Decreto N. 8109
DE 29 DE NOVEMBRO DE 2024

"“Institui a Política Municipal de Segurança da Informação – PSI, do Município Da Estância Balneária De Praia Grande/SP e revoga o Decreto N° 7.737 de 29 de dezembro de 2022”"

A Prefeita da Estância Balneária de Praia Grande, usando das atribuições que lhe são conferidas por Lei, nos termos do artigo 69 Inciso XXV, da Lei 681 de 06 de abril de 1990,

DECRETA

Art. 1º. Fica instituída a Política Municipal de Segurança da Informação - PSI, Decreto que orienta e estabelece as diretrizes para a proteção dos ativos de informação, práticas para a gestão da sua segurança e a prevenção de responsabilidade legal para todos os agentes públicos no âmbito da Administração Pública Direta do Município da Estância Balneária de Praia Grande.

Art. 2º. As diretrizes estabelecidas neste Decreto, deverão ser adotadas por todos os agentes públicos, bem como toda pessoa física ou jurídica que, de alguma forma, execute atividades funcionais amparadas por contratos ou instrumentos jurídicos e que para tanto venham a utilizar ou ter acesso às informações de propriedade do Poder Executivo Municipal ou sob sua custódia, em qualquer meio, especialmente, físico ou eletrônico.

Art. 3º. É também obrigação de cada agente público ou preposto de pessoa jurídica contratada se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou do Comitê de Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso ou descarte de informações.

CAPÍTULO I
OBJETIVOS DA PSI

Art. 4º. A PSI, orienta e estabelece as diretrizes institucionais da Administração Direta Municipal para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas e por todos os agentes públicos ou prepostos de pessoa jurídica contratada.

Parágrafo único. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Art. 5º. Constitui objetivo da PSI:

I. Estabelecer diretrizes que permitam aos agentes públicos ou prepostos de pessoa jurídica contratada seguirem padrões de comportamento relacionados à segurança da informação, segurança cibernética, segurança física de ambientes e de pessoas, segurança de canais, produtos e serviços, continuidade de negócios, uso e tratamento de dados e informações adequados às necessidades de negócio e de proteção legal do município e do indivíduo;

II. Estabelecer diretrizes para guiar a segurança cibernética contra ameaças e ataques cibernéticos, através da prevenção, detecção e redução das vulnerabilidades;

III. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento e;

IV. Preservar as informações da Administração Direta Municipal quanto à:

a. Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

b. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

c. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário e;

d. Rastreabilidade: Garantia de poder acompanhar ou identificar o percurso de um dado ou informação durante um processo.

CAPÍTULO II
CONCEITOS

Art. 6º. Para fins dessa PSI, considera-se:

I. Informação: conjunto organizado de dados, processados eletronicamente ou não, que podem ser utilizados para produção e transmissão de conhecimento. A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio pelo qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida;

II. Tratamento: toda operação realizada com qualquer tipo de informação, com dados do Município ou de terceiros, desde coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

III. Segurança da Informação: é a proteção da informação contra vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio;

IV. Comitê de Segurança da Informação (CSI): Grupo multidisciplinar, que tem o intuito de definir, deliberar e apoiar estratégias necessárias à implantação e manutenção da segurança da informação;

V. Proprietário da Informação: é quem tem a posse legal e define as regras de negócio para o tratamento das informações;

VI. Data Center: infraestrutura física projetada para abrigar servidores e outros recursos computacionais, como sistemas de armazenamento de dados (storages), ativos de redes (switches e roteadores) e passivos de redes (cabeamento de redes de dados e eletricidade);

VII. Backup ou Cópia De Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada e;

VIII. Login de serviço: login utilizado para aplicações internas.

CAPÍTULO III
PRINCÍPIOS DA PSI

Art. 7º. Toda informação produzida ou recebida pelos agentes públicos e prepostos de pessoa jurídica contratada como resultado da atividade profissional exercida no Poder Executivo Municipal pertence à Administração Direta Municipal. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Art. 8º. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos agentes públicos e prepostos de pessoa jurídica contratada para a realização das atividades profissionais.

Art. 9º. O Poder Executivo Municipal é responsável por registrar todos os acessos e operações realizadas nos sistemas e serviços, com o objetivo de assegurar a disponibilidade contínua e a segurança integral das informações utilizadas.

Parágrafo único. No caso de sistemas operados por terceiros, os mesmos deverão permitir à secretaria gestora do contrato o pleno acesso e controle sobre os registros mencionados no caput deste artigo, assegurando a conformidade com os requisitos de segurança estabelecidos.

CAPÍTULO IV
REQUISITOS DA PSI

Art. 10. Deverá constar em todos os contratos, convênios e instrumentos congêneres celebrados com o Poder Executivo, que visam o acesso aos ativos de informação do município, possuam cláusula visando ciência sobre a responsabilidade e confidencialidade necessárias para cumprimento à Lei Federal 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), bem como, a este decreto.

Art. 11. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Divisão de Infraestrutura e Segurança Dados que, por sua vez, encaminhará o caso ao Comitê de Segurança da Informação para análise, caso haja necessidade de revisão ou acionamento do Plano de Continuidade de Serviços de Tecnologia da Informação (PCTI).

Parágrafo Único. O Plano de Continuidade de Serviços de Tecnologia da Informação (PCTI), regulamentado pelo Decreto nº 7.934 de 27 de dezembro de 2023, tem como propósito assegurar a continuidade dos serviços em caso de paralisação decorrente de um ou mais processos críticos, além de promover estratégias e medidas de proteção eficazes e rápidas para os processos de TI, garantindo sua preservação após a ocorrência de um desastre.

Art. 12. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que o município julgar necessário para reduzir os riscos d seus ativos de informação como por exemplo, nas estações de trabalho, notebooks, nos acessos à intern correio eletrônico, nos sistemas comerciais e financeiros.

Art. 13. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento e testes.

Art. 14. Deve-se buscar constantemente no processo de segurança cibernética a inovação, automação, inteligência e melhores práticas de mercado com foco em mitigar os riscos cibernéticos, reduzir custos operacionais no processo, diminuir os tempos de detecção e resposta a incidentes, e manter a disponibilidade dos serviços.

Art. 15. A Administração Direta Municipal reserva-se ao direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis, no caso do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus agentes públicos e prepostos.

Art. 16. As instruções presentes neste decreto são obrigatórias para todos os agentes públicos e prepostos de pessoa jurídica contratada, independentemente do nível hierárquico ou função no município, bem como de vínculo empregatício ou prestação de serviço.

CAPÍTULO V
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 17. Fica instituído o Comitê de Segurança da Informação, com as seguintes atribuições:

I. Coordenar a implantação da PSI e das normas internas de segurança da informação do Poder Executivo Municipal, observada a legislação vigente;

II. Assessorar a Administração Direta Municipal nas atividades relacionadas à segurança da informação;

III. Estimular ações de boas práticas, de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV. Promover a divulgação da política e das normas internas de segurança da informação aos agentes públicos usuários de informações no Município;

V. Propor formas de orientação e divulgação de boas práticas para segurança cibernética aos usuários dos serviços municipais;

VI. Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII. Propor recursos necessários às ações de segurança da informação;

VIII. Supervisionar as políticas, estratégias e processos de segurança da informação no Poder Executivo Municipal;

IX. Orientar a respeito dos processos para identificação, priorização e tratamento de riscos de segurança da informação;

X. Propor regras e critérios para o gerenciamento de riscos de segurança da informação, além de ações corretivas relacionadas;

XI. Acompanhar os incidentes relevantes relacionados à segurança da informação;

XII. Definir, deliberar e apoiar estratégias necessárias à implantação e manutenção da segurança da informação e;

XIII. Revisar e atualizar a PSI e normas correlatas sempre que motivado por algum fato ou evento relev

Art. 18. O Comitê de Segurança da Informação será composto por 1 (um) representante titular e respectivo suplente indicados pelos seguintes órgãos:

I. Secretaria de Planejamento, que o coordenará;

II. Gabinete da Prefeita;

III. Procuradoria Geral do Município;

IV. Procuradoria Fiscal do Município;

V. Secretaria de Administração;

VI. Secretaria de Assuntos de Segurança Pública;

VII. Secretaria de Educação;

VIII. Secretaria de Governo e;

IX. Secretaria de Saúde Pública.

§ 1º. Os membros do Comitê de Segurança da Informação e os respectivos suplentes serão indicados pelos titulares dos órgãos que representam, preferencialmente entre os agentes públicos que possuam atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos.

§ 2º. Os membros titulares do Comitê de Segurança da Informação serão substituídos pelos respectivos

suplentes, em suas ausências ou impedimentos.

§ 3º. A participação no Comitê de Segurança da Informação será considerada prestação de serviço público relevante, não remunerada.

§ 4º. O Comitê de Segurança da Informação aprovará seu regimento interno, que disporá sobre a organização e o funcionamento do Comitê, no prazo de noventa dias, contado da data de publicação deste Decreto.

CAPÍTULO VI
DAS RESPONSABILIDADES ESPECÍFICAS

Seção I
Do agente público ou preposto de pessoa jurídica contratada em geral

Art. 19. Entende-se por agente público todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no Município.

Art. 20. Entende-se por preposto de pessoa jurídica contratada todo representante legal designado e autorizado pela referida pessoa jurídica para agir em seu nome em relação a determinadas atribuições, obrigações ou responsabilidades contratualmente estabelecidas. Este preposto é incumbido de representar os interesses da pessoa jurídica contratada perante terceiros, agindo de acordo com os termos e condições do contrato estabelecido entre as partes envolvidas.

Art. 21. Todos os agentes públicos e prepostos de pessoa jurídica contratada que venham a utilizar ou ter acesso às informações de propriedade do Poder Executivo Municipal ou sob sua custódia, em qualquer meio, bem como aqueles que possam ter acesso à infraestrutura de computadores e rede de dados a qualquer momento, devem:

I. Ler e assinar o Termo de Responsabilidade da Política de Segurança da Informação;

II. Ter ciência de que os ambientes, sistemas, computadores e redes da Administração Direta Municipal poderão ser monitorados e gravados, a fim de garantir a integridade e segurança de seus ativos, bem como a conformidade com as legislações vigentes e;

III. Manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou do setor competente pelas ações de tecnologia e inovação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações;

Parágrafo único. O Termo de Responsabilidade da Política de Segurança da Informação tem como objetivo comprovar a ciência do agente público ou preposto de pessoa jurídica contratada sobre a Política de Segurança da Informação e de suas respectivas normas de apoio, bem como sobre as regras a serem observadas para acesso aos recursos de Tecnologia da Informação e Comunicação (TIC) da rede institucional e às informações da Administração Direta Municipal e sob sua custódia, armazenadas ou registradas em qualquer meio, físico ou eletrônico, visando principalmente a manutenção da integridade, confidencialidade e disponibilidade das informações.

Art. 22. A Secretaria de Administração - SEAD deve manter arquivada no prontuário de todos os agentes públicos uma via do Termo de Responsabilidade da Política de Segurança da Informação, devidamente assinado pelo servidor.

Art.23. Os servidores temporários e prepostos de pessoa jurídica contratada deverão ter o Termo de Responsabilidade da Política de Segurança da Informação assinado e registrados no processo administrativo correspondente, pela secretaria gestora.

Art. 24. Não é permitido manter acessíveis ou permitir acesso a pessoas não autorizadas a documentos e informações em qualquer tipo de mídia eletrônica, impressa ou qualquer outra.

Art. 25. Será de inteira responsabilidade de cada agente público ou preposto de pessoa jurídica contratada, todo prejuízo ou dano que vier a sofrer ou causar à Administração Direta Municipal e a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Art. 26. A prática de “Mesa Limpa, Tela Limpa e Impressora Limpa” é recomendada a todos os agentes públicos e prepostos de pessoa jurídica contratada, seja nas dependências de próprios municipais ou em ambiente de trabalho remoto. São exemplos dessa prática:

I. Onde apropriado, os papéis (relatórios) e mídia eletrônica devem ser devidamente armazenados e quando não estiverem em uso, especialmente fora do horário do expediente;

II. Computadores de propriedade do município não devem ser deixados desbloqueados quando não houver um operador (usuário) junto, devendo ser protegidos por senhas e outros controles quando não estiverem em uso;

III. Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;

IV. Nunca deixar documentos impressos por longos períodos na impressora. Procure adotar a prática de buscar a impressão logo em seguida e;

V. Não deixe papéis, livros ou qualquer informação na sua mesa quando não estiver no local e, ao final do dia ou no caso de ausência prolongada limpar a mesa de trabalho.

Art. 27. É responsabilidade de todos os agentes públicos e prepostos de pessoa jurídica contratada manter sigilo de informações relacionadas a ocorrências de segurança que venham a ter conhecimento em razão do exercício de suas atividades, tanto em âmbito interno quanto externo, excetuando-se a divulgação aos seus gestores, unidades gestoras pertinentes e áreas de segurança.

Art. 28. Fica vedada a utilização de documentos que contenham qualquer tipo de dado pessoal atrelado Geral de Proteção de Dados como forma de rascunho, devendo todos os papéis que contenham informações que se enquadrem nessa lei serem descartados, preferencialmente por fragmentadoras ou equipamentos próprios para esta finalidade. Se enquadram na categoria de dados pessoais aqueles que possam identificar uma pessoa natural, dentre eles:

I. Nome;
II. RG;
III. CPF;
IV. Gênero;
V. Data e local de nascimento;
VI. Telefone;
VII. Endereço residencial;
VIII. Localização via GPS;
IX. Retrato em fotografia;
X. Prontuário de saúde;
XI. Cartão bancário;
XII. Renda;
XIII. Histórico de pagamentos;
XIV. Hábitos de consumo;
XV. Preferências de lazer e;
XVI. Endereço de IP (protocolo da internet).

Seção II
Do agente público em regime de exceção (temporários)

Art. 29. Os agentes em regime de exceção devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto neste Decreto.

Art. 30. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o agente público que o recebeu não estiver cumprindo as condições definidas neste Decreto.

Art. 31. É de responsabilidade dos parceiros e terceirizados observar as diretrizes desta Política, no que couber.

Seção III
Dos Diretores e Chefias

Art. 32. Os diretores e chefias da Administração Direta Municipal devem:

I. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os agentes públicos e prepostos de pessoa jurídica contratada sob a sua gestão;

II. Atribuir aos agentes públicos e prepostos de pessoa jurídica contratada na fase de admissão, a ciência e responsabilidade quanto ao cumprimento deste Decreto;

III. Exigir dos agentes públicos e prepostos de pessoa jurídica contratada, antes de conceder acesso às informações do Poder Executivo, a assinatura do Termo de Responsabilidade da Política de Segurança da Informação;

IV. Adequar os procedimentos e processos sob sua responsabilidade para atender a esta Política de Segurança da Informação;

V. Comunicar ao Comitê de Segurança da Informação qualquer evento que viole esta Política e;

VI. Na ocorrência de afastamento, exoneração, demissão ou transferência, a chefia imediata deverá prontamente comunicar a Secretaria de Planejamento, que fará a revisão imediata dos direitos de acesso

Parágrafo único. A mesma conduta se aplica aos prepostos de pessoa jurídica contratada cujo contrato ou prestação de serviços tenha se encerrado.

CAPÍTULO VII
DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Artigo 33. A Secretaria Municipal de Planejamento - SEPLAN é o órgão competente para a gestão e coordenação dos assuntos relacionados a área de tecnologia da informação e deve definir normas e regras para o bom funcionamento do parque tecnológico e dos serviços digitais de modo a garantir boas práticas para a sua compatibilidade, integração, integridade e, acima de tudo, para a segurança cibernética.

§ 1º. As normas e regras citadas no caput deste artigo devem ser observadas pelos setores de tecnologia dos demais órgãos da Administração Municipal, inclusive em suas relações com terceiros ou empresas contratadas.

§ 2º. A Comissão Municipal de Tecnologia da Informação – CMTI é a instância para dirimir divergências e deliberar sobre casos omissos relacionados a matéria.

Art. 34. Compete à Área de Tecnologia da Informação:

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

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

III. Configurar os equipamentos, ferramentas e sistemas concedidos aos agentes públicos e prepostos de pessoa jurídica contratada com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por este Decreto e pelas Normas de Segurança da Informação complementares;

IV. Realizar as configurações de backup e restauração de dados digitais, de acordo com o ANEXO V desde decreto, visando a segurança, proteção e disponibilidade dos dados digitais custodiados pelas unidades de tecnologia da informação (TI) e formalmente definidos como de necessária salvaguarda no Município;

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

VI. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

VII. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes;

VIII. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

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

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

XI. Proteger continuamente todos os ativos de informação do município contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malici indesejado;

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

XIII. O acesso às bases de dados dos sistemas em produção deve ser realizado somente pelas aplicações de produção ou pelos técnicos responsáveis pela manutenção dos bancos de dados;

XIV. Garantir o atendimento às regras formais para instalação de software e hardware em ambiente de produção, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da Administração Direta Municipal.

XV. Realizar auditorias periódicas de configurações técnicas e análise de riscos;

XVI. Garantir, após solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Administração.

XVII. Definir e manter as estratégias para acesso e uso seguro da internet e redes sociais, supervisionando as unidades da Administração Direta em relação à identificação, avaliação e mitigação do risco relacionado à segurança da informação.

Art. 35. A área de Tecnologia da Informação deverá monitorar o ambiente de TI, gerando indicadores e históricos de:

I. Uso da capacidade instalada da rede e dos equipamentos;

II. Tempo de resposta no acesso à internet e aos sistemas críticos da Administração Direta;

III. Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Administração Direta;

IV. Incidentes de segurança como vírus, trojans, furtos, acessos indevidos e outros similares e;

V. Atividade de todos os usuários durante os acessos às redes externas, tais como: sites visitados, e-mails recebidos ou enviados, upload ou download de arquivos, entre outros.

CAPÍTULO VIII
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 36. Todos os ativos e serviços de informação, recursos computacionais do Município, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, são de uso exclusivo para fins relacionados ao trabalho, e estão sujeitos à monitoramento.

Art. 37. Para garantir as regras mencionadas neste Decreto, o Poder Executivo poderá:

I. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede e de seu parque tecnológico. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, determinação do Secretário da pasta (ou superior) ou por solicitação justificada do Comitê de Segurança da Informação;

III. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

IV. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e perímetros de acesso e;

V. Utilizar mecanismos de prevenção e detecção de intrusão, prevenção de vazamento de informações, rastreabilidade, criptografia, proteção contra softwares maliciosos, controles de acesso e segmentação da rede de computadores, com o objetivo de reduzir a vulnerabilidade do município a incidentes cibernéticos.

CAPÍTULO IX
E-MAIL INSTITUCIONAL

Art. 38. O uso do e-mail institucional é obrigatório para fins corporativos e relacionados às atividades do agente público ou preposto de pessoa jurídica contratada dentro da Administração Direta Municipal, devendo o mesmo zelar pela imagem perante parceiros e munícipes;

Art. 39. O e-mail institucional é de propriedade da Administração Direta Municipal e instrumento de utilização exclusiva para atendimento do serviço público.

Art. 40. A senha pessoal, embora seja um elemento de segurança individual, não confere uma expectativa de privacidade ao usuário em relação ao e-mail institucional. Sua principal função é proteger a Administração Direta Municipal, servindo como uma barreira para prevenir o acesso não autorizado ao conteúdo das mensagens por terceiros que não sejam de confiança.

Art. 41. A veiculação de dados pessoais e sensíveis em e-mail institucional deverá observar os princípios e diretrizes estabelecidos através da Lei Federal nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados – LGPD, regulamentada pelo Decreto Municipal nº 7.729 de 22 de dezembro de 2022 e demais regramentos congêneres, devendo estar limitada à necessidade e finalidade necessária para cumprimento das atribuições legais do serviço público.

Art. 42. É proibido aos agentes públicos e prepostos de pessoa jurídica contratada no uso do e-mail

institucional da Administração Direta Municipal:

I. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do município e em conformidade com a Lei Federal nº 13.709/2018 (LGPD);

II. Enviar mensagem por e-mail institucional pelo endereço de outro setor que não aquele ao qual está lotado ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

III. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

IV. Apagar mensagens de e-mail institucional quando qualquer uma das unidades do Poder Executivo estiver sujeita a algum tipo de investigação e;

V. Produzir, transmitir ou divulgar mensagem que:

a). Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Administração Direta Municipal;

b). Contenham ameaças eletrônicas, como: spam, mail bombing, vírus de computador entre outros;

c). Vise obter acesso não autorizado a outro computador, servidor ou rede;

d). Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

e). Vise burlar qualquer sistema de segurança;

f). Vise vigiar secretamente ou assediar outro usuário;

g). Vise acessar informações confidenciais sem explícita autorização do proprietário;

h). Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

i). Inclua imagens criptografadas ou de qualquer forma mascaradas;

j). Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

k). Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental;

l). Tenha fins de propaganda partidária e eleitoral em geral e;

m). Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Art. 43. As mensagens de e-mail institucional deverão incluir assinatura com o seguinte formato:
I. Nome do agente público ou preposto de pessoa jurídica contratada;
II. Gerência ou setor;
III. Município da Estância Balneária de Praia Grande;
IV. Telefone(s);
V. Mensagem sobre uso indevido de informações: “As informações contidas nesse e-mail, bem como em qualquer dos seus arquivos anexos, podem conter restrições de divulgação classificadas como confidenciais e são direcionadas exclusivamente a seus destinatários. É vedado o uso, reprodução, divulgação ou distribuição por pessoas diversas aos destinatários ou para fins diferentes daqueles informados originalmente. Caso você não seja o destinatário correto para o recebimento desta mensagem, notifique o remetente e em seguida exclua e destrua permanentemente seu conteúdo”.

CAPÍTULO X
INTERNET

Art. 44. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Administração Direta Municipal, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Art. 45. Toda tentativa de alteração dos parâmetros de segurança, por qualquer agente público ou preposto de pessoa jurídica contratada, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao agente público ou preposto de pessoa jurídica contratada e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos o Município cooperará ativamente com as autoridades competentes.

Art. 46. Os agentes públicos ou prepostos de pessoa jurídica contratada com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades e deverão possuir a licença e registro desses programas.

Art. 47. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo Departamento de Informática.

Art. 48. O download e a utilização de programas e páginas web de entretenimento, jogos ou músicas em qualquer formato poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, uma solicitação formal e justificada deve ser realizada e encaminhada ao Departamento de Informática para liberação de acesso, instalação e demais permissionamentos necessários. Após análise e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvi de jogos.

Art. 49. Os agentes públicos ou prepostos de pessoa jurídica contratada não poderão utilizar os recursos do Município para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Art. 50. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e similares) e aplicativo de acesso remoto (Team Viewer, AnyDesk e similares) não autorizados pela Secretaria de Planejamento não serão permitidos.

Art. 51. Serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos devidamente autorizados e que possuam atribuição correlata.

Art. 52. Serviços de comunicação instantânea são disponibilizados aos usuários para fins corporativos do município, podendo ser bloqueados caso a chefia imediata requisite formalmente à Secretaria de Planejamento.

Art. 53. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada ou ferramentas aprovadas pelo Departamento de Informática, após as devidas autorizações.

§1º. A autorização prevista no caput deste artigo deverá ser concedida pelo secretário municipal responsável pelo agente público ou preposto requisitante.

§2º. O servidor ou preposto que necessitar utilizar de acesso remoto deverá ler e assinar o Termo de Responsabilidade para Utilização de Acesso Remoto (ANEXOS III e IV respectivamente), visando garantir a confidencialidade, sigilo e privacidade das chaves de acesso, bem como, dar ciência acerca da necessidade de infraestrutura para acesso e do monitoramento durante a conexão.

§3º. As credenciais de acesso remoto serão periodicamente revalidadas pela Secretaria de Planejamento, visando garantir a revogação de acessos que não sejam mais necessários.

Art. 54. Não é permitido acesso a sites de proxy.

CAPÍTULO XI
IDENTIFICAÇÃO

Art. 55. Todos os meios de identificação utilizados no Município, como o número de registro do agente público ou preposto de pessoa jurídica contratada, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente ao Cadastro de Pessoas Físicas – CPF.

§ 1º O disposto no caput deste artigo não se aplica a logins de serviço.

§ 2º É proibido o compartilhamento de dispositivos de identificação pessoal.

Art. 56. O usuário, vinculado a dispositivos identificadores, será responsável pelo seu uso correto perante o Município.

Art. 57. É proibido o compartilhamento de login para funções de administração de sistemas.

Art. 58. A Secretaria de Planejamento responde pela criação da identidade lógica dos agentes públicos e prepostos de pessoa jurídica contratada no município, nos termos do procedimento para gerenciamento de contas de grupos e usuários.

§ 1º Os sistemas desenvolvidos pela Administração Direta Municipal a partir da vigência deste decreto deverão possuir autenticação através de CPF e senha, por ferramenta de desenvolvimento próprio ou de código livre.

§ 2º A ferramenta referida no §1º deste artigo deve garantir a integridade, confidencialidade e disponibi dos dados cadastrados.

§ 3º Sistemas em produção que não possuam sua autenticação mediante ferramenta mencionada no § 1º deste artigo deverão ser adequados, substituídos ou contratados em até 4 anos a partir da vigência deste decreto.

§ 4º Casos omissos ou de inviabilidade técnica deverão ser deliberados pela Comissão Municipal de Tecnologia da Informação – CMTI.

Art. 59. A contratação de novos sistemas deverá conter cláusula acerca da obrigatoriedade de integração de dados, incluindo a autenticação de acesso, quando aplicável.

Art. 60. Para utilização dos recursos de TI da Administração Direta Municipal será sempre necessária a autenticação do agente público ou preposto de pessoa jurídica contratada, mediante credencial de acesso.

Art. 61. As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função.

Parágrafo Único. A atribuição de permissões de administrador e/ou root é reservada exclusivamente aos usuários devidamente autorizados pela Secretaria de Planejamento, sendo essas permissões concedidas somente quando estritamente necessárias para o desempenho de suas responsabilidades específicas dentro do contexto operacional estabelecido.

Art. 62. Devem ser distintamente identificados os visitantes, agentes públicos e prepostos de pessoa jurídica contratada.

Art. 63. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha.

Art. 64. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e

a guarda dos dispositivos de identificação que lhe forem designados.

Art. 65. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome do município, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Art. 66. É obrigatório que os usuários modifiquem imediatamente sua senha se houver qualquer suspeita de que terceiros possam ter obtido acesso às suas credenciais de login.

Parágrafo Único. Em situações de suspeita de acesso não autorizado é necessário comunicar à Secretaria de Planejamento para análise e providências necessárias.

Art. 67. Toda informação de dados pessoais será tratada de acordo com os princípios legais aplicáveis, em especial a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem.

CAPÍTULO XII
COMPUTADORES E RECURSOS TECNOLÓGICOS

Artigo 68. Para fins de preservar a disponibilidade, regularidade, integridade, e segurança da rede de dados, é vedada qualquer ação que cause prejuízo ou indisponibilidade de conectividade ou de serviços, dentre elas:

I. Interferências em cabeamentos, conectores e demais dispositivos de conectividade;
II. Instalação ou utilização de dispositivos ou equipamentos não autorizados e desconformes aos padrões estabelecidos por Seplan e sua conexão à rede;
III. Interrupção intencional, monitoração, bloqueio e desligamento de recursos, serviços, servidores ou rede de computadores por pessoas ou métodos não autorizados;
IV. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
V. Burlar quaisquer sistemas de segurança;
VI. Acessar informações confidenciais sem explícita autorização do proprietário;
VII. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

Parágrafo único. Detectada irregularidade ou desconformidade, será aberto processo de apuração de responsabilidades.

Art. 69. Os agentes públicos e prepostos de pessoa jurídica contratada devem informar à Secretaria de Planejamento qualquer identificação de dispositivo estranho conectado à rede corporativa do Poder Executivo.

Art. 70. É vedado todo procedimento de abertura, manutenção física ou lógica, configuração ou modificação em computadores ou demais equipamentos de informática, exceto por servidores com atribuições específicas na área ou por terceiros contratados para essa finalidade.

§ 1º. Estagiários da área de Sistemas de Informação poderão realizar as atividades mencionadas no caput, desde que sob a supervisão direta de um servidor com competência técnica compatível.

§ 2º. A instalação e desinstalação de softwares poderá ser efetuada por usuários que tenham sido previamente habilitados pelo Departamento de Informática.

Art. 71. É proibido o uso dos recursos de Tecnologia da Informação para conduzir negócios estranhos às suas funções profissionais, realizar atividades para fins de ganhos pessoais, propaganda pessoal, angariar ou promover causas religiosas, políticas, comerciais ou qualquer outra atividade incompatível com as atividades institucionais.

Art. 72. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente

poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Art. 73. Os computadores devem possuir versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no Sistema de Apoio ao Usuário.

Art. 74. Arquivos pessoais ou não pertinentes ao serviço público (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem prévio aviso.

Art. 75. Documentos imprescindíveis para as atividades dos agentes públicos deverão ser salvos em drives de rede. Arquivos gravados apenas localmente nos computadores não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo responsabilidade do próprio usuário.

Art. 76. Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de pessoas não autorizadas. Tais senhas serão definidas por servidores com atribuições específicas na área, que terão acesso a elas para manutenção dos equipamentos.

Art. 77. O agente público ou preposto de pessoa jurídica contratada deverá manter a configuração do equipamento disponibilizado seguindo os devidos controles de segurança exigidos pela PSI e pelas normas específicas do Município, assumindo a responsabilidade como custodiante de informações.

Art. 78. Todos os recursos tecnológicos adquiridos devem ter imediatamente suas senhas padrões (default) alteradas.

Art. 79. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos agentes públicos e prepostos de pessoa jurídica contratada, datas e horários de acesso.

CAPÍTULO XIII
DISPOSITIVOS MÓVEIS

Art. 80. Entende-se por “dispositivo móvel” qualquer equipamento eletrônico com atribuições de mobilidade de propriedade do município, ou aprovado e permitido pelo Departamento de Informática, como notebooks e smartphones.

Art. 81. A Administração Direta Municipal, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

Art. 82. O suporte técnico aos dispositivos móveis e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pelo município.

Art. 83. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs.

Art. 84. O agente público ou preposto de pessoa jurídica contratada deverá responsabilizar-se em manter ou utilizar quaisquer programas ou aplicativos, em dispositivo de propriedade do Poder Executivo Municipal, que não tenham sido instalados ou autorizados pelo Departamento de Informática do Município.

Art. 85. É responsabilidade do agente público ou preposto de pessoa jurídica contratada, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Poder Executivo, notificar imediatamente seu gestor direto e o Departamento de Informática. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência.

Art. 86. O agente público ou preposto de pessoa jurídica contratada deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à

Administração Direta Municipal ou a terceiros.

Art. 87. Equipamentos portáteis, como smartphones e demais dispositivos móveis quando não previamente aprovados pelo Departamento de Informática, não serão validados para uso e conexão em sua rede corporativa.

CAPÍTULO XIV
POLÍTICA DE CONTROLE E ACESSO AO DATA CENTER

Art. 88. A Segurança Física dos Data Centers tem como objetivos específicos:

I. Proteger edificações e equipamentos;
II. Prevenir perda, dano ou comprometimento dos ativos de rede;
III. Manter a continuidade das atividades institucionais; e
IV. Prevenir as ameaças que coloquem em risco o bom funcionamento dos sistemas.
Art. 89. Dada a criticidade dos Data Centers, o acesso às suas infraestruturas e aos seus sistemas deve ser totalmente controlado mediante credenciais, por profissionais com perfil técnico adequado.

§ 1º. Todo o acesso aos Data Centers deverá ser registrado (usuário, data e hora) em software de autenticação ou na falta deste, através de formulário próprio.

§ 2º. Os acessos de visitantes e terceiros aos Data Centers somente poderão ser realizados com expressa autorização do Departamento de Informática ou do Departamento de Integração da Informação, com acompanhamento de um membro do mesmo.

§ 3º. O registro do acesso ficará armazenado em log pelo período de 60 dias para posterior consulta e auditorias necessárias.

§ 4º. O controle de acesso deverá ser complementado por circuito fechado de TV nas áreas considerada estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão ser armazen em mídias, de forma que as imagens possam ser resgatadas em caso de ocorrência ou auditoria.

§ 5º. Deverão existir ao menos duas cópias de chaves das portas dos Data Centers. Uma das cópias ficará de posse do Departamento de Informática, outra de posse do Departamento de Integração da Informação.

Art. 90. O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, poderá ser feito somente com autorização por escrito do Departamento de Informática ou do Departamento de Integração da Informação e mediante supervisão.

Art. 91. Deverá ser indicada uma pessoa responsável pela execução do serviço dentro do Data Center para o devido cadastro no sistema de acesso. Esse acesso deverá ser validado pela chefia imediata do servidor responsável juntamente com o Departamento responsável pelo Data Center toda vez que for necessário o acesso, incluindo também os serviços de rotina.

Parágrafo único. O acesso aos Data Centers sem identificação prévia só poderá ocorrer em situações de emergência, quando a segurança física dos Data Centers estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Art. 92. A gestão e controle de acesso aos Data Centers serão efetuados pela Secretaria de Planejamento.

Art. 93. A permissão para o acesso remoto aos servidores do Poder Executivo Municipal será fornecida pelo Departamento de Informática e Departamento da Integração da Informação, os quais deverão ter o controle sobre os acessos visando o acompanhamento dos trabalhos e execução adequada das sessões remotas.

Art. 94. É proibido nas instalações físicas dos Data Centers:

I. Armazenar ou depositar elementos estranhos ao funcionamento dos Data Centers;
II. Utilizar o espaço para depósito ou guarda de inservíveis;

III. Realizar o acesso com algum tipo de alimento, líquido, produto fumígeno ou inflamável.

Art. 95. Qualquer ação que gere lixo ou sujeira no ambiente dos Data Centers deverá ser seguida por procedimento de limpeza adequado, devidamente autorizado e com produtos obrigatoriamente não inflamáveis e limpeza a seco.

Art. 96. A entrada ou retirada de qualquer equipamento dos Data Centers se dará com o preenchimento da solicitação de liberação e autorização formal deste instrumento pelo Departamento de Informática ou pelo Departamento de Integração da Informação, conforme o caso.

§ 1º. No caso de baixa patrimonial de qualquer equipamento o instrumento a ser utilizado para retirada será a guia de transferência patrimonial disponibilizada na intranet pela Secretaria de Administração.

§ 2º. Para equipamentos em garantia a empresa terceirizada deverá assinar uma declaração de retirada confeccionada em documento oficial onde constarão os seguintes dados:

I. Número de Patrimônio;
II. Descrição do Equipamento;
III. Modelo;
IV. Número de série;
V. Defeito e;
VI. Data de retirada.

Art. 97. Os Data Centers devem ser dotados de um sistema de geração de energia elétrica em standby (com redundância) com nobreaks, geradores e baterias, capazes de fornecer energia elétrica de qualidade e suprir toda a necessidade dos Data Centers em caso de falha no fornecimento externo de energia.

Art. 98. No ambiente do Nobreak deve haver:

I. Adequada refrigeração, evitando assim a sobrecarga térmica e desligamento dos equipamentos;

II. Sistema de nobreaks em módulos individuais ou em grupos paralelos com um banco de baterias que pode ser fornecido para cada módulo ou para um grupo de módulos.

Parágrafo único. O banco de baterias, deverá ser substituído de acordo com a estimativa de vida útil do fabricante.

Art. 99. O abastecimento do gerador deve ocorrer conforme normas técnicas vigentes e com o acompanhamento de um técnico do setor responsável pelo gerador.

Art. 100. O gerador deve estar configurado para atender a carga total dos equipamentos alocados nos Data Centers.

Parágrafo único. O gerador deve ter a disponibilidade de atender o mínimo necessário de aparelhos de ar-condicionado de cada Data Center para não ocorrer o shutdown térmico dos servidores.

Art. 101. Os Nobreaks deverão ter a capacidade mínima de fornecimento de energia de 5 a 30 minutos, de acordo com a carga, devido a eventos imprevisíveis que possam ocasionar falhas nos geradores.

Art. 102. A estrutura dos Nobreaks deve possuir um sistema de monitoramento capaz de identificar a capacidade atual de armazenamento das baterias e gravar as tensões, impedância, ou resistência que passam para o sistema de UPS.

Art. 103. O grupo-gerador e nobreaks deverá contar com manutenção preventiva e corretiva para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante.

Art. 104. Os Data Centers devem conter mecanismos de prevenção e combate a incêndios com vistas a evitar

e prevenir que os equipamentos sejam danificados.

Parágrafo único. O sistema de combate e prevenção contra incêndios deve ser composto por sistema de detecção de fumaça e extintores, gases inibidores e procedimentos de brigada de incêndio, observando-se as normas legais do Corpo de Bombeiro.

Art. 105. Os Data Centers deverão estar protegidos por um sistema contra descargas atmosféricas (para-raios) os quais possuam sistema de aterramento eficiente, observando-se o seguinte:

I. Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente;

II. O projeto, instalação e manutenção do sistema devem estar em conformidade com a norma NBR-5419-2015 e;

III. Recomenda-se a utilização de protetores para os equipamentos considerados essenciais.

Art. 106. As salas de Data Centers devem possuir iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade.

Art. 107. Os Diretores do Departamento de Informática e Departamento da Integração da Informação são responsáveis por fazer cumprir as regras relativas à Política de Controle e Acesso ao Data Center.

CAPÍTULO XV
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 108. Fazem parte integrante deste decreto os seguintes anexos:

I. ANEXO I - Termo de Responsabilidade da Política de Segurança da Informação;
II. ANEXO II – Termo de Responsabilidade da Política de Segurança da Informação para Preposto;
III. ANEXO III – Termo de Responsabilidade para Utilização de Acesso Remoto;
IV. ANEXO IV – Termo de Responsabilidade para Utilização de Acesso Remoto para Preposto e;
V. ANEXO V – Política de Backup e Restauração de Dados Digitais.

Art. 109. As propostas de alteração ou criação de normas internas sobre PSI deverão ser encaminhadas ao Comitê de Segurança da Informação.

Art. 110. A PSI deverá ser revisada e atualizada a cada 4 anos ou sempre que eventos ou mudanças significativas relativas ao tema assim o exigirem.

Art. 111. Ações que violem está PSI ou quaisquer de suas diretrizes, normas e procedimentos serão devidamente apuradas e aos responsáveis poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

Art. 112. Os casos omissos e as dúvidas surgidas na aplicação desta PSI serão dirimidos pelo Comitê de Segurança da Informação.

Art. 113. Fica revogado o Decreto nº. 7.737, de 29 de dezembro de 2022.

Art. 114. Este Decreto entra em vigor na data de sua publicação.

Palácio São Francisco de Assis, Prefeitura da Estância Balneária de Praia Grande, aos 29 de novembro de 2024, ano quinquagésimo oitavo da emancipação.

ENG. RAQUEL AUXILIADORA CHINI
PREFEITA

Gremacia Barbosa Pinheiro Salim
Secretária Municipal de Governo

Registrado e publicado na Secretaria de Administração, aos 29 de novembro de 2024.

Ruy Ferraz Fontes
Secretário Municipal de Administração

Processo nº. 26019/2024

.:: Clique aqui e visualize o aquivo anexo ::.

N°	Tipo	Ementa
7737	Decreto	Institui a Política Municipal de Segurança da Informação – PSI, do Município da Estância Balneária de Praia Grande. **(REVOGADO PELO DECRETO N.º 8109, DE 29 DE NOVEMBRO DE 2024)**