietário da informação não puder ser facilmente identificado, a Subsecretaria de Tecnologia da Informação será, por "default", designada como proprietária dessa informação;

- Todos os usuários dos sistemas da Prefeitura do Município de Osasco devem se submeter aos requisitos de acesso especificados pelo proprietário da informação;

- As obrigações do proprietário da informação não podem ser delegadas para fornecedores de serviços ou para indivíduos com trabalho temporário na Prefeitura do Município de Osasco;

USO ACEITÁVEL DE ATIVOS

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Os funcionários da Prefeitura do Município de Osasco podem usar mensagens de e-mail eletrônicas primariamente para os propósitos das atividades da organização, sendo que o uso desse recurso de comunicação não pode interferir nas atividades da Prefeitura do Município de Osasco, nem criar embaraço para Prefeitura do Município de Osasco e nem para outras atividades pessoais com o fim de gerar lucros;

- Os funcionários da Prefeitura do Município de Osasco não podem usar os recursos da Internet para participar em fóruns públicos e redes sociais não relacionadas com as atividades da Prefeitura do Município de Osasco e de sua função na organização;

- Os recursos de mensagens instantâneas corporativas da Prefeitura do Município de Osasco somente podem ser usados para fins relacionados às atividades e serviços da Prefeitura do Município de Osasco;

- Funcionários da Prefeitura do Município de Osasco que desejam usar serviços de e-mail para fins pessoais devem usá-lo através de contas pessoais em provedores de serviços de internet disponíveis no mercado;

- Uso dos telefones da Prefeitura do Município de Osasco pelos funcionários deve seguir as Normas Administrativas vigentes;

- O uso dos recursos de tecnologia da informação da Prefeitura do Município de Osasco pelos funcionários, de forma remota, deve ter autorização do proprietário da informação e da Subsecretaria de Tecnologia da Informação.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Gerenciamento de Ativos	25/02/21	

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Aprovado por	Título	Data	Assinatura
STI	Gerenciamento de Ativos	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Gerenciamento de Ativos

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Classificação da Informação

Norma	13	Data: 25/02/21		Email	sti.sf@osasco.sp.gov.br
Version	1.0				

PROPÓSITO

O sistema de classificação da informação da Prefeitura do Município de Osasco está definido de acordo com a Lei Federal nº 12.527/2011 e o Decreto Municipal nº 11.440/2017. Este conceito, quando combinado com as políticas definidas neste documento, protegerá a Prefeitura do Município de Osasco contra o uso não autorizado da informação, sua modificação e deleção.

ESCOPO E APLICAÇÃO

Aplicação – Esta Política de Classificação da Informação é aplicável a toda informação possuída pela Prefeitura do Município de Osasco ou sob seu controle. Por exemplo, informações confidenciais mantidas de usuários e clientes dos serviços da Prefeitura do Município de Osasco, fornecedores e parceiros e outras terceiras partes devem ser protegidas com esta Política. Espera-se dos funcionários da Prefeitura do Município de Osasco a proteção de informações de terceiras partes da mesma forma que protegem a informação da Prefeitura do Município de Osasco.

PAPÉIS E RESPONSABILIDADES

Responsabilidades dos funcionários da Prefeitura do Município de Osasco – Todo funcionário que tem acesso às informações ou aos sistemas de informação da Prefeitura do Município de Osasco tem um papel importante na segurança da informação na organização. Por exemplo cada funcionário é pessoalmente responsável pela proteção da informação sob os seus cuidados. Todo funcionário que entra em contato com informações internas sensíveis devem estar familiarizado com esta política de classificação da informação. Informação sensível é Confidencial ou Secreta. Embora esta política preveja um guia geral para atender a proteção consistente da informação, espera-se que os funcionários da Prefeitura do Município de Osasco a apliquem no seu dia a dia.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

CONTROLE DE ACESSO

Necessidade de conhecer – A informação somente pode ser disponibilizada para pessoas que tem o direito legítimo de usar a informação para fins de executar suas atividades na organização. Este princípio se aplica, por exemplo, a informações sobre histórico médico do funcionário e informações da Prefeitura do Município de Osasco como planos, projetos de novos serviços e produtos, seguindo os preceitos da Lei Federal nº 12.527/2011 e do Decreto Municipal nº 11.440/2017.

Controles de Acesso – Acesso a toda informação sensível da Prefeitura do Município de Osasco deve ser protegida contra uso impróprio, modificação e deleção. Independente da tecnologia usada o controle de acesso deve ser controlado para cada funcionário em função de sua necessidade de acesso para realizar o seu trabalho.

Decisões Sobre Direitos de Acesso – Acesso à informação sensível da Prefeitura do Município de Osasco deve ser garantido somente após autorização do proprietário da informação e seguindo o disposto na Lei Federal nº 12.527/2011 e no Decreto Municipal nº 11.440/2017.

RÓTULOS DE CLASSIFICAÇÃO

Proprietários e Produtores da Informação – Toda informação produzida por uma unidade organizacional da Prefeitura do Município de Osasco deve ter um proprietário designado. Os proprietários da informação são responsáveis pela rotulação da informação como definido a seguir e seguindo o determinado na Lei Federal nº 12.527/2011 e no Decreto Municipal nº 11.440/2017.

- **SECRETO** – Esta classificação se aplica às informações mais sensíveis tratadas pela Prefeitura do Município de Osasco e que podem trazer danos a sua imagem, ao seu normal funcionamento, seus usuários, parceiros e fornecedores.

- **CONFIDENCIAL** – Esta classificação se aplica a informações menos sensíveis da Prefeitura do Município de Osasco como, por exemplo, avaliações de desempenho do pessoal, estudos e pesquisas ainda não publicadas, senhas de acesso aos sistemas, relatórios de auditoria, etc.

- **PARA USO INTERNO SOMENTE** – Esta classificação se aplica para todas as informações que não se enquadram nas duas classificações acima. Exemplos incluem a lista de telefones dos funcionários, manuais de normas internas, materiais de treinamento, etc.

- **PÚBLICO** – Esta classificação aplica-se a toda informação que pode ser disponibilizada para o público externo a Prefeitura do Município de Osasco. Exemplos: portais, produtos e serviços da Prefeitura do Município de Osasco, comunicação externa, etc.

- **Outros Rótulos** – Esquemas de classificação específicos podem ser permitidos como informações privadas ou financeiras, mas têm que ser compatíveis com o esquema de classificação acima definido.

Decisões de Acesso dos Proprietários - Os proprietários devem tomar decisões acerca sobre a quem será dada a permissão para ganhar acesso à informação.

ROTULAÇÃO

Classificação Consistente – Se a informação é sensível, desde o momento da sua criação até o momento da sua destruição, deve ser rotulada de forma apropriada em todas as mídias, impressa ou digital. Os funcionários não poderão remover o rótulo sem expressa autorização do proprietário da informação.

Informação sem Rótulo – Informação sem rótulo é, por default, informação que pode ser publicizada externamente de acordo com o determinado na Lei Federal nº 12.527/2011 e no Decreto Municipal nº 11.440/2017.

Coleções de Informações – Criações de coleções de informações devem ser notificadas aos respectivos proprietários das informações. Se na coleção tiver informação PARA USO INTERNO SOMENTE e CONFIDENCIAL, a coleção inteira deverá ser rotulada como CONFIDENCIAL. Se tiver informação SENSÍVEL e outro tipo de classificação deverá ser rotulado como SENSÍVEL.

Mídia de Armazenamento – Se a informação armazenada numa mídia digital com uma classificação Sensível for movida para uma mídia de menor grau de classificação então ela deve ser atualizada para Sensível. Se vários níveis de classificação da informação são residentes em um computador então o controle do sistema deverá refletir os requisitos da classificação mais restritiva que estiver armazenada.

Rótulos Para Informações Fornecidas Externamente – Todas as informações recebidas de fontes externas devem ser classificadas visando à proteção dos direitos de propriedade.

Rótulos de Documentos – Todo documento impresso (seja a mão ou não) que tenha informação sensível deverá ter classificação apropriada clara e evidente, seja no rodapé, seja marca d'água, na capa do documento, etc. O mesmo se aplica a informações sensíveis contidas em microfichas.

Rótulo para Mídias de Armazenamento em Computadores – Todas as mídias que têm informação sensível devem ser rotuladas de forma apropriada. Isto inclui CD´s, DVD´s, hard-disk, pen-drive e outros meios de armazenamento digital. A menos que afete o funcionamento do programa, arquivos de computadores devem ter o rótulo no caso de informação sensível.

Rótulo Adicional de Informação Pública – Informação pública também pode ser classificada como – Aprovada para Distribuição Pública. A aprovação deve ser obtida junto ao proprietário da informação.

Uso de Gravadores – Informações sensíveis não podem estar gravadas em aparelhos como telefones celulares, gravadores de bolso, etc.

INTERAÇÕES COM TERCEIRAS PARTES

Necessidades de Conhecimento por Terceiros – A menos que a informação seja classificada como pública toda e qualquer informação interna tem que ser protegida do acesso por terceiros. Terceiros podem ter acesso à informação interna da Prefeitura do Município de Osasco quando ficar demonstrado sua necessidade ou quando o acesso for autorizado pelo Proprietário da Informação. Para efeito desta política, consultores, estagiários, fornecedores de qualquer tipo são considerados terceiros.

Disponibilização para Terceiros e Acordos de Confidencialidade – A disponibilização de informações para terceiros deve ser precedida pela assinatura de um Termo de Confidencialidade. É recomendável que a informação que o terceiro irá ter acesso seja registrada no Termo de Confidencialidade.

Solicitações de Informações por Terceiros – A menos que o funcionário da Prefeitura do Município de Osasco esteja autorizado pelo proprietário da informação, todas as solicitações de informações sobre a Prefeitura do Município de Osasco, como respostas a pesquisas, enquetes ou o equivalente, deverá ser encaminhado a cada pasta proprietária da informação para que a mesma realize os devidos esclarecimentos.

Revisão Prévia – Cada palestra, apresentação, ou outra comunicação a ser disponibilizada para o público deve ser aprovado pelas Secretarias, Diretorias e Gerências para liberação. Esta política se aplica a toda informação obtida pelo funcionário a partir do seu trabalho na Prefeitura do Município de Osasco.

Notificação ao Proprietário – Se a informação sensível é perdida, o proprietário da informação e o responsável pela segurança da informação devem ser notificados imediatamente.

EXPEDIÇÃO E MANUSEIO

Cópias – De informações sensíveis devem ter a autorização do proprietário da informação.

Uso de Serviços Externos – Antes de enviar informação sensível para terceiros fazerem cópias, impressão ou formatação ou outro manuseio, o terceiro deverá assinar um Termo de Confidencialidade.

Numeração de Páginas – Toda informação sensível manifestada em papel deve indicar a primeira e a última página.

Mídias de Cópias de Segurança – Toda informação sensível armazenada fora da Prefeitura do Município de Osasco deverá ser criptografada.

Envelopes – Se a informação sensível for enviada por malote interno, serviços de entrega, correios a mesma deverão ser colocada em dois envelopes, um dentro do outro, sendo que o envelope de fora não poderá indicar a natureza da informação.

Saídas de Computadores – Saídas impressas de informações sensíveis somente podem ser fornecidas pessoalmente ao recipiente designado de forma protocolada.

Remoção de Escritórios – Informação sensível não pode ser removida do escritório ou instalações da Prefeitura do Município de Osasco a menos que tenha autorização do proprietário da informação.

Guarda em cofres – A informação sensível impressa quando não em uso, deve ser guardada em local seguro aprovado pelo Subsecretaria de Tecnologia da Informação.

Avisos Orais – Se informações confidenciais são transmitidas oralmente em uma reunião o apresentador, condutor da reunião ou apresentador, tem que dar ciência sobre o grau de confidencialidade da informação à audiência.

Celulares – Funcionários não deverão falar sobre informação sensível em celulares ou dispositivos como MSN, Skype e outros.

DESCLASSIFICAÇÃO E REBAIXAMENTO

Datas de Reclassificação - Se do conhecimento, a data em que a informação sensível será desclassificada tem que ser indicada em toda informação sensível da Prefeitura do Município de Osasco.

Extensões de Classificação – O proprietário da informação poderá estender o período de validade da classificação da informação.

Notificações – O proprietário da informação pode, a qualquer tempo, desclassificar ou rebaixar a classificação da informação sob seus cuidados.

Revisão – O proprietário da informação deverá rever, anualmente, a classificação das informações sob sua responsabilidade.

Autorização de Rebaixamento – Somente poderá ser realizada com a aprovação formal do proprietário da informação.

DESTRUIÇÃO E DESCARTE

Destruição e Descarte – Toda a informação da Prefeitura do Município de Osasco, independente do meio em que se encontra, deve ser destruída quando não tiver mais necessidade de seu uso, seguindo a legislação vigente. Para apoiar esta política, o proprietário da informação tem que rever, periodicamente, o valor e utilidade da informação. Os proprietários das informações também devem rever a programação de retenção da informação.

Aprovação da Destruição – O proprietário da informação é a autoridade para decidir sobre a destruição da informação e deverá aprovar a destruição da informação.

SEGURANÇA FÍSICA

Acesso às Instalações – Áreas que contêm informação sensível devem ter o seu acesso controlado.

EXCEÇÕES

A Subsecretaria de Tecnologia da Informação poderá determinar exceções a esta Política.

VIOLAÇÕES

O funcionário da Prefeitura do Município de Osasco que violar deliberadamente esta política ficará sujeito a ações disciplinares.

REFERÊNCIAS

NBR ISO/IEC 27002:2013, Decreto Municipal nº 11.440/2017 e Lei Federal nº 12.527/2011

DOCUMENTOS RELACIONADOS

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	**Classificação da Informação**	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	**Classificação da Informação**	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Classificação da Informação

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Gerenciamento de Segurança em Recursos Humanos

Norma 14 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mal-uso de recursos.

ESCOPO E APLICAÇÃO

Aplicação – A segurança relacionada aos recursos humanos da Prefeitura do Município de Osasco, fornecedores e terceiros.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da informação fomentar junto a área de recursos humanos a alteração de descrições de cargos vigentes, a inclusão de atributos de segurança da informação nas avaliações de desempenho, a transferência para outras funções funcionários com histórico médico que coloque em risco ativos de informação da Prefeitura do Município de Osasco, a implantação de um programa de conscientização em segurança da informação, a execução do plano de treinamento elaborado pela Subsecretaria de Tecnologia da Informação e fornecer registros pessoais aos funcionários.
É de responsabilidade da área contratante a averiguação a priori de terceiros.
É de responsabilidade da Procuradoria Geral do Município garantir os direitos de propriedade da Prefeitura do Município de Osasco.
É de responsabilidade das Secretarias, Diretorias e Gerencias e outros funcionários em cargos de chefia garantir o retorno de ativos de funcionários ou terceiros cujos contratos estejam terminando.
É de responsabilidade das Secretarias, Diretorias e Gerencias o encaminhamento das ocorrências à Procuradoria Geral do Município para aplicação de medidas disciplinares.

- As responsabilidades do funcionário a respeito da Política de Segurança da Informação da Prefeitura do Município de Osasco devem estar descritas em toda nas atribuições do cargo;

- A conformidade com a Política de Segurança da Informação deve ser colocada como item a ser considerado em avaliações de desempenho dos funcionários;

AVALIAÇÃO A PRIORI DE TERCEIROS

- Temporários, consultores e demais terceiros que sejam contratados para execução de serviços por tempo determinado na Prefeitura do Município de Osasco e que podem ter acesso a ativos críticos e sensíveis podem ser averiguados previamente quanto aos aspectos de histórico em outras organizações;

- Pessoas que já foram "hackers" ou que tenham processos legais em andamento, relativamente a crimes virtuais, não podem ser alocadas por terceiros para a prestação de serviços de qualquer natureza na Prefeitura do Município de Osasco;

DURANTE A CONTRATAÇÃO OU PRESTAÇÃO DE SERVIÇOS

- Enquanto funcionário ou contratado da Prefeitura do Município de Osasco, deve garantir a Prefeitura do Município de Osasco todos os direitos de patentes, direito de propriedade intelectual, invenções que por eles foram originadas ou geradas;

RESPONSABILIDADES GERENCIAIS

- A responsabilidade pela Segurança da Informação na Prefeitura do Município de Osasco é de todos os funcionários e não somente da Subsecretaria de Tecnologia da Informação;

- Funcionários da Prefeitura do Município de Osasco não podem aceitar suporte em informática de empresas que não mantenham relação contratual com a Prefeitura do Município de Osasco, exceção é feita com suporte fornecido por comunidades de práticas ou grupos de usuários "open source". Entretanto tal suporte deverá ser aprovado pela Subsecretaria de Tecnologia da Informação;

- A qualquer momento o funcionário terá o direito de ter acesso a informações a seu respeito nos registros da área de recursos humanos da Prefeitura do Município de Osasco para verificar sua acuidade e solicitar possíveis correções;

-
- Propriedade intelectual desenvolvida ou concebida enquanto o funcionário esteja trabalhando fora das instalações da Prefeitura do Município de Osasco em termos de planos, programas de computador, patentes, relacionadas às suas atividades e desempenho de função também são de propriedade da Prefeitura do Município de Osasco;
  -

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO, TREINAMENTO E EDUCAÇÃO

- Usuários somente poderão ter acesso aos ativos de informação da Prefeitura do Município de Osasco se derem ciência, por escrito, acerca da Política de Segurança da Informação da Prefeitura do Município de Osasco;

- Os funcionários da Prefeitura do Município de Osasco e terceiros devem participar de treinamentos específicos a ser dado pela Subsecretaria de Tecnologia da Informação a respeito da Política de Segurança da Informação da Prefeitura do Município de Osasco;

- Todo funcionário da Prefeitura do Município de Osasco ou terceiro deve receber um manual com a Política de Segurança da Informação da Prefeitura do Município de Osasco;

- A Subsecretaria de Tecnologia da Informação deve determinar um Plano de Treinamento em Segurança da Informação para os funcionários e terceiros conforme a criticidade do ativo que os mesmos têm acesso;

- A Subsecretaria de Tecnologia da Informação deve informar a todos os funcionários e terceiros sobre mudanças e atualizações na Política de Segurança da Informação da Prefeitura do Município de Osasco;

PROCESSO DISCIPLINAR

- A não conformidade na aplicação da Política de Segurança da Informação da Prefeitura do Município de Osasco e violações intencionais dessa política por funcionários e terceiros será encaminhado a Procuradoria Geral do Município;

TÉRMINO DE CONTRATO, APOSENTADORIA OU TRANSFERÊNCIA

- É de responsabilidade de cada superior imediato obter o retorno ou entrega de ativos de informação que estejam com o funcionário ou terceiro em processo de rescisão contratual, aposentadoria, demissão ou transferência;

- É de responsabilidade de cada superior imediato do funcionário ou do terceiro, informar à Subsecretaria de Tecnologia da Informação o término do contrato, para fins de revogar direitos de acesso aos ativos de informação da Prefeitura do Município de Osasco, inclusive com a revogação de USer´s ID e senhas e deleção de arquivos pessoais contidos em estações de trabalho e em diretórios na rede da Prefeitura do Município de Osasco ou em outros tipos de dispositivos de armazenamento de informação;

- Em caso de término de contrato, o funcionário ou terceiro somente poderá retirar das instalações da Prefeitura do Município de Osasco informações e pertences pessoais.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Gerenciamento de Segurança em Recursos Humanos	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Gerenciamento de Segurança em Recursos Humanos	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Segurança em Recursos Humanos

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Segurança Física e do Ambiente

Norma	15	Data: 25/02/21	Email	sti.sf@osasco.sp.gov.br
Version	1.0			

PROPÓSITO

Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

ESCOPO E APLICAÇÃO

Aplicação – Instalações de processamento da informação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades - É de responsabilidade da Subsecretaria de Tecnologia da Informação a autorização de acesso de pessoas ao Data Center, a manutenção de dispositivos de segurança do Data Center, proteção física do Data Center, o descarte de equipamentos obsoletos, os registros desse descarte, a alteração de configurações de equipamentos e a autorização de uso de equipamentos fora das instalações da Prefeitura do Município de Osasco.
É de responsabilidade de cada secretaria da municipalidade a administração da infraestrutura a segurança física das estações de trabalho e outros dispositivos sob sua responsabilidade.

PERÍMETRO DE SEGURANÇA FÍSICA

- O acesso de visitantes e terceiros às instalações do Data Center deve ser acompanhado por pessoal autorizado;
- As instalações de processamento de informações devem estar em local protegido de acessos não autorizados;

- As instalações de processamento de informações devem estar conformes normas aplicáveis para proteção contra incêndio, energização, cabeamento, umidade e refrigeração;

CONTROLES DE ENTRADA FÍSICA

- Os acessos de funcionários, visitantes e terceiros às instalações de processamento de informação devem ser registrados e autorizados pela Subsecretaria de Tecnologia da Informação;

- Acesso aos locais de armazenamento de informação como fitas, discos e documentação de produção e de operações, de software básico e de suporte somente poderá ser feito por funcionários autorizados;

- Salas e escritórios com informações sensíveis nas dependências da Subsecretaria de Tecnologia da Informação devem ser trancados ao término do expediente ou quando não houver funcionários autorizados no local;

PROTEÇÃO CONTRA AMEAÇAS EXTERNAS

- Materiais combustíveis devem ser armazenados em distância segura do Data Center;

- Deve ser providenciado proteção física adequada para a sala do Data Center considerando ameaças como incêndios e a outras ameaças que possam causar danos aos recursos e ativos de informação instalados na sala do Data Center;

TRABALHO EM ÁREAS SEGURAS

- O trabalho em áreas seguras que contém informação sensível deve ser monitorado continuamente;

- Reuniões com o uso de informações sensíveis e confidenciais com terceiros não podem ocorrer em áreas públicas e não seguras da organização;

- Recursos humanos de fornecedores de serviços, executando serviços de natureza contínua, deverão ater-se ao horário normal de expediente da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco. Caso necessitem trabalhar fora do

Secretaria de Finanças – Subsecretaria de Tecnologia da Informação - Rua Narciso Sturlini, 201 – Centro – Osasco – São Paulo – CEP 06018-100. E-mail: sti.sf@osasco.sp.gov.br

expediente ou em dias em que não haja expediente deverá ser obtida autorização da Subsecretaria de Tecnologia da Informação;

- Toda área que contenha recursos computacionais e que esteja vazia deverá ser trancada e tal procedimento seja verificado por vigilância, principalmente fora do expediente;

- Áreas que contenham recursos de comunicação, como central telefônica, roteadores, etc. devem estar sempre trancadas e seu acesso deve ser permitido somente para pessoas autorizadas;

ACESSO DO PÚBLICO, ÁREAS DE ENTREGA E DE CARREGAMENTO

- Deve ter uma área intermediária para recebimento de material e equipamentos a serem usados na sala do Data Center;

SEGURANÇA DE EQUIPAMENTOS

- É vedado aos funcionários, visitantes e terceiros autorizados a alimentar-se e beber líquidos de qualquer natureza na sala do data Center ou próximos a ativos de informação sensíveis nas dependências da Subsecretaria de Tecnologia da Informação;

- Todos os locais de processamento de informações como o Data Center devem ter isolamento contra descargas elétricas estáticas;

- Os funcionários podem usar seus recursos próprios de processamento da informação como notebooks, mediante autorização da Subsecretaria de tecnologia da Informação;

- As portas dos racks de servidores sempre devem ser mantidas fechadas. Exceção permitida é no caso de pessoal autorizado estar fazendo serviço de reparação, configuração e de manutenção;

- O Data Center deve ter redundância no suprimento de energia;

- A instalação e manutenção de cabeamento de rede e comunicação devem ser feitas de acordo com as Normas Internacionais que tratam do assunto;

- Todos os equipamentos e softwares devem ser registrados junto aos seus respectivos fornecedores assim que forem instalados;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Manutenção preventiva deve ser realizada para todos os equipamentos auxiliares de informática da Prefeitura do Município de Osasco, como UPS´s, Nobreaks, sistemas de refrigeração e de proteção contra incêndio, estabilizadores, etc.

- A manutenção corretiva e preventiva dos equipamentos deve ser realizada de acordo com as especificações dos respectivos fabricantes e somente por pessoal qualificado;

- Os computadores não podem ser alterados ou modificados sem a autorização da Subsecretaria de Tecnologia da Informação;

- Uso de recursos computacionais da Prefeitura do Município de Osasco fora de suas instalações deve ser aprovado pelo superior imediato do funcionário e considerando as Normas da Subsecretaria de Tecnologia da informação;

- Antes do descarte das estações de trabalho, servidores e componentes de armazenamento de dados, a Subsecretaria de Tecnologia da Informação deve verificar se não há informação sensível armazenada e se tiver deve apagá-la;

- A Subsecretaria de Tecnologia da Informação deve manter um registro de todos os equipamentos descartados da rede da Prefeitura do Município de Osasco;

- Nenhuma informação sensível deve ser armazenada em dispositivos móveis como notebooks, pendrive e outros dispositivos;

- Toda mídia de armazenamento de informações deve ter autorização para deixar as instalações da Prefeitura do Município de Osasco;

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

STI	Segurança Física e do Ambiente	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Segurança Física e do Ambiente	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Segurança Física e do Ambiente

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Comunicações e Gestão de Operações

Norma 16 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Garantir a operação segura e correta dos recursos de processamento das informações.

ESCOPO E APLICAÇÃO

Aplicação – Gestão de operações de todos os recursos de processamento de informações.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação a manutenção da documentação dos procedimentos de operação, a manutenção dos logs de acesso e de operação, desabilitar software que não são usados no ambiente, proceder a promoção para o ambiente da rede equipamentos e dispositivos, atualizar versões de sistemas operacionais, análises de vulnerabilidades de sistemas operacionais, estabelecer procedimentos de back-off, segregar ambientes de desenvolvimento e produção, alterar prioridades de produção, desconectar da rede computadores com vírus, gerenciar serviços de terceiros, monitorar vírus e estações de trabalho, gerar cópias de segurança, gerenciar a rede da Prefeitura da Prefeitura do Município de Osasco, etc.
Assim como realizar a aceitação de sistemas aplicativos de desenvolvidos externamente a Prefeitura do Município de Osasco, aprovar a promoção de sistemas para a produção, gerenciar serviços de terceiros de desenvolvimento de sistemas.
É de responsabilidade do proprietário da informação a aprovação de postagem de informações na Intranet e Internet.
É de responsabilidade dos usuários e funcionários seguir os procedimentos de segurança no trato de mensagens de e-mail, uso de blogs e outros serviços.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

DOCUMENTAÇÃO DOS PROCEDIMENTOS DE OPERAÇÃO

- Documentação para cada aplicação, que inclui os recursos requeridos por cada aplicação, arquivos e tabelas de bancos de dados usadas, lista de requisitos de segurança, procedimentos de produção, de gerenciamento e monitoramento e tratamento de saídas, procedimentos de back-up, de reinício e recuperação em caso de falhas, devem estar documentados e com a aprovação do proprietário da informação;

- O acesso à documentação operacional da produção deve ser controlado pela Subsecretaria de Tecnologia da Informação;

- Devem ser mantidos atualizados os registros dos profissionais que mantém a operação e de suas habilidades em termos de conhecimento do processamento das aplicações para fins de necessidades de suporte técnico;

- Mudanças na produção das aplicações somente poderão ocorrer através do processo de Gerenciamento de Mudanças.

GESTÃO DA MUDANÇA

- Antes que qualquer servidor seja colocado em operação é necessário desabilitar User´s ID e senhas de terceiros, fornecedores e do pessoal que configurou o equipamento;

- Qualquer software não utilizado em ambiente de produção deve ser desabilitado ou removido do ambiente;

- A promoção de aplicações para produção somente poderá ocorrer com a autorização dos membros da Gestão de Mudança da Prefeitura do Município de Osasco;

- Qualquer mudança em sistemas operacionais ou adição ou descarte de servidores e outros dispositivos da configuração tecnológica da Prefeitura do Município de Osasco somente poderá ocorrer com a autorização da Subsecretaria de Tecnologia da Informação;

- Análises de vulnerabilidades dos sistemas operacionais devem ser realizadas periodicamente pela Subsecretaria de Tecnologia da Informação;

- A Subsecretaria de Tecnologia da Informação deve averiguar, periodicamente, a necessidade de migrar os softwares operacionais para versões mais atualizadas visando diminuir vulnerabilidades;

- Procedimentos adequados de back-off, que permitem o retorno do ambiente antes de uma mudança de sistema operacional ou de aplicação devem estar estabelecidos pela Subsecretaria de Tecnologia da Informação;

- Todos os sistemas críticos devem ter acompanhamento gerencial quando somente uma única pessoa tem o conhecimento de sua operação.

SEPARAÇÃO DOS RECURSOS DE DESENVOLVIMENTO, TESTE E DE PRODUÇÃO

- O ambiente de desenvolvimento deve estar separado do ambiente de produção, tanto em termos lógicos como físicos;

- As seguintes atividades devem estar separadas em termos de atribuição de responsabilidades: desenvolvimento de sistemas e programas de computador, operação de sistemas e manipulação de dados de sistemas em produção;

- Teste e desenvolvimento de sistemas e programação de computador devem estar separados em termos de ambientes;

- Pessoal de desenvolvimento deve estar separado do pessoal de teste de aceitação e homologação.

GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS

- Anualmente a Subsecretaria de Tecnologia da Informação pode requerer uma auditoria de terceira parte sobre os serviços terceirizados visando obter informação sobre a adequação dos controles de segurança da informação usados pelo fornecedor;

- Fornecedores de serviços de desenvolvimento que estejam trabalhando em suas próprias instalações, através de link de comunicação com a Prefeitura do Município de Osasco, deverão usar sistemas de gerenciamento de biblioteca de configuração com acesso irrestrito pela Prefeitura do Município de Osasco sobre os ativos de códigos-fonte, assim como manter os procedimentos operacionais de produção atualizados;

- Será vedado o acesso de programadores de fornecedores externos aos códigos fontes das aplicações da Prefeitura do Município de Osasco. Este acesso somente será permitido a parte do código necessária para executar o serviço demandado;

- A concessão de permissão de acesso às informações processadas para ou na Prefeitura do Município de Osasco não pode ser atribuição de pessoal do fornecedor de serviços;

- Deve ser estabelecido, nos contratos de terceirização de serviços de processamento de informação, o direito da Prefeitura do Município de Osasco auditar os controles de segurança empregados pelo fornecedor de serviços em seu ambiente de produção;

- O fornecedor de serviços de processamento de informação deve informar a Subsecretaria de Tecnologia da Informação com antecedência as mudanças que fará em seu ambiente de produção e que pode afetar o processamento das aplicações da Prefeitura do Município de Osasco;

- O fornecedor de serviços de processamento de informação deve apresentar para a Subsecretaria Tecnologia da Informação um plano de contingência e procedimentos operacionais de back-out.

PLANEJAMENTO E ACEITAÇÃO DE SISTEMAS

- A Subsecretaria de Tecnologia da Informação poderá alterar prioridades de produção caso uma aplicação não esteja conforme os requisitos de segurança ou esteja exigindo recursos excessivos e que possam estar degradando a disponibilidade e tempo de resposta de serviços e aplicações;

- A Subsecretaria de Tecnologia da Informação deverá estabelecer para cada serviço e aplicação, um nível de serviços de disponibilidade adequado para as funções fins e meio da organização;

- Os usos dos recursos de processamento de informação devem ser monitorados e registrados continuamente através de logs. O histórico de utilização deve ser comunicado periodicamente para a Subsecretaria de Tecnologia da Informação;

- Todos os recursos e ativos de informação em termos de servidores, firewall, devem ser configurados de acordo com os requisitos de segurança da informação da Prefeitura do Município de Osasco;

- Sistemas e aplicações desenvolvidas interna e externamente a Prefeitura do Município de Osasco e "hospedadas" nos computadores da Prefeitura do Município de Osasco somente serão aceitas com todos os procedimentos operacionais de produção e a respectiva documentação de sistemas atualizada;

- Toda nova tecnologia também deverá ser avaliada pela Subsecretaria de Tecnologia da Informação visando mitigar riscos de mudança para o ambiente de desenvolvimento e de produção;

- Sistemas e aplicações que possam afetar a privacidade de dados dos usuários e funcionários e terceiros da Prefeitura do Município de Osasco devem ser avaliados pela Subsecretaria de

Tecnologia da Informação o qual poderá ter contramedidas para que riscos de vazamento de informações não ocorram;

- Aplicações desenvolvidas externamente a Prefeitura do Município de Osasco e que deverão ser mantidas e atualizadas internamente deverão ser aceitas somente se empregaram os padrões de desenvolvimento da Prefeitura do Município de Osasco e serem desenvolvidas com softwares homologados pela Prefeitura do Município de Osasco.

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

- Sistemas em produção que estejam infestados por vírus devem ser desconectados da rede da Prefeitura do Município de Osasco;
- Qualquer estação de trabalho conectada à rede e que esteja com vírus deve ser imediatamente desconectada da rede pela Subsecretaria de Tecnologia da Informação;
- Somente o pessoal da Subsecretaria de Tecnologia da Informação poderá eliminar vírus das estações de trabalho;
- Os usuários não poderão realizar "download" de qualquer sistema de fora da rede da Prefeitura do Município de Osasco em computadores móveis e estações de trabalho da Prefeitura do Município de Osasco a partir da Internet e de outras redes;
- Os usuários não poderão instalar softwares em suas estações de trabalho e notebooks da Prefeitura do Município de Osasco que não sejam homologados pela Subsecretaria de Tecnologia da Informação;
- Todo software recebido de fontes externas para serem instalados na rede da Prefeitura do Município de Osasco deverá ser avaliado quanto à existência de vírus ou código malicioso pela Subsecretaria de Tecnologia da Informação;
- Todo software a ser envidado a fontes externas deve estar livres de vírus;
- A Prefeitura do Município de Osasco utiliza software antivírus em sua rede, o qual deve estar permanentemente atualizado;
- Qualquer tipo de mídia eletrônica adquirida e que for usada pela Prefeitura do Município de Osasco dever verificada quanto a existência de vírus antes de ser utilizada;
- A verificação completa de estações de trabalho e de servidores quanto à existência de vírus deve ser feita diariamente;

- Computadores próprios dos usuários da Prefeitura do Município de Osasco que sejam usados em suas instalações e conectados em sua rede devem ser verificados periodicamente quanto à atualização de antivírus. Caso o computador não tenha antivírus atualizado deverá ser proibido sua conexão na rede;

- Quando uma mídia de back-up for usada para atualização de arquivos em produção devem ser verificadas antes usando as atualizações mais recentes do software antivírus;

- Computadores portáteis da Prefeitura do Município de Osasco que sejam usados pelos funcionários por necessidade do trabalho devem ser configurados para que evitem a instalação de software a alteração de configuração pelo usuário.
  •

CÓPIAS DE SEGURANÇA

- Cópias de segurança de toda informação e software residente em servidores da Prefeitura do Município de Osasco deve ser periodicamente realizada conforme o esquema documentado da Subsecretaria de Tecnologia da Informação;

- Usuários que usem computadores móveis da Prefeitura do Município de Osasco devem ser avisados para realizarem cópias de segurança das informações pelo menos a cada semana;

- Informações sensíveis devem ser copiadas com recursos de criptografia;

- Sempre devem ser mantidas cópias back-up atualizadas off-line;

- Cópias de segurança devem estar armazenadas em locais fora da Prefeitura do Município de Osasco e armazenadas de forma adequada em termos de proteção e de ambiente.

GERENCIAMENTO DA SEGURANÇA DA REDE

- A Prefeitura do Município de Osasco deverá implementar um sistema único de gerenciamento de senhas para acesso a todas as suas aplicações críticas;

- Somente protocolos e interfaces de conexão de rede aprovados pela Subsecretaria de Tecnologia da Informação podem ser usados para conexão dos sistemas da Prefeitura do Município de Osasco com outras redes externas;

- O tráfego da Internet pelos usuários da Prefeitura do Município de Osasco deve ser monitorado;

- A rede da Prefeitura do Município de Osasco deve ter mecanismos de contingência em caso de falha;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- A Subsecretaria de Tecnologia da Informação deve administrar todos os registros de domínios de sites da Prefeitura do Município de Osasco e ser responsável por sua criação, renovação, manutenção do registro, encaminhamentos a entidade gestora de domínios, para tanto os interessados devem solicitar formalmente a sua criação e também a sua desabilitação;

- A Prefeitura do Município de Osasco deve ter sistemas de detecção de intrusão pela Internet;

- Todos os computadores pessoais que se conectam na rede da Prefeitura do Município de Osasco devem ter seu próprio sistema de firewall;

- Todos os firewalls conectados à internet devem ter conexão alternativa de acesso de backup;

- Uma política de firewall, definindo quais serviços e conexões são permitidos e negados, deve ser documentada, revisada e aprovada pelo menos duas vezes por ano pela Subsecretaria de Tecnologia da Informação. Sempre quando houver mudanças de configuração, e incidentes de segurança da informação essa política deve ser imediatamente revista;

- Testes da política de firewall devem ser realizados periodicamente pela Subsecretaria de Tecnologia da Informação;

- Acesso remoto ao firewall deve ser feito em sessões criptografadas e com restrições de acesso determinados pela Subsecretaria de Tecnologia da Informação;

- A rede da Prefeitura do Município de Osasco deve ser segmentada de forma que os acesso a serviços públicos de internet não permitam acesso à rede interna;

- Todos os firewalls usados pela Prefeitura do Município de Osasco devem ser processados em servidores dedicados;

- Mudanças nas configurações dos firewalls somente serão permitidas com a aprovação da Subsecretaria de Tecnologia da Informação;

- A rede interna deve ser configurada de forma que possa detectar e prevenir que computadores não autorizados possam ser conectados a ela;

- Todas as conexões pela Internet a partir da rede da Prefeitura do Município de Osasco devem ser roteadas para o firewall;

- Redes sem fio na Prefeitura do Município de Osasco devem usar criptografia;

- Pontos de acesso a rede sem fio a partir de servidores de produção devem ser desabilitados.

SEGURANÇA DE SERVIÇOS DE REDE

- Contratos com serviços de redes de provedores de serviços devem estabelecer requisitos de segurança da Prefeitura do Município de Osasco.

MANUSEIO DE MÍDIAS

- Deve ser vedado aos funcionários da Prefeitura do Município de Osasco o armazenamento de informações sensíveis em mídias removíveis;
- Informações sensíveis, tanto em papel como armazenada em mídia, quando não mais usadas devem ser destruídas.

SEGURANÇA DE DOCUMENTAÇÃO DE SISTEMAS

- Envio de documentação dos sistemas da Prefeitura do Município de Osasco para terceiros deve ser aprovado pela Subsecretaria de Tecnologia da Informação.

ACORDOS DE TROCAS

- A cessão de software aplicativo desenvolvido pela Prefeitura do Município de Osasco para terceiros deve ser autorizada pelo Subsecretaria de Tecnologia da Informação;
- Acordos de troca de informações entre a Prefeitura do Município de Osasco e outras organizações devem ser feitas com base em um acordo formal e com a aprovação da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco.

MÍDIAS EM TRÂNSITO

- Toda informação sensível armazenada em mídias removíveis e que estarão em trânsito deve ser criptografada;

MENSAGENS ELETRÔNICAS

- Informação sensível enviada por e-mails deve ser criptografada;
- Contas de e-mail da Prefeitura do Município de Osasco somente podem ser usadas para fins das atividades inerentes à função desempenhada pelo funcionário;
- Mensagens eletrônicas ofensivas não podem ser feitas por contas de e-mail da Prefeitura do Município de Osasco;

- Monitoramento de mensagens de e-mail somente poderá ocorrer com a autorização da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco, quando houver suspeitas de atividades criminosas ou outras que causem danos legais e de imagem para a Prefeitura do Município de Osasco;

- A Subsecretaria de Tecnologia da Informação deve implementar e manter dispositivos AntiSpam e filtros para o envio e recebimento de e-mails;

- A criação de blogs, wikis e contas em recursos de redes sociais que serão usadas para fins dos serviços da Prefeitura do Município de Osasco devem ser aprovadas pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco;

- Não será permitido criar blogs, wikis de uso pessoal usando os ativos de informação da Prefeitura do Município de Osasco;

- Os funcionários não podem abrir arquivos anexados a mensagens de e-mail de fontes desconhecidas.

SISTEMAS DE INFORMAÇÃO

- Informação sensível somente poderá ser enviada via e-mail com autorização do proprietário da informação;

- O proprietário da informação deve autorizar toda postagem de informação, sob sua responsabilidade, na Intranet da Prefeitura do Município de Osasco;

- Todo conteúdo postado na Intranet da Prefeitura do Município de Osasco é de sua propriedade intelectual;
-
- É de responsabilidade da Subsecretaria de Tecnologia da Informação determinar os padrões de páginas da Intranet e que deverão ser usadas pelas demais áreas da Prefeitura do Município de Osasco;

- Toda postagem de informação no website da Prefeitura do Município de Osasco deve ser aprovada pelo proprietário da informação e deve seguir a política de segurança da informação da Prefeitura do Município de Osasco, não revelando informações sensíveis e nem com mensagens ofensivas ou que violem algum dispositivo legal;

- Periodicamente o proprietário da informação deve revisar o conteúdo da Internet sob a sua responsabilidade.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

MONITORAMENTO

- Todo sistema que manuseie informações sensíveis deve ter logs de adição, modificação e deleção dessas informações, assim como registros de tempo de sessão, datas de logon por User ID;
- Sistemas com informações sensíveis devem ter logs de tentativas de acesso por pessoas não autorizadas;
- Manter logs de criação e modificação de privilégios de acesso;
- Manter logs de operação dos sistemas;
- Estabelecer procedimentos específicos para armazenar as informações sobre os logs de uso e operação dos sistemas;
- Os registros de logs que indiquem questões de segurança da informação devem ser analisados periodicamente pela Subsecretaria de Tecnologia da Informação;
- O monitoramento de computadores usados pelos usuários e funcionários da Prefeitura do Município de Osasco somente poderá ser realizado com a aprovação da Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco e no caso de aprovação os funcionários deverão ser notificados apropriadamente.

PROTEÇÃO DE LOGS

- Somente pessoas autorizadas pela Subsecretaria de Tecnologia da Informação podem ter acesso aos registros de logs;
- Os registros de logs devem ser protegidos contra acesso indevido;
- Todo os logs de operação dos servidores do Data Center devem ser registrados;
- Periodicamente os registros de logs de operação devem ser revisados pela Subsecretaria de Tecnologia da Informação.

LOG DE PROBLEMAS

- Um processo de gerenciamento de incidentes relativos a problemas em produção deve ser criado de forma que as informações sobre problemas possam ser tratadas de forma adequada.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

SINCRONIZAÇÃO DE RELÓGIOS

- Todos os servidores ou computadores conectados a redes internas da Prefeitura do Município de Osasco devem ter os seus relógios sincronizados.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

NENHUMAPROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Comunicações e Gestão de Operações	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Comunicações e Gestão de Operações	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			Gerenciamento das Operações e Comunicações

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Controle de Acessos

Norma	17	Data: 25/;02/21	Email	sti.sf@osasco.sp.gov.br
Version	1.0			

PROPÓSITO

Controlar acesso à informação.

ESCOPO E APLICAÇÃO

Aplicação – Acesso à informação, recursos de processamento das informações e processos de negócios devem ser controlados com base em requisitos de segurança e do negócio.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – É de responsabilidade da Subsecretaria de Tecnologia da Informação o controle de acesso aos recursos e sistemas, adquirir ou desenvolver sistemas de controle de acesso e aprovar privilégios.

REQUISITOS DO NEGÓCIO PARA CONTROLE DE ACESSO

- Funcionários da Prefeitura do Município de Osasco e terceiros não podem usar sistemas da Prefeitura do Município de Osasco para atividades de "hacking" como:
  (1) obter acesso não autorizado para qualquer sistema de informação;
  (2) criar danos, alterar ou corromper as operações e outros sistemas de informação;
  (3) capturar e obter Senhas, chaves criptografadas ou outro mecanismo que pode permitir acesso não autorizado;

- Todo software instalado na Prefeitura do Município de Osasco dever ser regulado por um sistema central de controle de acesso;

- Pequenos sistemas que tratam de informações sensíveis devem ter um sistema de controle de acesso;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Funcionários da Prefeitura do Município de Osasco não podem, sem autorização do proprietário da informação, mover informação em bancos de dados de um nível de classificação maior para menor;
- A Subsecretaria de Tecnologia da Informação deve inibir o acesso aos usuários quando o sistema de controle de acesso estiver com mau funcionamento;
- Todos os registros de privilégios de acesso devem ser armazenados em um banco de dados centralizado;
- Todo User ID deve estar refletido no banco de dados centralizado com os registros de acesso;
- Programadores e pessoal técnico devem estar cientes de não introduzir códigos que possam fazer "by-pass" nos sistemas de controle de acesso;
- Todas as solicitações de informações da Prefeitura do Município de Osasco feitas por entidades externas, em forma de pesquisas, entrevistas ou outros meios devem ser respondidas pelas diversas pastas responsáveis pela informação de acordo com a Lei Federal nº 12.527/2011 e o Decreto Municipal nº 11.440/2017;
- A programação de novos protocolos de segurança em sistemas deve ser realizada a partir de requisitos determinados pela Subsecretaria de Tecnologia da Informação;
- Gerenciamento de Acesso do Usuário;
- User´s ID não podem ser estabelecidos de forma que haja correlação óbvia com o usuário envolvido;
- Todos os User´s ID devem seguir um padrão de construção estabelecido pela Subsecretaria de Tecnologia da Informação;
- Cada usuário deve ter um único User ID e uma Senha correspondente para acessar os sistemas e a rede da Prefeitura do Município de Osasco;
- Todos os privilégios de acesso à rede da Prefeitura do Município de Osasco devem ser revogados quando não houver mais relação contratual ou de serviço entre o funcionário ou terceiro com a Prefeitura do Município de Osasco;
- Não deve ser permitido a criação de User´s ID para grupos ou coletivos;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Cada User ID deve identificar somente um funcionário e não pode ser criado User ID com base no título do cargo que ocupa o usuário;
- User´s ID não podem ser novamente atribuídos a outras pessoas depois que o usuário terminou sua relação de trabalho com a Prefeitura do Município de Osasco;
- Os usuários da rede da Prefeitura do Município de Osasco devem usar somente um único User ID para diferentes sistemas, com exceção de acesso a computadores conectados à Internet e à Intranet;
- Solicitações de mais privilégios de acesso devem ser encaminhadas pelo superior imediato do usuário, sendo que essa solicitação deve ser também aprovada pela Subsecretaria de Tecnologia da Informação; User´s ID com mais de 120 dias inativo deve ser desativado;
- Arquivos pessoais mantidos em diretórios na rede da Prefeitura do Município de Osasco de usuários que já terminaram sua relação de trabalho devem ser deletados imediatamente após o seu desligamento;
- User´s ID que tenham acesso à rede da Prefeitura do Município de Osasco através da Internet devem expirar a cada 6 meses;
- Usuários da rede da Prefeitura do Município de Osasco, funcionários notadamente, não podem usar seus User ID e senhas em web sites públicos;
- O estabelecimento dos privilégios de acesso deve ser feito considerando a necessidade específica de acesso do funcionário ou terceiro em função do seu trabalho e atividades;
- Privilégios especiais podem ser atribuídos para servidores da Subsecretaria de Tecnologia da Informação;
- Não deve ser permitido aos usuários finais acesso a sistemas operacionais;
- Somente pessoal autorizado pela Subsecretaria de Tecnologia da Informação pode atualizar sistemas em produção;
- Devem ser mantidos registros de acesso de cada usuário da rede da Prefeitura do Município de Osasco;
- Senhas defaults emitidas pelo Administrador da Rede deve expirar forçando o usuário definir uma nova senha pessoal após o próximo acesso à rede;
- Quando houver intrusão no sistema, o Administrador da Rede inabilitará todas as senhas fazendo com que os usuários finais tenham que criar nova senha;
- Senha inicial para usuários remotos não devem ser transmitidas através da rede da Prefeitura do Município de Osasco e sim por outros meios;

- Usuários finais poderão modificar a qualquer momento sua Senha;
- O acesso à rede da Prefeitura do Município de Osasco deverá ser bloqueado após a terceira tentativa de acesso com Senha não correspondente ao User ID;
- Não é permitida ao usuário final a delegação de criação ou mudança de Senha;
- Todo usuário deve ter uma identificação positiva para acessar a rede da Prefeitura do Município de Osasco;
- Os direitos de acesso do usuário devem ser avaliados trimestralmente pelo superior imediato e compartilhados com a Subsecretaria de Tecnologia da Informação.
- A Subsecretaria de Tecnologia da Informação deve realizar auditorias periódicas sobre os direitos de privilégio.

RESPONSABILIDADES DOS USUÁRIOS

- Usuários não podem empregar uma estrutura de Senha que seja fácil de ser identificada ou facilmente adivinhada por terceiros, portanto não deve criar Senhas com nomes ou datas de aniversários, derivativos de User ID, palavras de dicionários, detalhes pessoais ou algo similar;
- Usuários não podem usar Senhas cíclicas, ou seja, com pequenas mudanças em relação a Senhas prévias;
- Usuários não podem registrar suas Senhas em arquivos de computadores pessoais ou em discos rígidos de estações de trabalho ou em outra forma que possa ser lida por outra pessoa;
- Os usuários devem mudar imediatamente sua Senha se suspeitar que ela foi violada;
- Senhas não podem ser compartilhadas e nem reveladas para outros funcionários da Prefeitura do Município de Osasco ou para funcionários de terceiros no ambiente da Prefeitura do Município de Osasco;
- Qualquer usuário que tenha compartilhado sua senha com outros funcionários ou terceiros deve ter seus privilégios de acesso cancelados;
- Usuários são responsáveis por qualquer atividade realizada com seu User ID;
- Os usuários não podem explorar vulnerabilidades ou deficiências em sistemas de informação para criar danos à informação armazenada e para obter recursos além do que seu privilégio permite;

- Usuários não podem usar contas de e-mail de outros usuários, tanto para receber como enviar mensagens;

- Se a estação de trabalho ou computador que estiver sendo usado em sistemas com informações sensíveis estiver conectada à rede e não estiver sendo usado, a sessão deve ser encerrada ou o computador deve ser bloqueado pelo usuário.

CONTROLE DE ACESSO À REDE

- A Prefeitura do Município de Osasco, por meio da Subsecretaria de Tecnologia da Informação, se reserva o direito de descontinuar, negar, bloquear serviços de rede a qualquer momento;

- Se computadores são deixados conectados à rede em horários fora do expediente os mesmos devem ser protegidos por meio de um sistema de controle de acesso aprovado pela Subsecretaria de Tecnologia da Informação;
-
- Computadores pessoais somente poderão ser conectados à rede interna da Prefeitura do Município de Osasco mediante autorização da Subsecretaria de Tecnologia da Informação;

- Não será permitido o acesso a websites que contenham orientação de homofobia, pornográficos, pedofilia e equivalentes;

- Usuários não podem baixar arquivos de vídeos, de áudio, jogos e outros com grandes volumes de informação sem a autorização da Subsecretaria de Tecnologia da Informação, a qual permitirá somente se esses arquivos forem para uso a execução das atividades do funcionário;

- A instalação de pontos de acesso à rede sem fio somente poderá ser realizada por pessoal autorizado pela Subsecretaria de Tecnologia da Informação;

- User´s ID em branco ou Senhas nulas não devem ganhar acesso à rede da Prefeitura do Município de Osasco;

- Todos os computadores remotos e externos que dialogam com computadores da rede da Prefeitura do Município de Osasco devem ter mecanismo específico de controle de acesso;

- Todos os usuários devem ser autenticados através de um User ID e uma Senha secreta;

- Um diretório comum de serviços aprovado pela Subsecretaria de Tecnologia da Informação deve ser usado para o processo de autenticação dos usuários de computadores conectados à rede da Prefeitura do Município de Osasco;
-

- Administração remota de computadores deve ser realizada através de links criptografados;
- Acesso a todas as portas de diagnóstico e manutenção deve ser controlado de forma segura;
- A rede da Prefeitura do Município de Osasco deve ser segmentada em zonas de segurança, em termos do que pode ser acessível para o público, paras as funções do negócio que não tratam de informações sensíveis e para as funções que tratam com informações sensíveis;
- Acesso à Internet ou redes externas a partir de computadores de visitantes pode ser feito através de uma rede independente não conectada à rede da Prefeitura do Município de Osasco;
- Todos os servidores de web acessíveis através da Internet devem ser protegidos por firewall;
- Todos os dispositivos da rede interna como firewall, roteadores e servidores de controle de acesso devem ter sua senha única;
- Conexão de computadores da rede da Prefeitura do Município de Osasco à rede de terceiros somente é permitida com autorização da Subsecretaria de Tecnologia da Informação;
- As estações de trabalho da Prefeitura do Município de Osasco não devem ter modem para conexões dial-up.

CONTROLE DE ACESSO AO SISTEMA OPERACIONAL

- O acesso ao sistema operacional deve ser controlado através de um procedimento de logon, sendo que três tentativas malsucedidas de acesso, o User ID do usuário envolvido deve ser desabilitado;
- No acesso à rede através de procedimento de logon, se a sequência de logon estiver incorreta, limitar o feedback para o usuário, informando que o procedimento está incorreto, não informando se é o User Id ou a senha que está incorreta;
- Os desenvolvedores da Subsecretaria de Tecnologia da Informação devem usar os requisitos de segurança estabelecidos pelos sistemas operacionais ou por utilitários que reforcem esses requisitos, sendo proibido o desenvolvimento de outros mecanismos para controlar o acesso;
- Não é permitido o uso de Senha nula;
- Deve ser mantido o histórico de Senhas dos usuários, pelo menos das últimas 30 Senhas;
- Senhas geradas por sistemas devem ter mecanismos que permitam a mudança frequente de sua fonte de geração;

- Todo software e arquivo que contém fórmulas e algoritmos usados para gerar Senha devem ser protegidos contra acesso não autorizado de forma rigorosa;

- As Senhas devem ser criptografadas quando transmitidos pela Internet e quando mantidos armazenados por um período significativo;

- Sempre quando um sistema estiver compromissado por acesso não autorizado, a Subsecretaria de Tecnologia da Informação deve imediatamente carregar a versão correta do sistema operacional e dos softwares de segurança instalados, sendo que as mudanças recentes em privilégios dos usuários devem ser revistas;

- A instalação de software na rede da Prefeitura do Município de Osasco para avaliar vulnerabilidades em segurança da informação deve ser avaliada quanto aos possíveis danos que o software pode causar aos mecanismos já instalados de segurança da informação. Remover o software do sistema quando não estiver em uso;

- O acesso a ferramentas de diagnóstico de hardware e software deve estar restrito a pessoal autorizado pela Subsecretaria de Tecnologia da Informação;

- O acesso e uso de utilitários para o gerenciamento da rede da Prefeitura do Município de Osasco e para a restauração de arquivos e resolução de problemas é de acesso exclusivo de pessoas autorizadas pela Subsecretaria de Tecnologia da Informação;

- O acesso aos sistemas deve ser restringido considerando dias da semana e horários, em função do tipo de privilégio concedido aos usuários.

CONTROLE DE ACESSO À APLICAÇÃO E INFORMAÇÃO

- Programadores não podem embutir em seus programas, User´s ID e Senhas secretas que tenham privilégios especiais, e que não estejam claramente documentados na documentação do sistema;

- Logs de sistemas ou rotinas de auditoria somente podem ser acessados por pessoal autorizado pela Subsecretaria de Tecnologia da Informação;

- Não é permitido o acesso às aplicações em produção pelo pessoal de sistemas;

- Toda a informação cadastral sobre usuários e que contenham dados de identificação pessoal somente podem ser acessadas por funcionários com privilégios especiais e tal acesso deve ser continuamente monitorado;

- Sem a autorização do proprietário da informação, o administrador somente poderá fornecer privilégios de acesso a serviços de e-mail e de uso de planilhas eletrônicas e processadores de texto para qualquer usuário;

- Sistemas que processam aplicações críticas para a Prefeitura do Município de Osasco devem ser processados em servidores dedicados.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	**Controle de Acessos**	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	**Controle de Acessos**	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Norma 18 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Garantir que a segurança é parte integrante de sistemas de informação.

ESCOPO E APLICAÇÃO

Aplicação – Sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócios, produtos de prateleira e aplicações desenvolvidas pelo usuário.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – A Subsecretaria de Tecnologia da Informação é responsável por implantar controles de segurança da informação no processo de desenvolvimento de sistemas, por estabelecer os padrões de criptografia, rever sistemas de informação para assegurar que os requisitos de segurança foram implantados, pela gestão de vulnerabilidades técnicas, pela promoção de sistemas para produção, pelo controle de versões de software em produção, por instalar e configurar servidores, por instalar e atualizar sistemas operacionais e outros aplicativos de fornecedores.

REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

- Antes que um sistema de informação seja desenvolvido ou adquirido, a Subsecretaria de Tecnologia da Informação e os usuários solicitantes devem acordar quanto aos requisitos de segurança do sistema;

- Todo o sistema em desenvolvimento ou adquirido deve ser revisto pela Subsecretaria de Tecnologia da Informação para garantir que os requisitos de segurança da informação,

aplicáveis, estejam sendo aplicados no sistema, considerando todo o ciclo de vida do sistema, do desenvolvimento à produção e manutenção;

- Todo sistema considerado crítico pela Prefeitura do Município de Osasco ou que trate de informações sensíveis deve ter especificações formais documentadas de acordo com a metodologia de desenvolvimento de sistemas adotada pela Prefeitura do Município de Osasco;

- A Subsecretaria de Tecnologia da Informação deve especificar os princípios de programação segura, a qual deverá ser seguida pelos programadores e desenvolvedores e fornecedores.

PROCESSAMENTO CORRETO NAS APLICAÇÕES

- Todo sistema deve ser projetado considerando requisitos de identificação de cada uma das transações, validação dos dados de entrada com tratamento de entradas não válidas e identificação da origem da transação;

- O sistema de gerenciamento de privilégios deve ser estabelecido de forma a não permitir que usuários modifiquem dados de sistemas em produção;

- Mensagens de erro sempre devem ser emitidas para o usuário quando há falhas no software ou o mesmo não gera os resultados esperados;

- Se um sistema está indisponível deve ser comunicado ao usuário antes dele fazer o logon no sistema;

- Todos os erros do sistema em termos de segurança da informação devem ser comunicados à Subsecretaria de Tecnologia da Informação imediatamente.

CONTROLES CRIPTOGRÁFICOS

- A Subsecretaria de Tecnologia da Informação deve estabelecer o padrão de controles criptográficos da Prefeitura do Município de Osasco, os quais deverão ser comunicados aos usuários;

- Somente podem ter acesso a chaves de criptografia pessoas autorizadas pela Subsecretaria de Tecnologia da Informação;

- Chaves de criptografia devem expirar periodicamente.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

SEGURANÇA DOS ARQUIVOS DE SISTEMAS

- Todo software open source antes de ser usado pela Prefeitura do Município de Osasco deve ter suas vulnerabilidades de segurança avaliadas e documentadas;

- Softwares P2P como Morpheus, Limewire, MojoNation, iMesh, and KaZaA e outros equivalentes, que permitem o compartilhamento de arquivos e o "download" de vídeo, músicas, etc. devem ser evitados no âmbito da Prefeitura do Município de Osasco, sendo que mudanças no firewall ou em dispositivos de proteção (anti-vírus) não podem ser configurados para aceitar o acesso essas redes;

- Todo código fonte recebido ou desenvolvido pela Prefeitura do Município de Osasco deve ser armazenado em um sistema de gerenciamento de código fonte com acesso autorizado e aprovado pela Subsecretaria de Tecnologia da Informação;

- Acesso de pessoal de suporte técnico e de desenvolvimento a sistemas em produção somente podem ser autorizados para a resolução de incidentes, sendo que este acesso deve ser monitorado.

SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E SUPORTE

- Antes de se promover um sistema para a produção todos os requisitos de segurança alocados ao sistema devem ser testados;

- Sistemas que consomem recursos de rede, de processamento e de memória devem ser avaliados visando sua otimização;

- Todo o desenvolvimento de software na Prefeitura do Município de Osasco deve obedecer aos padrões metodológicos e de desenvolvimento estabelecidos;

- Somente poderão ser promovidos para a produção sistemas com suas funcionalidades documentadas conforme os padrões estabelecidos pela Subsecretaria de Tecnologia da Informação;

- A mudança da configuração em produção (hardware, sistemas aplicativos, software e outros dispositivos) deve ser autorizada conforme procedimento, visando avaliar o risco da mudança na configuração e aprovada pela Subsecretaria de Tecnologia da Informação;

- Software que possam comprometer a segurança da informação deve ser desabilitado;

- As mudanças na configuração devem ser documentadas;

- Somente funcionários autorizados pela Subsecretaria de Tecnologia da Informação podem instalar e atualizar sistemas operacionais e outros softwares no ambiente de produção da Prefeitura do Município de Osasco;

- Na aquisição de softwares de terceiros a Prefeitura do Município de Osasco deve obter, formalmente, uma declaração de que o software não contém funções não documentadas e que não contém mecanismos que possam comprometer a segurança da rede da Prefeitura do Município de Osasco;

- Todo contrato de desenvolvimento de sistemas por parte de terceiros deve prever de forma clara os direitos de propriedade, arranjos de licença, medidas de segurança, processos de teste e direitos da Prefeitura do Município de Osasco auditar os serviços.

GESTÃO DE VULNERABILIDADES TÉCNICAS

- Todos os sistemas da Prefeitura do Município de Osasco com acesso à Internet devem ser submetidos, periodicamente, a testes de vulnerabilidade;

- A Subsecretaria de Tecnologia da Informação deve manter um inventário das versões dos softwares utilizados no ambiente de produção;

- Periodicamente deverão ser feitos testes de vulnerabilidades na rede da Prefeitura do Município de Osasco através de profissionais ou empresas especializadas.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Gestão de Incidentes de Segurança da Informação

Norma 19 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

ESCOPO E APLICAÇÃO

Aplicação – Convém que todos os funcionários, fornecedores e terceiros estejam conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança de ativos da organização.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – A Subsecretaria de Tecnologia da Informação deve conduzir o gerenciamento de incidentes de segurança da informação, bem como estabelecer equipes de emergência em respostas a incidentes críticos de segurança da informação.

NOTIFICAÇÃO DE FRAGILIDADES E EVENTOS DE SEGURANÇA DA INFORMAÇÃO

- Eventos de perda de informações sensíveis ou acesso não autorizado a esse tipo de informação devem ser comunicados imediatamente para a Subsecretaria de Tecnologia da Informação e para o proprietário da informação;
- Vulnerabilidades de segurança da informação em sistemas de informação devem ser de conhecimento somente de pessoas autorizadas;
- Declaração pública de vulnerabilidades de segurança de informação em sistemas deve ser feita com poucos detalhes;

- Funcionários ou terceiros com relação contratual com a Prefeitura do Município de Osasco não podem abrir informações sobre prejuízos causados a pessoas, sistemas e a organização em face de um incidente de segurança da informação;

- Todos os erros significantes de sistemas em produção devem ser comunicados imediatamente ao pessoal de suporte ao usuário e a Subsecretaria de Tecnologia da Informação;

- Os funcionários devem comunicar ao seu superior imediato qualquer dano ou perda que ocorrer em computadores, software e informação sob a sua responsabilidade, em trabalho remoto ou no transporte de mídias;

- Todos os incidentes de segurança da informação devem ser comunicados imediatamente à Subsecretaria de Tecnologia da Informação por funcionários, fornecedores e terceiros;

- A identificação de funcionários que comunicarem violações da política de segurança da informação ou incidentes de segurança da informação deve ser mantida em sigilo;

- Se um incidente de segurança da informação causa exposição de informações de terceiras partes, as mesmas devem ser comunicadas imediatamente, após a aprovação pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco;

- Todos os eventos de segurança da informação devem ser investigados quanto a sua causa pela Subsecretaria de Tecnologia da Informação de forma que contramedidas necessárias sejam implantadas para minimizar ou eliminar a recorrência do incidente;

- Os funcionários, fornecedores e terceiros que descobrirem vulnerabilidades em sistemas de informação ou que forem comunicar algum incidente de segurança da informação o devem fazer somente para a Subsecretaria de Tecnologia da Informação;

- A descoberta de vulnerabilidades em hardware e software de fornecedores deve ser comunicada, de forma sigilosa e imediatamente ao mesmo;

- A introdução de vírus na rede da Prefeitura do Município de Osasco, descoberta pelos usuários, deve ser notificada imediatamente a Subsecretaria de Tecnologia da Informação e para o pessoal de suporte ao usuário visando evitar a infestação.

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E MELHORIAS

- Somente pessoas autorizadas pela Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco poderão ser porta-vozes no caso de comunicação de evento de segurança da informação para imprensa ou outras partes;

- A Subsecretaria de Tecnologia da Informação deve preparar e testar, periodicamente, planos de emergência no caso da ocorrência de eventos de segurança da informação que causem interrupções e degradação em serviços;
- A Subsecretaria de Tecnologia da Informação deve manter uma equipe para agir em caso de emergência de interrupções e degradações de serviços;
- A Subsecretaria de Tecnologia da Informação deve estabelecer um mecanismo no qual os funcionários, fornecedores e terceiros possam comunicar incidentes de segurança da informação;
- A resolução de problemas relativos a incidentes de segurança da informação deve ser realizada com a participação da Subsecretaria de Tecnologia da Informação, usuário e do pessoal designado para a equipe de resolução de emergências;
- Semestralmente, a Subsecretaria de Tecnologia da Informação deve elaborar relatórios com indicadores sobre incidentes e violações de segurança da informação, resultados desses incidentes, causas dos incidentes e violações e contramedidas adotadas e implementadas e contramedidas a implementar;
- Informações sobre incidentes e violações devem ser armazenadas em local seguro com as evidências necessárias da violação ou do incidente de forma que possa ser usado, quando for o caso, para ações disciplinares e/ou legais;
- Investigações internas sobre violações de segurança da informação feita por funcionários, fornecedores e terceiros devem ser conduzidas de forma sigilosa pela Subsecretaria de Tecnologia da Informação, juntamente com a Procuradoria Geral do Município;
- Não pode haver conflito de interesse entre o pessoal que está realizando a investigação e as pessoas que estão sendo investigadas.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Criado por	Título	Data	Assinatura
STI	Gestão de Incidentes de Segurança da Informação	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Gestão de Incidentes de Segurança da Informação	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Gestão da Continuidade do Negócio

Norma 20 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.

ESCOPO E APLICAÇÃO

Aplicação – Convém que o processo de gestão de continuidade do negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação a um nível aceitável através da combinação de ações de prevenção e recuperação.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – A Subsecretaria de Tecnologia da Informação é responsável por estabelecer e manter um processo de continuidade dos serviços de TI, coordenar a elaboração de planos de contingência, avaliar os níveis de criticidade de sistemas, coordenar a elaboração de planos de recuperação de desastres, definir esquema lógico de prioridade de recuperação de informações e definir níveis de suporte no caso de interrupções críticas de serviços, estruturar equipe para o gerenciamento de crises e aprova a divulgação de planos de continuidade e contingência para terceiras partes.

ASPECTOS DA GESTÃO DA CONTINUIDADE DO NEGÓCIO RELATIVOS À SEGURANÇA DA INFORMAÇÃO

- Deve ser estabelecido e mantido um processo para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da Prefeitura do Município de Osasco;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Todos os serviços de tecnologia da informação providos pela Subsecretaria Tecnologia da Informação devem ter planos de contingência atualizados, os quais devem ser acessíveis para as pessoas que possuem responsabilidades no tocante a restauração e recuperação de serviços de tecnologia da informação;

- Os planos de contingência devem ser testados periodicamente e especificar além de ambientes de contingência, as instalações e recursos requeridos para que os funcionários da Prefeitura do Município de Osasco possam desempenhar suas funções no caso de interrupções de serviços;

- Hardware e software para processar sistemas críticos devem ser adquiridos de fornecedores confiáveis tanto em termos de confiabilidade dos componentes como da qualidade dos serviços de manutenção;

- Computadores que já sofreram muitas reconfigurações de componentes não podem ser usados para sistemas críticos da Prefeitura do Município de Osasco;

- A Subsecretaria de Tecnologia da Informação, juntamente com os proprietários da informação devem avaliar, pelo menos anualmente, o nível de criticidade dos sistemas de informação processados pela Prefeitura do Município de Osasco visando à manutenção de sua classificação ou sua reclassificação;

- Os sistemas da Prefeitura do Município de Osasco deverão ser classificados em cinco níveis de criticidade: altamente crítico, crítico, prioritário, requerido e sem prioridade.

- A Subsecretaria de Tecnologia da Informação deverá realizar, anualmente, uma Análise de Impacto no Negócio, especificando, pelo menos: o tempo que a Prefeitura do Município de Osasco pode ficar sem serviços de TI e sistemas críticos, o tempo necessário para acionar os mecanismos de contingência e a configuração mínima necessária para ambientes de contingência;

- A Subsecretaria de Tecnologia da Informação deve estabelecer um esquema lógico para segmentar os recursos de informação conforme a prioridade de recuperação;

- A Subsecretaria de Tecnologia da Informação deve estabelecer uma equipe para o gerenciamento de crises;

- A Subsecretaria de Tecnologia da Informação deve preparar e manter um Plano de Recuperação de Desastres, de forma a tornar disponíveis os principais recursos de processamento e comunicação em caso de interrupção crítica de serviços;

- A divulgação dos Planos de Continuidade para terceiras partes somente poderá ocorrer com a aprovação formal da Subsecretaria de Tecnologia de Informação da Prefeitura do Município de Osasco;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Anualmente a Subsecretaria de Tecnologia da Informação da Prefeitura do Município de Osasco, deve definir níveis de suporte no caso de interrupções críticas de serviços.

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Gestão da Continuidade do Negócio	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Gestão da Continuidade do Negócio	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

Normas de Segurança da Informação

Conformidade

Norma 21 Data: 25/02/21 Email sti.sf@osasco.sp.gov.br

Version 1.0

PROPÓSITO

Evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

ESCOPO E APLICAÇÃO

Aplicação – Convêm os projetos, operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários.

PAPÉIS E RESPONSABILIDADES

Responsabilidades – A Subsecretaria de Tecnologia da Informação deve considerar requisitos legais internos e externos para o desenvolvimento de sistemas, usar software licenciado para o desenvolvimento de sistemas, identificar o copyright nos documentos de sistemas, os Diretores e Gerentes da Prefeitura do Município de Osasco devem identificar copyright em documentos, somente usar software licenciado em estações de trabalho e computadores móveis, proteger os registros organizacionais e pessoais, deve realizar avaliações de conformidade com a política e requisitos legais internos e externos, avaliar riscos de sistemas da Prefeitura do Município de Osasco, manter ferramentas de testes de intrusão protegidas, deve comunicar aos funcionários da Prefeitura do Município de Osasco sobre as implicações da não utilização de recursos de processamento da informação autorizados.

CONFORMIDADE COM REQUISITOS LEGAIS

- Todo o projeto de um novo sistema deve estar conforme, quando for o caso, com requisitos legais internos e externos;

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

- Quando não desenvolvido internamente, todo software usado para o desenvolvimento e a operação/produção de sistemas deve ser licenciado, e a opção de se utilizar shareware somente com aprovação da Subsecretaria de Tecnologia da Informação;

- Toda documentação de sistemas e sites da Prefeitura do Município de Osasco devem ter identificação do "copyright";

- Todo software usado em estações de trabalho e computadores móveis da Prefeitura do Município de Osasco devem ser licenciados, excluindo-se software livre;

- A assinatura de Termo de Confidencialidade a partir de terceira parte por parte de funcionários da Prefeitura do Município de Osasco somente poderá ser feita com a aprovação formal da Secretaria da Procuradoria Geral do Município;

- Todos os registros organizacionais, importantes para a Prefeitura do Município de Osasco, devem ser protegidos contra perda, destruição e falsificação, de acordo com requisitos regulamentares, estatutários, contratuais do negócio;

- Todos os registros pessoais de funcionários da Prefeitura do Município de Osasco ou de prestadores de serviços devem ser protegidos contra acesso indevido, perda, falsificação, de acordo com requisitos regulamentares, estatutários, contratuais do negócio;

- A Subsecretaria de Tecnologia da Informação deve dar ciência a todos os usuários da rede da Prefeitura do Município de Osasco sobre as implicações de usos não autorizados de recursos de processamento da informação, sobre os mecanismos de monitoramento sobre a rede e sobre as penalidades correspondentes;

- Os controles de criptografia devem estar conforme com a regulamentações internas e externas;

- A Subsecretaria de Tecnologia da Informação deve preparar e executar um plano, anualmente, para a verificação da conformidade com a política de segurança da informação, visando identificar não conformidades e estabelecer planos de ação para a melhoria da política, para tanto poderá contar com auxílio de terceira parte para realizar as verificações e auditorias;

- A Subsecretaria de Tecnologia da Informação deve realizar, a cada dois anos, com auxílio externo ou não, uma avaliação geral dos riscos de segurança da informação;

- Ferramentas usadas para testes de intrusão e de auditoria de sistemas de informação e da segurança da informação devem ser protegidas para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

Prefeitura Municipal de Osasco
Secretaria de Finanças
Subsecretaria de Tecnologia da Informação

REFERÊNCIAS

NBR ISO/IEC 27002:2013

DOCUMENTOS RELACIONADOS

Nenhum

APROVAÇÃO

Criado por	Título	Data	Assinatura
STI	Conformidade	25/02/21	
Aprovado por	**Título**	**Data**	**Assinatura**
STI	Conformidade	25/02/21	

HISTÓRICO DE REVISÃO

Versão	Data de Emissão	Data da Revisão	Descrição
1.0			