PREFEITURA DE
SÃO PAULO
FINANÇAS E
DESENVOLVIMENTO ECONÔMICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

(Anexo Único da Portaria SF 132/2016, de 15 de junho de 2016)

PREÂMBULO

1) A Secretaria de Finanças e Desenvolvimento Econômico, objetivando atender, implementar e manter a governança da Segurança da Informação, declara que:

a) A Segurança da Informação é uma questão sensível que engloba e permeia toda a atuação da Secretaria;

b) A Segurança da Informação é um requisito de negócio para a Secretaria;

c) A Segurança da Informação é responsabilidade de todos os integrantes da Secretaria;

d) A Segurança da Informação exige políticas, procedimentos e ações implementados e com efetividade;

e) A Segurança da Informação se baseia em gestão apropriada de riscos, ativos e controles;

f) A Segurança da Informação demanda adequada alocação de recursos;

g) A Segurança da Informação requer treinamento e conscientização;

h) A Segurança da Informação deve ser planejada, gerenciada, mensurável e mensurada;

i) A Segurança da Informação exige definição e atribuição adequadas de competências, papéis e responsabilidades;

j) A Segurança da informação demanda devida qualidade de bens e serviços, adequando-se conforme a necessidade e as condições de fato; e

k) A Segurança da Informação impõe processos de avaliação e melhoria contínua.

2) A Política de Segurança da Informação – POSIN é uma norma em nível estratégico que estabelece, entre outras coisas, princípios, diretrizes, competências, responsabilidades e disposições gerais para a Segurança da Informação no âmbito da Secretaria Municipal de Finanças e Desenvolvimento Econômico.

a) A POSIN adota a abordagem finalística e baseada em riscos e oportunidades, visando a efetividade da Segurança da Informação.

b) A POSIN adota a visão de Segurança Centrada em Pessoas, para promover maior autonomia, agilidade e flexibilidade nas ações e decisões de Segurança da Informação, ao mesmo tempo em que reforça a responsabilização e o monitoramento.

c) Para esta POSIN, a acepção da palavra "Informação", com a primeira letra em maiúscula, é diferente da acepção da palavra "informação", com a primeira letra em minúscula, conforme disposto no Capítulo III.

3) Esta POSIN deverá ser interpretada de forma a maximizar a efetividade de suas disposições e a concretização dos princípios nelas inerentes.

CAPÍTULO I
DOS OBJETIVOS

4) São objetivos desta POSIN:

I. Instituir o Programa de Governança de Segurança da Informação da Secretaria Municipal de Finanças e Desenvolvimento Econômico - PGSEG;

II. Munir a Secretaria de instrumentos jurídicos e organizacionais que habilitem tecnológica e administrativamente seus agentes, de modo a prover Segurança da Informação em níveis adequados;

III. Estabelecer controles e mecanismos para embasar, direcionar e avaliar as iniciativas relacionadas à Segurança da Informação;

IV. Garantir a autonomia da Secretaria em relação à segurança da sua Informação independentemente do meio e do ambiente;

V. Nortear a elaboração das normas necessárias à efetiva implementação da Segurança da Informação;

VI. Promover as ações necessárias à implementação, manutenção, adequação e melhoria da Segurança da Informação;

VII. Fomentar a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação;

VIII. Estimular a conscientização e a disseminação de uma mentalidade adequada relativa à Segurança da Informação.

CAPÍTULO II

DA ABRANGÊNCIA

5) Estão submetidos a esta Política e a todas as suas Normas Complementares todos os servidores, colaboradores, estagiários, prestadores de serviço e todos que, de alguma forma, exerçam atividades no âmbito da Secretaria Municipal de Finanças e

Desenvolvimento Econômico, bem como qualquer pessoa, física ou jurídica, que venha a ter acesso a qualquer Informação desta Secretaria.

6) Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela Secretaria deverão incluir dispositivos de forma a viabilizar ou facilitar a implementação do disposto nesta POSIN.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

7) No âmbito desta POSIN, define-se:

I. Alta Administração: servidores ocupantes dos cargos assim identificados, conforme Decreto n.º 56.130/2015 - Código de Conduta Funcional dos Agentes Públicos e da Alta Administração Municipal;

II. ameaça: causa potencial de um incidente não desejado, que pode causar danos ou exposição indevida à Informação;

III. autenticidade: propriedade de que uma pessoa, organização, entidade, documento ou Informação realmente é o que ela diz ser;

IV. classificação da Informação: identificação de quais são os níveis de proteção que a Informação demanda e estabelecimento de categorias e formas de identificá-las, além de determinar os controles necessários a cada uma;

V. competência: poder ou autoridade passível de ser aplicado para a consecução de uma determinada atividade ou tarefa;

VI. confiabilidade: propriedade de obter comportamentos e resultados de forma prevista e consistente;

VII. confidencialidade: propriedade de não estar disponível ou não ser revelado para indivíduos, entidades ou processos não autorizados;

VIII. conformidade: atendimento a um ou mais requisitos pré-estabelecidos;

IX. conhecimento: resultado da ordenação e/ou processamento de uma ou mais informações, aliadas ao contexto, à experiência e/ou à intuição;

X. continuidade de negócio: capacidade de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas ou comprometimentos da Informação das atividades relevantes, de forma a manter suas operações em um nível aceitável, previamente definido;

XI. controle: método ou ação que avalia ou altera o risco de uma Informação;

XII. dado: um ou mais fatos, sinais ou símbolos quantificados ou quantificáveis;

XIII. disponibilidade: propriedade de estar acessível e usável para atender tempestivamente à demanda de uma pessoa, processo, ou entidade autorizada;

XIV. fiel depositário: pessoa, organização ou entidade responsável pelo armazenamento, transporte ou processamento da Informação. É também responsável pela aplicação apropriada das diretrizes desta POSIN para a Informação sobre a qual detenha responsabilidade ou que custodie, dentro dos limites das suas atribuições, competências e conhecimentos;

XV. gestão de incidentes: processos para detectar, registrar, relatar, dimensionar, responder, lidar e aprender a partir dos incidentes;

XVI. gestão de risco: atividades coordenadas para direcionar e controlar uma organização com relação ao risco;

XVII. governança da Segurança da Informação: conjunto de princípios e processos pelo qual a Secretaria fornece visões e orientações das atividades relacionadas à Segurança da Informação;

XVIII. incidente: evento ou sequência de eventos já ocorridos, que podem ou não causar impactos em termos de Segurança da Informação.

XIX. informação: conjunto de dados estruturados e/ou ligados por meio de uma ou mais relações;

XX. Informação: ativos materiais e imateriais da Secretaria, compreendendo, entre outros aspectos, dados, informações, conhecimentos e competências, bem como comunicações, atividades, ações, processos, estruturas, relações, táticas e estratégias;

XXI. Informação Documentada: Informação, independente de formato, mídia e fonte, que deve ser controlada e mantida adequadamente pela Secretaria, bem como o meio que a contém, incluindo evidências, processos e documentações.

XXII. integridade: propriedade de completude e fidedignidade;

XXIII. irretratabilidade: também conhecida como não-repúdio, é a capacidade de provar a ocorrência de determinado evento ou ação, bem como provar a sua autoria ou responsabilidade;

XXIV. Parte Interessada: pessoa ou organização que pode afetar, ser afetada ou perceber que afeta ou que é afetada por uma decisão ou atividade;

XXV. política: intenções e diretrizes de uma organização conforme dispostas pela Alta Administração, seja ela normatizada ou não;

XXVI. procedimento: uma ou mais instruções que detalham e permitem a operacionalização, total ou parcial, de uma política;

XXVII. rastreabilidade: capacidade de detectar a ocorrência de determinado evento ou ação, prover caracterização adequada do fato e determinar a sua autoria;

XXVIII. requisito: materialização formal da necessidade ou expectativa, seja implícita ou obrigatória;

XXIX. risco: efeito da incerteza sobre o objetivo;

XXX. Segurança Centrada em Pessoas: abordagem de Segurança da Informação focada em modelagem de comportamento, priorizando educação e monitoramento.

XXXI. segurança da informação: preservação das Bases Fundamentais da Segurança da Informação dispostas no Capítulo IV;

XXXII. Segurança da Informação: preservação de todos os princípios da Segurança da Informação dispostos no Capítulo IV;

XXXIII. terceiro: Parte Interessada externa à Secretaria;

XXXIV. validação: confirmação, por meio de evidências objetivas, que um requisito específico foi atendido por um ou mais ativos em processo de aquisição, contratação ou desenvolvimento;

XXXV. verificação: confirmação, por meio de evidências objetivas, da aderência de um ou mais ativos já existentes ao requisito especificado para ele(s);

XXXVI. vulnerabilidade: fragilidade potencial existente em um ativo ou controle que pode ser explorada por uma ou mais ameaças.

CAPÍTULO IV

DOS PRINCÍPIOS

8) Esta POSIN se encontra calcada nos seguintes princípios:

I.Valoração da Informação;

II. Vulnerabilidade da Informação;

III. Princípio da Confiança;

IV. Extensibilidade;

V. Bases Fundamentais da Segurança da Informação;

VI. Qualidade;

VII. Proporcionalidade;

a) A Valoração da Informação define que a Informação possui valor para a Administração e, portanto, devem existir mecanismos físicos, tecnológicos, pessoais, processuais, organizacionais e normativos implementados para conferir adequado tratamento à Informação de forma a atender efetivamente aos interesses da Secretaria.

i) Em particular, a Informação protegida pelo sigilo, tal como o disposto nos incisos X e XII do Artigo 5º da Carta Magna, no Artigo 325 do Código Penal, no Artigo 198 do Código Tributário Nacional e demais instrumentos normativos, deve receber especial atenção para que apenas as partes corretamente autorizadas tenham os devidos privilégios de acesso, manuseio e descarte.

b) A Vulnerabilidade da Informação declara que a Informação possui vulnerabilidades em termos físicos, tecnológicos, pessoais, processuais e organizacionais, exigindo a adoção de medidas e controles nos níveis estratégico, tático e operacional para que haja efetiva Segurança da Informação.

c) O Princípio da Confiança estabelece que uma pessoa ou um processo automatizado que esteja aderente aos critérios e atributos de Segurança da Informação podem ter maior autonomia e ter a sua atuação facilitada em função do tipo do ativo, do perfil da pessoa e da criticidade da Informação.

i) O Princípio da Confiança não obsta a adoção da Denegação por Padrão, na qual, salvo disposição em contrário, a Administração só concederá e manterá os privilégios estritamente necessários e suficientes para a execução das atividades.

d) A Extensibilidade preconiza a extensão e a complementação desta POSIN, por meio de normas adicionais, visando a dar adequado alcance e profundidade às normas de Segurança da Informação.

e) No âmbito desta POSIN, as Bases Fundamentais da Segurança da Informação são:

I. Confidencialidade;

II. Integridade;

III. Disponibilidade;

IV. Autenticidade;

V. Rastreabilidade;

VI. Irretratabilidade;

VII. Confiabilidade;

VIII. Utilidade;

IX. Ética;

X. Consciência;

XI. Posse; e

XII. Conformidade.

f) A Qualidade determina que a qualidade de bens e serviços é um fator relevante para a Segurança da Informação.

i) Os bens e serviços abrangem todos os bens e serviços adquiridos ou contratados pela Secretaria, não se limitando àqueles relacionados à segurança da informação.

g) Para fins desta POSIN, a Proporcionalidade é uma manifestação dos Princípios da Razoabilidade, da Economicidade e da Eficiência e define que os aspectos qualitativos e quantitativos da efetiva aplicação das normas e princípios aqui expressos serão definidos em função dos benefícios trazidos à Segurança da Informação e dos custos associados à aplicação.

CAPÍTULO V

DAS DIRETRIZES GERAIS

9) Esta POSIN define e estabelece a Segurança da Informação em nível estratégico. O detalhamento de suas diretrizes será regulamentado em Normas Complementares.

a) As Normas Complementares possuem efeito para toda a Secretaria.

b) Como documentação auxiliar, as Normas Complementares poderão ter:

I. Padrões, que definem os procedimentos a serem seguidos na falta de disposição específica;

II. Boas Práticas, que apresentam exemplos não vinculantes de procedimentos considerados como adequadamente seguros e aderentes à POSIN; e

III. Manuais Operacionais, elaborados por cada unidade, em conjunto com a COTEC, que formalizam o seu *modus operandi* em termos de Segurança da Informação.

10) Todas as Informações devem estar em conformidade com esta POSIN e, no que for aplicável, com as suas Normas Complementares.

11) É vedada a utilização de informações produzidas por terceiros para uso exclusivo da Secretaria em quaisquer outros projetos ou atividades que não sejam do interesse da Secretaria, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Secretário, nos demais casos.

12) As normas, procedimentos e ações de Segurança da Informação da Secretaria decorrentes desta POSIN deverão promover também:

I. Continuidade dos processos e serviços essenciais para o funcionamento da Secretaria;

II. Qualidade adequada na prestação de serviços, tanto pela Secretaria quanto pelos agentes externos, colaboradores, prestadores de serviços e outros terceiros, para a Secretaria;

III. Qualidade adequada na aquisição de ativos para a Secretaria.

13) A Informação poderá ser classificada de acordo com os níveis definidos conforme a legislação e as normas vigentes.

a) Categorias adicionais poderão ser estabelecidas pela POSIN ou pelas suas Normas Complementares.

14) Todas as partes interessadas relevantes devem estar explicitadas claramente em cada iniciativa referente à Segurança da Informação.

15) Para cada uma das diretrizes, gerais ou específicas, constantes desta POSIN podem ser elaboradas uma ou mais Normas Complementares específicas para detalhar, modular ou implementar de maneira efetiva o disposto nesta POSIN.

CAPÍTULO VI

DAS DIRETRIZES ESPECÍFICAS

SEÇÃO I

DO PROGRAMA DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO DA SECRETARIA MUNICIPAL DE FINANÇAS E DESENVOLVIMENTO ECONÔMICO

16) Fica instituído o Programa de Governança de Segurança da Informação da Secretaria Municipal de Finanças e Desenvolvimento Econômico - PGSEG;

a) O PGSEG visa a promover o alinhamento estratégico com os objetivos da Secretaria, a agregação e entrega de valor para as partes interessadas, bem como a gestão adequada dos riscos de Informação da Secretaria.

b) O PGSEG se pauta pelas seguintes premissas:

I. Difusão da Segurança da Informação em todo o âmbito da Secretaria;

II. Adoção de uma abordagem baseada na gestão de riscos;

III. Investimento de recursos para alcançar os objetivos de Segurança da Informação em consonância com os objetivos estratégicos;

IV. Aderência a requisitos relevantes interna e externamente;

V. Promoção de um ambiente positivo em termos de Segurança da Informação;

VI. Aplicação de mecanismos de avaliação da adequação da Segurança da Informação.

c) O PGSEG, como parte essencial da Segurança da Informação da Secretaria, será objeto de avaliação e melhoria contínuas.

d) O planejamento das iniciativas e ações relativas à Segurança da Informação deve considerar os fatores externos e internos relevantes, que podem afetar a efetividade do PGSEG.

e) A Administração determinará e fornecerá os recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do PGSEG.

17) O PGSEG deverá definir os processos de análise, avaliação e tratamento de riscos da Informação da Secretaria.

18) O PGSEG deverá definir os processos de detecção e resposta a incidentes de Segurança da Informação.

19) O PGSEG deverá definir os processos de monitoramento, avaliação, auditoria e melhoria contínua da Segurança da Informação.

20) O PGSEG deverá definir os processos de gestão de Informação Documentada relativa à Segurança da Informação.

21) O PGSEG deverá gerar um Plano Estratégico de Segurança da Informação – PESEG – para a Secretaria, em conformidade com os ditames da POSIN.

a) O PESEG deverá conter o planejamento estratégico a médio e longo prazo e estar alinhado com os objetivos estratégicos da Secretaria.

b) O PESEG poderá estar contido dentro do Plano Estratégico de Tecnologia da Informação (PETI) da Secretaria.

22) O Conselho do PGSEG é o órgão gestor do Programa de Governança da Segurança da Informação e será composto pelo Coordenador Geral da Coordenadoria de Tecnologia de Informação e Comunicação – COTEC, pelo Subsecretário da Receita Municipal – SUREM, pelo Subsecretário do Tesouro Municipal – SUTEM, pelo Coordenador Geral da Coordenadoria de Controle Interno – COCIN e pelo Subsecretário de Planejamento e Orçamento Municipal – SUPOM, com o apoio da Alta Administração.

a) No tocante à Segurança da Informação, a gestão das metas, ações, riscos, controles e decisões da Secretaria em nível estratégico e estratégico-tático são de atribuição do Conselho do PGSEG, enquanto que a gestão das metas, ações, riscos, controles e decisões da Secretaria em nível tático e tático-operacional são de atribuição dos Gestores de Negócio ou a quem determinarem as normas vigentes ou, subsidiariamente, a quem determinar o Conselho do PGSEG.

b) O Conselho do PGSEG será responsável pela orientação, monitoramento e avaliação para Segurança da Informação em nível estratégico e estratégico-tático.

c) Compete ao Conselho do PGSEG publicar Normas Complementares e Padrões.

d) Compete à COTEC a competência para publicar Boas Práticas, mediante anuência do Conselho do PGSEG.

e) O Conselho do PGSEG será presidido pela COTEC, com o apoio da Alta Administração.

f) A assessoria em tecnologia do Conselho será feita pela Divisão de Segurança da Informação (DISEG), vinculada à COTEC, ou por membros da Secretaria ou ainda por terceiros, com a anuência do Conselho do PGSEG.

g) O Conselho do PGSEG se reunirá trimestralmente, mediante convocação da COTEC, ou quando surgir evento relevante que demande a sua atuação.

h) A COTEC poderá autorizar tratamento urgente aos casos assim considerados, visando a aprovação do Conselho do PGSEG, por meio de correspondência eletrônica, no prazo máximo de 48 (quarenta e oito) horas.

i) Em até 90 dias após a publicação desta POSIN, o Conselho do PGSEG deverá publicar o seu regimento interno, que deverá estabelecer no mínimo os critérios e procedimentos de tomada de decisão do Conselho.

j) Em até 90 dias após a publicação desta POSIN, o Conselho do PGSEG deverá deliberar sobre a edição e publicação de Normas Complementares consideradas prioritárias.

k) O tratamento de incidentes de Segurança da Informação considerados de criticidade alta será feito pelo Conselho do PGSEG.

l) O tratamento de incidentes de Segurança da Informação relativos à Tecnologia de Informação e Comunicação que não sejam de criticidade alta será realizado pela COTEC ou para quem a COTEC delegar esta atribuição, mediante anuência do Conselho do PGSEG.

m) A gestão de continuidade do negócio sob os aspectos de Tecnologia de Informação e Comunicação será realizada pela COTEC ou para quem a COTEC delegar esta atribuição, ouvida a área de negócio.

n) Em caso de violação de alguma diretriz da POSIN ou de suas Normas Complementares que coloque em risco iminente uma ou mais Bases Fundamentais de Segurança da Informação das Informações ou ativos da Secretaria, o Conselho do PGSEG poderá determinar restrições de caráter temporário à Informação e a ativos, físicos ou não, para garantir a continuidade do negócio.

o) Compete ao Conselho do PGSEG deliberar sobre os casos de Segurança da Informação que estejam omissos nesta POSIN ou em suas Normas Complementares.

SEÇÃO II

DO PLANEJAMENTO E GESTÃO DO CONTEXTO

23) A Secretaria, por meio do Conselho do PGSEG, deverá planejar, implementar e controlar as metas, iniciativas e ações necessárias para a Segurança da Informação.

24) A Segurança da Informação sempre estará presente na gestão de projetos, independentemente do tipo de projeto.

25) É dever de todos determinar riscos e oportunidades que devem ser considerados para garantir a efetividade da Segurança da Informação, prevenindo ou reduzindo efeitos indesejados e mantendo melhoria contínua.

26) A Secretaria, por meio do Conselho do PGSEG, determinará as necessidades relevantes de comunicação, interna e externa para a Segurança da Informação e definirá os processos para a sua efetivação.

27) É dever de todo Gestor de Negócio manter Informação Documentada na extensão necessária e suficiente para a efetividade da Segurança da Informação.

a) A Informação Documentada será elaborada, mantida, controlada e protegida nos moldes do que estabelecerem esta POSIN, Normas Complementares, Padrões e os Manuais Operacionais para que possa ser utilizada sempre e onde for necessária;

b) A Informação Documentada será detalhada em função do tamanho e complexidade da Informação, bem como da capacidade das pessoas envolvidas.

c) A Informação Documentada terá controles em termos de distribuição, acesso, obtenção, uso, armazenamento, preservação, controle de mudanças, retenção e descarte.

28) Papéis e responsabilidades em termos de Segurança da Informação devem ser definidos e atribuídos de maneira apropriada e efetiva, devendo-se aplicar a sua segregação sempre que possível para reduzir vulnerabilidades em termos de Segurança da Informação.

29) Contatos com grupos especiais de interesse ou outras organizações de segurança da informação devem ser mantidos, sempre que possível.

30) A Secretaria, por meio da COCIN e da COTEC, periodicamente avaliará a conformidade da Segurança da Informação com relação ao disposto na POSIN, nas Normas Complementares, Padrões, Boas Práticas e Manuais Operacionais.

a) A Secretaria manterá Informação Documentada para as evidências da auditoria;

b) O resultado da auditoria será disponibilizado para os gestores envolvidos, para o Conselho do PGSEG e para a Alta Administração.

31) É dever de todos adotar ações reativas e preventivas com relação a não conformidades em termos de Segurança da Informação.

SEÇÃO III

DA OPERAÇÃO

32) A Secretaria, por meio de cada uma de suas unidades, monitorará o uso dos seus recursos, ativos e informações, incluindo em termos de desempenho e usabilidade e respeitando-se os princípios legais.

a) Mecanismos serão implementados para o monitoramento, incluindo-se trilhas de auditoria que permitam rastrear, acompanhar, controlar e verificar os acessos e/ou interações do usuário com relação aos sistemas e dados da Pasta e à rede interna da Secretaria, bem como as interações feitas pelo usuário a partir de ativos da Secretaria ou valendo-se da infraestrutura da mesma.

b) Mecanismos serão implementados para garantir a exatidão e proteção dos dados coletados pelo monitoramento.

33) Controles e mecanismos criptográficos deverão ser implementados em Informações e ativos, físicos ou não, de forma a garantir a efetividade da Segurança da Informação e deverão estar atualizados e adequados para atender aos requisitos de negócio.

34) Os serviços de tecnologia da informação e comunicação fornecidos à Secretaria terão cláusulas que definirão níveis de serviço adequados e que sejam aplicados e atualizados de forma consistente ao longo do tempo, de forma a atender às necessidades da Secretaria.

SEÇÃO IV

DA SEGURANÇA DOS RECURSOS HUMANOS

35) A Secretaria, por meio da EMAF e da COTEC, com o apoio da ASCOM, promoverá a conscientização dos servidores e usuários de seus sistemas com relação às normas, políticas, procedimentos e boas práticas, a sua contribuição para a efetividade da Segurança da Informação e as implicações de não conformidades com as exigências da Segurança da Informação.

36) Os desvios de conduta em termos de Segurança da Informação serão apurados nos termos da legislação em vigor.

37) A Secretaria definirá e aplicará os procedimentos, em termos de Segurança da Informação, relativos à perda de vínculo do recurso humano com a Secretaria.

SEÇÃO V

DA GESTÃO DE ATIVOS

38) Os ativos relativos à tecnologia da informação e comunicação devem estar devidamente identificados e classificados em termos de Segurança da Informação.

a) A classificação será feita em função de exigências legais, valor, criticidade e sensibilidade à exposição ou modificação não autorizadas.

b) A classificação poderá ensejar diferentes formas de gestão da Informação, as quais serão respeitadas durante todo o seu ciclo de vida, desde a criação até o descarte.

39) Deve-se manter um inventário atualizado dos ativos e um catálogo atualizado de serviços.

a) Os ativos inventariados e os serviços catalogados devem ter um gestor responsável associado.

b) O gestor responsável pelo ativo deverá zelar permanentemente pela aderência do ativo com relação ao disposto nesta POSIN.

40) Todos os ativos da Secretaria custodiados pelos servidores e terceiros devem ser devolvidos quando do encerramento do seu vínculo com a Secretaria ou quando cessar a condição que demande ou permita tal custódia.

41) Os ativos físicos da Secretaria, incluindo-se as redes de comunicação e as instalações de infraestrutura, devem estar adequadamente protegidos contra indisponibilidade, acessos indevidos e falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

SEÇÃO VI

DO CONTROLE DE ACESSO

42) Devem-se estabelecer políticas e procedimentos de controle de acesso de acordo com os requisitos de negócio e de Segurança da Informação.

a) A identificação do usuário, independentemente da forma, será pessoal e intransferível e permitirá o seu reconhecimento de forma clara e inequívoca.

b) Os usuários deverão ter acesso apenas às instalações, à rede, aos serviços, aos sistemas e às Informações aos quais possuem autorização de acesso.

c) O acesso deverá ser feito por meios adequadamente seguros e deve ser condicionado ao aceite de um Termo de Responsabilidade, ou equivalente em meio eletrônico.

43) Os resultados do monitoramento em termos de Segurança da Informação poderão se refletir em alterações nos privilégios de acesso.

a) Deverá existir uma base de dados corporativa de gestão de pessoas, a qual deverá ser atualizada tempestivamente de forma automatizada ou por meio de notificações da unidade, se a automatização for inexistente ou inviável.

SEÇÃO VII

DA SEGURANÇA FÍSICA E DO AMBIENTE

44) A Secretaria implementará ações, controles e mecanismos de segurança de instalações físicas e/ou de equipamentos, sempre que houver a necessidade de garantir a segurança do usuário ou proteger a sua Informação de acesso não autorizado ou de dano ou de interferência, dentro do Princípio da Proporcionalidade.

a) Os procedimentos e mecanismos para descarte também serão realizados de forma a garantir adequadamente a segurança do usuário ou proteger a sua Informação de acesso não autorizado, dentro do Princípio da Proporcionalidade.

b) As ações, controles e mecanismos de segurança de instalações físicas e/ou de equipamentos podem incluir a definição de áreas de acesso restrito.

45) Políticas, procedimentos, ações e mecanismos serão adotados para Segurança da Informação em ambientes móveis, bem como em situações de trabalho remoto.

SEÇÃO VIII

DA SEGURANÇA DAS COMUNICAÇÕES

46) Mecanismos de segurança, níveis de serviço e requisitos de gerência de todos os serviços relacionados à comunicação de dados devem estar identificados e incluídos nos contratos de serviços de rede, inclusive quando os serviços forem contratados com terceiros.

a) A Secretaria tomará as ações necessárias para garantir que os mecanismos de segurança, níveis de serviço e requisitos de gerência de todos os serviços relacionados à comunicação de dados sejam compatíveis com os padrões de mercado, com as boas práticas e com os requisitos de segurança e que sejam aplicados e atualizados de forma consistente ao longo do tempo de forma a atender aos requisitos de qualidade e às necessidades da Secretaria.

47) A transferência de informações, independentemente do meio de comunicação, deverá ser realizada utilizando-se de meios adequados de proteção.

a) O tráfego das informações deve contar com métodos e mecanismos adequados de proteção contra transmissão incompleta, repetição ou comutação ou roteamento incorretos, adulteração de mensagem, revelação não autorizada e duplicação ou reenvio não autorizados de mensagens.

b) As informações trafegadas em redes públicas deve contar com métodos e mecanismos adequados de proteção contra atividade fraudulenta, bem como contra revelação e modificação não autorizadas.

48) A proteção da transferência de informações abrange inclusive o acesso a redes externas como a internet, o uso de ativos de rede e o uso de equipamentos de acesso à rede.

SEÇÃO IX

DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

49) Os requisitos de Segurança da Informação devem ser incluídos nos requisitos para novos sistemas ou nas melhorias dos sistemas existentes.

50) A COTEC, em conjunto com os Gestores de Negócio, monitorará o desenvolvimento, correção e melhoria de sistemas produzidos por terceiros.

SEÇÃO X

DA GESTÃO DE INCIDENTES E CONTINUIDADE DE NEGÓCIOS DE SEGURANÇA DA INFORMAÇÃO

51) Servidores e terceiros que utilizarem os sistemas e serviços da Secretaria deverão registrar e relatar qualquer vulnerabilidade de Segurança da Informação.

a) A Secretaria disponibilizará canais e meios para relatar as vulnerabilidades de Segurança da Informação.

52) Eventos avaliados pelo Gestor de Negócio como causadores, potenciais ou não, de impactos não desprezíveis aos interesses da Secretaria, deverão ser identificados, monitorados, comunicados e tratados em tempo hábil de forma a minimizar os danos.

a) A Secretaria disponibilizará canais e meios para relatar tempestivamente os eventos citados no *caput*.

53) A Secretaria responderá de maneira adequada aos incidentes de Segurança da Informação, incluindo a implementação de processos, procedimentos, infraestrutura e mecanismos para auditorias em resposta a incidentes, bem como a gestão de Informação Documentada e de conhecimentos relativa a incidentes.

a) Todos os incidentes de Segurança da Informação, no que tange à Tecnologia da Informação e Comunicação, deverão ser notificados à COTEC.

b) A Secretaria poderá acessar qualquer Informação e/ou ativo, físico ou não, de sua propriedade, para fins de averiguação.

54) Os incidentes de Segurança da Informação serão classificados e tratados de acordo com a sua criticidade, que poderá ser baixa ou alta, considerando-se a gravidade do risco ou dano à segurança da sociedade ou da Secretaria.

CAPÍTULO VII

DA COMPETÊNCIA E RESPONSABILIDADE

55) É de responsabilidade de todos que têm acesso, parcial ou total, à Informação de propriedade ou que transite pela Secretaria prezar pela Segurança da Informação,

segundo preceitos desta Política, das Normas Complementares, Padrões e Manuais Operacionais e de forma condizente com suas responsabilidades e sua atribuição.

SEÇÃO I

DA ALTA ADMINISTRAÇÃO

56) A Alta Administração desta Secretaria proverá ativamente o direcionamento, os recursos e o apoio necessários à Segurança da Informação, de acordo com o preâmbulo desta POSIN, com os objetivos estratégicos e com as normas pertinentes, respeitadas as restrições orçamentárias.

a) A Alta Administração fornecerá ativamente o seu apoio para iniciativas que visam a:

I. Suportar a efetividade do PGSEG, tais como:

i. Garantir a difusão da Segurança da Informação dentro da Secretaria;
ii. Alinhar o PGSEG com as estratégias da Secretaria;
iii. Garantir a integração do PGSEG nos processos da Secretaria;
iv. Prezar para que o PGSEG alcance os seus objetivos;
v. Promover a melhoria contínua.

II. Promover a capacitação e conscientização relativos à Segurança da Informação;

III. Normatizar e operacionalizar as diretrizes estabelecidas nas normas relativas à Segurança da Informação.

SEÇÃO II

DOS GESTORES DE NEGÓCIO

57) No âmbito da POSIN, cada unidade da Secretaria contará com um servidor ativo designado como Gestor de Negócio, que será o responsável pela gestão da Segurança da Informação no âmbito da unidade e das competências a ela atribuídas.

a) O Gestor de Negócio no âmbito da POSIN será o gestor da unidade, que poderá delegar expressamente, inclusive por meio eletrônico, essa atribuição.

b) Norma Complementar poderá especificar unidades que poderão prescindir de um Gestor de Negócio.

c) Conflitos de competência, tanto positiva quanto negativa, serão dirimidos pelo Conselho do PGSEG.

58) O Gestor de Negócio possui autonomia, assim entendida como a conjugação de habilidades e responsabilidade, para gerir as Informações da sua unidade ou sob sua guarda, alinhada aos objetivos de negócio da Secretaria ao mesmo tempo em que mantém aderência à Segurança da Informação conforme disposto nesta POSIN e em suas Normas Complementares.

59) Sem prejuízo da atuação do Conselho do PGSEG, o Gestor de Negócio tem como atribuições:

I. Promover a cultura da Segurança da Informação nas suas equipes, incentivando a participação em atividades de sensibilização, conscientização, capacitação e especialização e facilitando a disseminação e a implantação da Segurança da Informação no âmbito das suas áreas de atuação;

II. Orientar seus subordinados quanto à existência e aplicabilidade à sua unidade desta POSIN, das Normas Complementares, Boas Práticas e Manuais Operacionais, com o apoio técnico da COTEC, se necessário;

III. Elaborar e publicar Manuais Operacionais para a sua unidade, com o apoio técnico da COTEC, se necessário;

IV. Propor melhorias e novos procedimentos de Segurança da Informação relacionados às suas áreas de competência, submetendo as propostas ao Conselho do PGSEG;

V. Gerir, dentro dos limites da sua atuação e da sua unidade, os controles a serem realizados em termos de Segurança da Informação e determinar, de forma subsidiária ao estabelecido nas normas vigentes e ao estabelecido pelo Conselho do PGSEG, eventuais controles adicionais que se façam convenientes ou necessários para a unidade;

VI. Classificar as Informações de sua unidade ou sob sua guarda, de acordo com os critérios estabelecidos nas normas vigentes;

VII. Atuar de forma diligente com relação a incidentes e vulnerabilidades das Informações de sua unidade ou sob sua guarda;

VIII. Atuar de forma tempestiva com relação a incidentes de criticidade alta, realizando o seu tratamento em caráter precário enquanto não houver a atuação do Conselho do PGSEG;

IX. Resolver, de maneira motivada, excepcional e pontual, eventuais conflitos entre os interesses da Secretaria e as normas de Segurança da Informação, apenas com relação a incidentes ou não-conformidades irrelevantes ou de criticidade baixa com relação à Segurança da Informação de sua unidade ou sob sua guarda;

X. Comunicar imediatamente casos relevantes de violação de Segurança da Informação ao Conselho do PGSEG;

XI. Participar e apoiar integralmente a apuração de incidentes de Segurança da Informação relacionados à Informação sob a guarda ou responsabilidade da unidade e

prover informações acerca da Segurança da Informação para o Conselho do PGSEG ou para a Alta Administração, no âmbito da sua atuação e da atuação da sua unidade.

60) Todo sistema deverá estar vinculado a um Gestor de Negócio, que será responsável pela gestão do sistema em termos de regras de negócio.

a) O Gestor de Negócio terá o apoio técnico da COTEC.

b) Caso o sistema seja gerido por apenas uma unidade organizacional ou implemente regras de negócio de apenas uma unidade organizacional, o Gestor de Negócio vinculado ao sistema será o dessa unidade.

c) Caso o sistema seja gerido por mais de uma unidade ou implemente regras de negócio de mais de uma unidade, o primeiro superior hierárquico comum a todas designará o Gestor de Negócio associado ao sistema, dentre os das unidades envolvidas.

d) Em caso de indefinição sobre qual unidade realiza a gestão do sistema, o Gestor de Negócio associado ao sistema será o da unidade cujas competências ou atribuições funcionais estejam mais alinhadas com as regras de negócio implementadas pelo sistema.

e) O Conselho do PGSEG poderá definir quem será o Gestor de Negócio em caso de haver conflitos de interesse que dificultem ou inviabilizem a definição consoante os itens anteriores.

f) A partir da publicação desta Norma, novos sistemas só poderão entrar em produção se houver um Gestor de Negócio previamente associado consoante os critérios anteriores.

g) Os sistemas já em produção no momento da publicação desta Norma terão seus respectivos Gestores de Negócio definidos pelo Conselho do PGSEG em até 90 dias após a publicação desta Norma, conforme os critérios anteriores.

h) O Conselho do PGSEG poderá definir outros ativos, além de sistemas, que deverão ter um vínculo expresso com um Gestor de Negócio.

SEÇÃO III

DOS SERVIDORES E COLABORADORES

61) São deveres de todo servidor ou colaborador da Secretaria:

I. Adotar e promover a cultura da Segurança da Informação nas suas atividades, participando de atividades de sensibilização, conscientização, capacitação e especialização, facilitando a disseminação e a implantação da Segurança da Informação no âmbito da sua atuação, seguindo sempre que possível os procedimentos definidos

como Boas Práticas e cumprindo com os deveres dispostos na POSIN e nas demais normas de Segurança da Informação;

II. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à Segurança da Informação;

III. Assinar os termos ou instrumentos equivalentes que venham a ser instituídos por normas de Segurança da Informação, formalizando a ciência e o aceite da política, das normas e procedimentos respectivos, bem como assumindo responsabilidade por seu fiel cumprimento no que diz respeito a suas atribuições;

IV. Utilizar os recursos de segurança que lhe forem disponibilizados para proteger as informações a que tenha acesso contra acesso, modificação, destruição ou divulgação não autorizados nos termos da POSIN e Normas Complementares;

V. Sugerir melhorias em termos de Segurança da Informação no âmbito das suas atividades, competências ou conhecimentos.

CAPÍTULO VIII

DAS DISPOSIÇÕES GERAIS

62) A POSIN e suas Normas Complementares serão disponibilizadas para consulta de todos os servidores e colaboradores na rede corporativa desta Secretaria, sem prejuízo da publicação oficial.

a) Alterações na POSIN e/ou nas Normas Complementares serão objeto de ampla divulgação.

63) Além do disposto nesta POSIN, as iniciativas de Segurança da Informação desta Secretaria deverão também se orientar, de forma subsidiária e sem prejuízo da aplicação do Princípio da Razoabilidade e das restrições orçamentárias, pelas melhores práticas e procedimentos de Segurança da Informação recomendados oficialmente por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

64) Fica revogada a Portaria SF 160/2006, que estabelece a Política de Segurança da Informação.

65) O disposto na Portaria SF 39/2007, que dispõe sobre o controle de acesso aos bancos de dados da Secretaria Municipal de Finanças – SF, fica recepcionado por esta POSIN até a publicação de uma Norma Complementar que contenha disposições sobre o mesmo tema.

66) O disposto na Portaria SF 104/2010, que disciplina a utilização, controle e responsabilidade pelos ativos de informação da Secretaria Municipal de Finanças, fica recepcionado por esta POSIN até a publicação de uma Norma Complementar que contenha disposições sobre o mesmo tema.

67) As normas de referência desta POSIN são:

I. Constituição Federal de 1998 e suas atualizações, notadamente o Artigo 5º.

II. Código Tributário Nacional e suas atualizações, notadamente o Artigo 198.

III. Código Penal Brasileiro e suas atualizações, notadamente os Artigos 153, 313-A, 313-B e 325.

IV. Lei 12.527/2011 (Lei de Acesso à Informação) e o Decreto 53.623/2012 e suas atualizações, que regulamentam a Lei no âmbito municipal.

V. Lei 14.098/2005 e o Decreto 49.914/2008, que dispõe sobre a proibição de acesso a "sites" da Internet com conteúdos relacionados a sexo, drogas, pornografia, pedofilia, violência e armamento, no âmbito dos órgãos integrantes da Administração Municipal Direta e Indireta.

VI. Lei Nº 12.737/2012, que dispõe sobre a tipificação criminal de delitos informáticos.

VII. Lei 12.965/2014 (Marco Civil da internet).

VIII. Decreto 56.130/2015 e suas atualizações, que institui, no âmbito do Poder Executivo, o Código de Conduta Funcional dos Agentes Públicos e da Alta Administração Municipal.

IX. Orientação Normativa 02/2013, do Gabinete do Prefeito de São Paulo.

X. Padrões internacionais ISO 27001/2013, ISO 27002/2013 e ISO 27014/2013, que versam respectivamente sobre Requisitos da Segurança da Informação, Boas Práticas da Segurança da Informação e Governança da Segurança da Informação.

CAPÍTULO IX

DA ATUALIZAÇÃO

68) Esta POSIN deverá ser revisada e atualizada a cada três anos ou quando houver fatos relevantes que exigirem revisão extemporânea.

a) As Normas Complementares serão revisadas a cada dois anos ou sempre que surgirem fatos relevantes que justifiquem a revisão.

b) A revisão e a atualização da POSIN e das Normas Complementares serão realizadas pelo Conselho do PGSEG, com o apoio de todas as unidades da Secretaria.