DIÁRIO OFICIAL
MUNICÍPIO DE BOCAINA

Conforme Lei Municipal nº 2.774, de 08 de março de 2018

www.bocaina.sp.gov.br | www.imprensaoficialmunicipal.com.br/bocaina

SUMÁRIO

Poder Executivo 2
Atos Oficiais 2
Decretos 2
Portarias 59

EXPEDIENTE

O Diário Oficial do Município de Bocaina, veiculado exclusivamente na forma eletrônica, é uma publicação das entidades da Administração Direta e Indireta deste Município, sendo referidas entidades inteiramente responsáveis pelo conteúdo aqui publicado.

ACERVO

As edições do Diário Oficial Eletrônico de Bocaina poderão ser consultadas através da internet, por meio do seguinte endereço eletrônico: www.bocaina.sp.gov.br
Para pesquisa por qualquer termo e utilização de filtros, acesse www.imprensaoficialmunicipal.com.br/bocaina
As consultas e pesquisas são de acesso gratuito e independente de qualquer cadastro.

ENTIDADES

Prefeitura Municipal de Bocaina
CNPJ 44.498.988/0001-36
Rua 7 de Setembro, 177
Telefone: (14) 3666-8000
Site: www.bocaina.sp.gov.br
Diário: www.imprensaoficialmunicipal.com.br/bocaina

Câmara Municipal de Bocaina
CNPJ 49.895.410/0001-37
Rua Floriano Peixoto, 498
Telefone: (14) 3666-1555
Site: www.camarabocaina.sp.gov.br

Diário Oficial Assinado Eletronicamente com Certificado Padrão ICPBrasil, em conformidade com a MP nº 2.200-2, de 2001

O Município de Bocaina garante a autenticidade deste documento, desde que visualizado através do site www.bocaina.sp.gov.br

Compilado e também disponível em www.imprensaoficialmunicipal.com.br/bocaina

Prefeitura Municipal de Bocaina

Estado de São Paulo

DECRETO Nº 098/25

Dispõe sobre a homologação da Política Municipal de Segurança da Informação e do Plano de Continuidade de Serviços no âmbito da Administração Pública Municipal de Bocaina – Estado de São Paulo, e dá outras providências.

O Prefeito do Município de Bocaina, Estado de São Paulo, no uso de suas atribuições legais;

CONSIDERANDO que a informação constitui ativo essencial para a gestão pública, devendo ser tratada com segurança, integridade e disponibilidade em conformidade com os princípios constitucionais da legalidade, moralidade, publicidade e eficiência;

CONSIDERANDO a necessidade de estabelecer diretrizes, responsabilidades e controles para a proteção de dados, sistemas e ativos tecnológicos da Administração Pública Municipal;

CONSIDERANDO o disposto na Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que impõe aos órgãos públicos o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais sob seu tratamento;

CONSIDERANDO o disposto na Lei Federal nº 14.129/2021 (Lei do Governo Digital), que determina a adoção de padrões de segurança da informação, interoperabilidade e continuidade dos serviços públicos digitais;

CONSIDERANDO o Decreto Federal nº 9.637/2018, que institui a Política Nacional de Segurança da Informação e estabelece diretrizes para os entes federados;

CONSIDERANDO as normas internacionais ABNT NBR ISO/IEC 27001:2022 (Sistema de Gestão da Segurança da Informação) e ABNT NBR ISO 22301:2020 (Gestão da Continuidade de Negócios), que servem de referência para boas práticas de governança pública;

CONSIDERANDO, por fim, a necessidade de formalizar e garantir eficácia à Política de Segurança da Informação e ao Plano de Continuidade de Serviços elaborados pela Prefeitura Municipal de Bocaina;

DECRETA:

Art. 1º Ficam homologados e instituídos, no âmbito da Administração Pública Municipal de Bocaina – Estado de São Paulo, a Política de Segurança da Informação (PSI) e o Plano de Continuidade de Serviços (PCS), conforme textos anexos a este Decreto.

Art. 2º A Política de Segurança da Informação tem como finalidade estabelecer princípios, diretrizes, responsabilidades e controles voltados à proteção das informações, sistemas e dados sob guarda da Prefeitura Municipal,

assegurando a confidencialidade, integridade, disponibilidade e autenticidade das informações públicas e pessoais.

Art. 3º O Plano de Continuidade de Serviços (PCS) tem por objetivo garantir a manutenção ou rápida retomada das atividades essenciais da administração pública em caso de incidentes, falhas, desastres ou ataques cibernéticos, assegurando a continuidade das operações críticas e o atendimento à população.

Art. 4º A execução e acompanhamento da Política e do Plano referidos neste Decreto serão coordenados pelo Comitê Municipal de Segurança da Informação e Proteção de Dados, que contará com a participação do Coordenador de Tecnologia da Informação, do Encarregado de Dados (DPO) e dos representantes das Diretorias Municipais.

Parágrafo único. O Comitê deverá adotar as providências necessárias à implementação, revisão periódica e atualização dos documentos homologados por este Decreto.

Art. 5º Compete ao Coordenador de Tecnologia da Informação:

I – implementar as medidas técnicas previstas na Política e no Plano;

II – manter atualizados os controles de acesso, os mecanismos de backup e recuperação de dados;

III – garantir a segurança física, lógica e operacional da infraestrutura tecnológica municipal.

Art. 6º Os Diretores Municipais e dirigentes de autarquias e fundações deverão:

I – assegurar o cumprimento das normas estabelecidas na Política e no Plano;

II – indicar ponto focal de segurança da informação em suas unidades;

III – apoiar a execução das ações de capacitação, auditoria e conscientização sobre segurança da informação.

Art. 7º A Política de Segurança da Informação e o Plano de Continuidade de Serviços deverão constar nas minutas de editais e contratos oriundos de processos licitatórios de contratação de serviços de TI, notadamente licenciamento de sistemas informáticos.

Art. 8º Todos os servidores, estagiários, colaboradores e prestadores de serviço que utilizem sistemas, equipamentos ou informações sob responsabilidade da Prefeitura estão sujeitos às disposições da Política de Segurança da Informação e do Plano de Continuidade de Serviços.

Parágrafo único. O descumprimento das normas estabelecidas poderá ensejar responsabilização administrativa, civil e penal, conforme a legislação aplicável.

Art. 9º Comitê de Segurança da Informação deverão elaborar relatórios anuais de auditoria e conformidade sobre a aplicação desta Política, apresentando recomendações de melhoria contínua à Alta Administração.

Prefeitura Municipal de Bocaina

Estado de São Paulo

Art. 10. O conteúdo integral da Política de Segurança da Informação e do Plano de Continuidade de Serviços deverá ser disponibilizado no Portal da Transparência e comunicado a todos os órgãos e servidores da Prefeitura.

Parágrafo único: os contratos em vigor deverão ser aditados e os prestadores de serviço devidamente notificados do cumprimento deste decreto e seus anexos.

Art. 11. Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Bocaina, em 29 de dezembro de 2.025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrado na Secretaria, na data acima.

Denise Chotti
Agente Administrativo

Prefeitura Municipal de Bocaina

Estado de São Paulo

PSI – Política de Segurança da Informação

Município de Bocaina - Estado de São Paulo

Capítulo 1 – Introdução e Objetivo

1.1 Introdução

A Prefeitura Municipal de Bocaina – Estado de São Paulo, no exercício de suas competências administrativas e constitucionais, reconhece que a informação é um ativo estratégico essencial à gestão pública, à transparência e à continuidade dos serviços prestados à população.

Com a crescente digitalização dos processos e a adoção de sistemas eletrônicos de gestão, torna-se imprescindível garantir que as informações institucionais e pessoais sejam tratadas com segurança, confidencialidade, integridade e disponibilidade, prevenindo acessos indevidos, perdas, vazamentos ou qualquer forma de comprometimento.

Esta **Política de Segurança da Informação (PSI)** estabelece diretrizes, princípios e responsabilidades para proteger os ativos informacionais da Prefeitura, assegurando a conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), com a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), com a Lei nº 14.129/2021 (Lei do Governo Digital), e com o Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação – PNSI).

A adoção desta política tem como referência as normas ABNT NBR ISO/IEC 27001:2022 e 27002:2023, o NIST *Cybersecurity* Framework (CSF), o COBIT 2019 e as boas práticas da Estratégia de Governo Digital (EGD), adaptadas à realidade de um município de pequeno porte.

Ao implementar esta política, a Prefeitura busca criar uma cultura organizacional de segurança, garantindo a proteção das informações em todas as suas formas — digitais, impressas ou orais — e fortalecendo a confiança da sociedade nas ações da administração pública.

1.2 Objetivo

O objetivo desta Política de Segurança da Informação é estabelecer as diretrizes gerais e os princípios de governança da informação, visando proteger os ativos informacionais da Prefeitura e assegurar que o tratamento de dados e informações seja realizado de forma segura, ética e em conformidade com as legislações vigentes.

Em especial, esta política tem por finalidade:

I. Proteger as informações da Prefeitura Municipal contra acessos não autorizados, uso indevido, modificação, destruição ou divulgação indevida;

II. Assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, em conformidade com os princípios da segurança da informação definidos pela ABNT NBR ISO/IEC 27001;

III. Orientar servidores, colaboradores, prestadores de serviço, estagiários e terceiros quanto às práticas adequadas de segurança, uso e proteção de informações e sistemas;

IV. Estabelecer responsabilidades institucionais relacionadas à segurança da informação, incluindo o papel do Coordenador de TI, do Encarregado de Dados (DPO) e dos usuários;

V. Integrar a segurança da informação à governança pública, alinhando-se ao Plano Diretor

de Tecnologia da Informação (PDTI) e à Política de Proteção de Dados Pessoais da Prefeitura;

VI. Promover a conformidade com a legislação aplicável, em especial com a LGPD, a LAI, a Lei do Governo Digital, Marco Civil da Internet e demais normas correlatas;

VII. Fomentar a cultura de segurança e de prevenção de incidentes, por meio de treinamentos, auditorias e revisões periódicas desta política;

VIII. Definir diretrizes para o uso, armazenamento, transmissão, compartilhamento e descarte de informações, garantindo sua proteção em todo o ciclo de vida.

1.3 Abrangência e Escopo

Esta Política aplica-se a todos os órgãos, diretorias, secretarias, departamentos, autarquias e entidades vinculadas à Prefeitura Municipal de Bocaina – Estado de São Paulo, incluindo:

- Servidores públicos efetivos e comissionados;
- Estagiários e colaboradores terceirizados;
- Prestadores de serviços, consultores e empresas contratadas que tratem informações institucionais ou dados pessoais sob responsabilidade da Prefeitura;
- Sistemas, equipamentos, redes, bancos de dados e demais ativos de informação pertencentes ou sob guarda do Município.

1.4 Base Legal e Referências Normativas

A presente política fundamenta-se nos seguintes instrumentos legais e técnicos:

Legislação Brasileira:

- Constituição Federal de 1988 (arts. 5º, 37 e 216);
- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 14.129/2021 – Lei do Governo Digital;
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Decreto nº 10.046/2019 – Compartilhamento de Dados no Poder Público;
- Lei nº 14.063/2020 – Assinaturas Eletrônicas na Administração Pública;
- Marco Civil da Internet – Lei nº 12.965/2014.

Normas e Frameworks Técnicos:

- ABNT NBR ISO/IEC 27001:2022 – Sistema de Gestão da Segurança da Informação (SGSI);
- ABNT NBR ISO/IEC 27002:2023 – Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27701:2021 – Sistema de Gestão de Privacidade da Informação (PIMS);

- NIST Cybersecurity Framework (EUA) – Estrutura de Gerenciamento de Riscos Cibernéticos;
- COBIT 2019 – Governança e Gestão de TI;
- ITIL 4 – Boas práticas de gestão de serviços de TI.

Capítulo 2 – Princípios e Diretrizes de Segurança da Informação

2.1 Princípios Fundamentais

A Política de Segurança da Informação da Prefeitura Municipal de Bocaina – Estado de São Paulo é guiada pelos princípios que norteiam a boa governança da informação, em conformidade com a Constituição Federal, a Lei Geral de Proteção de Dados (LGPD), a Lei de Acesso à Informação (LAI) e as normas internacionais da série ISO/IEC 27000.

Tais princípios orientam todas as ações, decisões e controles relacionados à proteção da informação pública e dos dados pessoais sob guarda do Município.

I. Confidencialidade

Garantir que a informação seja acessada apenas por pessoas, sistemas ou entidades devidamente autorizadas.

➡ Fundamentação: art. 46 da LGPD; controles 5.1.1 e 8.2 da ISO/IEC 27002.

II. Integridade

Assegurar que a informação permaneça exata, completa e não tenha sido alterada de forma indevida, acidental ou maliciosa.

➡ Fundamentação: ISO/IEC 27001, cláusula 6.1.2; art. 6º, VI da LGPD.

III. Disponibilidade

Garantir que a informação e os sistemas que a armazenam estejam acessíveis aos usuários autorizados sempre que necessário, dentro dos níveis de serviço estabelecidos.

➡ Fundamentação: art. 7º da LAI; princípio da continuidade do serviço público.

IV. Autenticidade

Assegurar que a identidade das partes envolvidas no processamento de informação possa ser verificada, e que as informações sejam genuínas.

➡ Fundamentação: Lei nº 14.063/2020 (assinaturas eletrônicas) e ISO/IEC 27002, controle 8.4.

V. Legalidade

Todo tratamento de informação e dado pessoal deve respeitar as leis e regulamentos aplicáveis, especialmente a LGPD e as normas municipais correlatas.

➡ Fundamentação: art. 6º, I e II da LGPD; art. 37 da Constituição Federal.

VI. Ética e Responsabilidade

Servidores e prestadores de serviços devem agir com zelo, lealdade e boa-fé no trato da informação pública e pessoal, mantendo o sigilo quando necessário e respeitando os direitos dos titulares.

➡ Fundamentação: art. 116 da Lei nº 8.112/1990 (aplicável por analogia), e princípios da moralidade e eficiência administrativa.

VII. Transparência e Controle Social

A segurança da informação não deve ser usada como pretexto para restringir o acesso às informações de interesse público.

➡ Fundamentação: art. 5º, XXXIII da Constituição Federal e art. 3º da Lei nº 12.527/2011.

VIII. Responsabilização e Prestação de Contas (Accountability)

Cada servidor, colaborador ou terceiro deve ser responsável pelos atos praticados no tratamento e proteção da informação.

➡ Fundamentação: art. 6º, X da LGPD e art. 8º da Lei nº 14.129/2021 (Governo Digital).

2.2 Diretrizes Gerais de Segurança da Informação

Para assegurar a observância dos princípios acima, esta política estabelece as seguintes diretrizes, aplicáveis a todos os órgãos e entidades da Prefeitura:

Diretriz 1 – Gestão da Informação como Ativo Institucional

Toda informação gerada, recebida ou armazenada pela Prefeitura é considerada ativo público e deve ser protegida conforme sua criticidade e valor para a administração e para a sociedade.

Diretriz 2 – Classificação da Informação

As informações devem ser classificadas quanto ao seu nível de sigilo, valor e impacto em caso de comprometimento, conforme níveis definidos em regulamento específico (por exemplo: pública, restrita, confidencial e sigilosa).

Diretriz 3 – Gestão de Riscos de Segurança

A Prefeitura deverá identificar, avaliar e tratar riscos que possam afetar a segurança da informação, adotando medidas preventivas, corretivas e mitigadoras, compatíveis com sua capacidade operacional e orçamentária.

Diretriz 4 – Conscientização e Capacitação

Todos os servidores, colaboradores e prestadores de serviço devem ser capacitados sobre boas práticas de segurança, privacidade e proteção de dados, com ênfase nas rotinas diárias da administração municipal.

Diretriz 5 – Controle de Acesso e Autenticação

O acesso a sistemas, redes e bancos de dados deverá ser concedido apenas a usuários devidamente autorizados, com base em perfis de acesso definidos e revisados periodicamente.

Diretriz 6 – Continuidade de Negócios

A Prefeitura deve garantir que incidentes ou desastres não comprometam a continuidade dos serviços essenciais, mantendo planos de backup e recuperação regularmente testados.

Diretriz 7 – Gestão de Incidentes de Segurança

Todo incidente de segurança deve ser comunicado imediatamente à unidade de TI e ao Encarregado de Dados, devendo ser registrado, analisado e tratado de acordo com o Plano de Resposta a Incidentes.

Diretriz 8 – Segurança de Terceiros e Contratos

Os contratos com fornecedores e prestadores de serviços que tratem informações ou dados pessoais devem conter cláusulas específicas de confidencialidade, proteção de dados e segurança da informação, incluindo responsabilidades e penalidades.

Diretriz 9 – Auditoria, Monitoramento e Melhoria Contínua

A política e seus controles devem ser auditados periodicamente, com relatórios encaminhados à alta administração, visando à melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI).

Diretriz 10 – Alinhamento com o Governo Digital e a Transparência

As ações de segurança da informação devem estar alinhadas às diretrizes da Lei do Governo Digital (Lei nº 14.129/2021), priorizando soluções tecnológicas seguras, interoperáveis e sustentáveis.

Capítulo 3 – Papéis e Responsabilidades

3.1 Princípio da Responsabilidade Compartilhada

A segurança da informação é responsabilidade de todas as pessoas que tratam informações ou utilizam ativos tecnológicos da Prefeitura Municipal de Bocaina – Estado de São Paulo.

Cada agente público, servidor, colaborador ou prestador de serviço é corresponsável pela proteção das informações sob sua guarda, devendo agir com zelo, ética e observância às normas desta Política.

3.2 Alta Administração Municipal

A Alta Administração – composta pelo Prefeito, Diretores Municipais e dirigentes de autarquias e fundações – possui papel estratégico na governança da segurança da informação.

Compete à Alta Administração:

I. Aprovar esta Política de Segurança da Informação e suas revisões;

II. Garantir que a segurança da informação seja tratada como prioridade institucional, integrando-a aos planos estratégicos da Prefeitura;

III. Designar formalmente os responsáveis pela gestão da segurança da informação e pelo tratamento de dados pessoais;

IV. Assegurar que os recursos humanos, técnicos e financeiros necessários à execução da política sejam providos;

V. Acompanhar periodicamente relatórios de auditoria, risco e conformidade em segurança da informação;

VI. Zelar pelo cumprimento das legislações aplicáveis, especialmente a LGPD, a LAI, a Lei do Governo Digital e o Decreto nº 9.637/2018 (PNSI).

3.3 Comitê Municipal de Segurança da Informação e Proteção de Dados

A Prefeitura instituirá, por ato normativo, um Comitê Municipal de Segurança da Informação e Proteção de Dados, de caráter consultivo e deliberativo.

Compete ao Comitê:

I. Propor normas complementares, manuais e planos específicos de segurança da informação;

II. Avaliar e priorizar ações decorrentes de incidentes de segurança e vazamentos de dados;

III. Acompanhar os indicadores de maturidade de segurança e de governança digital;

IV. Promover a integração entre as unidades de Tecnologia da Informação, Controladoria, Procuradoria Geral, Secretaria de Administração e demais órgãos envolvidos;

V. Emitir pareceres sobre contratos, convênios e parcerias que envolvam tratamento de informações sensíveis ou pessoais.

➡ Fundamentação: arts. 50 e 52 da LGPD; Decreto nº 9.637/2018 (PNSI); Lei nº 14.129/2021 (Governo Digital).

3.4 Gestor de Tecnologia da Informação

O Coordenador de TI é o responsável técnico pela implementação dos controles de segurança e pela administração dos ativos tecnológicos da Prefeitura.

Compete ao Gestor de TI:

I. Implementar e manter o Sistema de Gestão da Segurança da Informação (SGSI) em conformidade com a ISO/IEC 27001;

II. Executar os planos de backup, contingência e recuperação de desastres;

III. Gerir as permissões de acesso a sistemas e redes, assegurando controle, rastreabilidade e revisão periódica;

IV. Monitorar incidentes e vulnerabilidades, adotando medidas corretivas;

V. Elaborar relatórios técnicos de conformidade e apresentar resultados ao Comitê e à Alta Administração;

VI. Orientar fornecedores e prestadores de serviço sobre requisitos mínimos de segurança;

VII. Apoiar o Encarregado de Dados (DPO) nas análises técnicas relacionadas a incidentes e riscos de privacidade.

3.5 Encarregado pelo Tratamento de Dados Pessoais (DPO)

O Encarregado de Dados, designado conforme o art. 41 da LGPD, atua como canal de comunicação entre o Município, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Compete ao DPO:

I. Orientar servidores e gestores sobre as práticas de tratamento de dados pessoais e segurança da informação;

II. Receber e responder comunicações de titulares e da ANPD;

III. Acompanhar e registrar incidentes de segurança envolvendo dados pessoais;

IV. Coordenar a implementação da Política de Proteção de Dados Pessoais e apoiar o Comitê na revisão desta Política;

V. Elaborar relatórios de impacto à proteção de dados pessoais (RIPD), em articulação com o Gestor de TI;

VI. Zelar pela integração entre as práticas de privacidade (ISO/IEC 27701) e de segurança da informação (ISO/IEC 27001).

3.6 Gestores de Diretorias e Unidades Administrativas

Cada Diretoria ou Unidade Administrativa da Prefeitura é responsável pela proteção das informações sob sua gestão.

Compete aos Gestores:

I. Cumprir e fazer cumprir esta Política em sua unidade;

II. Classificar as informações sob sua responsabilidade conforme níveis de sigilo definidos;

III. Designar, quando necessário, um ponto focal para assuntos de segurança da informação;

IV. Garantir que documentos e sistemas estejam devidamente protegidos física e logicamente;

V. Comunicar imediatamente ao Gestor de TI e ao DPO qualquer incidente ou suspeita de violação de dados;

VI. Promover a conscientização de seus servidores e colaboradores.

3.7 Servidores Públicos, Estagiários e Colaboradores

Todos os usuários dos ativos de informação têm responsabilidades individuais no uso ético, seguro e responsável dos recursos tecnológicos da Prefeitura.

Compete a cada usuário:

I. Cumprir as normas desta Política e das demais políticas correlatas contidas nos Termos de Uso dos Sistemas e Termo de Uso da Internet;

II. Zelar pela confidencialidade de senhas e credenciais de acesso;

III. Não compartilhar dados pessoais ou institucionais sem autorização;

IV. Evitar a instalação de softwares não autorizados (comunicando imediatamente o Depto de

II) ou o uso indevido de equipamentos públicos;

V. Reportar imediatamente quaisquer incidentes, erros ou comportamentos suspeitos;

VI. Participar de capacitações e treinamentos oferecidos sobre segurança e proteção de dados.

➡ Fundamentação: art. 116 da Lei 8.112/1990 (aplicável por analogia); arts. 46 e 50 da LGPD; ISO/IEC 27002, controle 6.3.

3.8 Prestadores de Serviço, Fornecedores e Terceiros

Toda empresa contratada que tenha acesso a dados, sistemas, equipamentos ou informações da Prefeitura deve observar esta Política e as cláusulas contratuais específicas de segurança da informação.

Compete aos terceiros:

I. Cumprir as normas de segurança estabelecidas nos contratos e aditivos;

II. Manter confidencialidade sobre todas as informações a que tiver acesso;

III. Adotar medidas técnicas e administrativas compatíveis com o risco da informação tratada;

IV. Comunicar imediatamente incidentes que envolvam dados ou sistemas do Município;

V. Não instalar, em hipótese alguma, softwares que não sejam de sua propriedade, mesmo que se trate de softwares livres;

VI. Submeter-se a auditorias e verificações de conformidade, quando solicitadas.

➡ Fundamentação: art. 39 da LGPD; ISO/IEC 27036 – Segurança em Relacionamentos com Fornecedores.

Capítulo 4 – Gestão de Riscos da Informação

4.1 Conceito e Finalidade

A Gestão de Riscos da Informação é o processo sistemático de identificar, analisar, avaliar, tratar e monitorar eventos que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações da Prefeitura Municipal de Bocaina – Estado de São Paulo.

O objetivo deste processo é reduzir a probabilidade e o impacto de incidentes de segurança, garantindo a continuidade dos serviços públicos, a conformidade legal e a confiança dos cidadãos nos sistemas municipais.

➡ Base normativa:

- ABNT NBR ISO/IEC 27005:2023 – Gestão de Riscos de Segurança da Informação;
- ABNT NBR ISO/IEC 27001:2022 – Cláusula 6.1.2 (Ações para tratar riscos);
- NIST SP 800-37 Rev. 2 e NIST CSF (Identify, Protect, Detect, Respond, Recover);
- Artigos 6º (VII e X) e 46 da LGPD;
- Art. 15 da Lei 14.129/2021 (Lei do Governo Digital).

4.2 Princípios da Gestão de Riscos

A gestão de riscos da informação observará os seguintes princípios:

I. Proporcionalidade: as medidas de controle devem ser compatíveis com o porte do município, a criticidade da informação e a capacidade operacional da Prefeitura.

II. Prevenção: prioriza-se a identificação e mitigação de vulnerabilidades antes da ocorrência de incidentes.

III. Continuidade: os riscos devem ser geridos de forma permanente, como processo cíclico de melhoria contínua.

IV. Responsabilidade Compartilhada: todos os servidores e gestores são corresponsáveis pela identificação e reporte de riscos.

V. Rastreabilidade e Transparência: as decisões e tratamentos de risco devem ser documentados, auditáveis e comunicáveis à Alta Administração.

4.3 Escopo da Gestão de Riscos

A gestão de riscos abrange todos os ativos de informação sob responsabilidade da Prefeitura, incluindo:

- Sistemas corporativos e bancos de dados;
- Equipamentos de informática, redes e servidores;
- Documentos físicos e eletrônicos;
- Dados pessoais e sensíveis tratados por diretorias municipais;
- Processos administrativos que dependem de tecnologia da informação;
- Fornecedores, contratos e terceiros que tratem informações municipais.

4.4 Etapas do Processo de Gestão de Riscos

O processo seguirá o ciclo contínuo previsto na ISO/IEC 27005, adaptado à realidade municipal:

Etapa 1 – Identificação de Ativos e Ameaças

Mapeamento dos ativos de informação e identificação das possíveis ameaças (internas ou externas) que possam comprometer a segurança.

Etapa 2 – Análise de Vulnerabilidades e Impactos

Analisar as vulnerabilidades existentes e os impactos potenciais sobre as operações municipais, classificando-os como baixo, médio ou alto impacto, conforme critérios definidos pelo Comitê de Segurança da Informação.

Etapa 3 – Avaliação de Probabilidade

Avaliar a probabilidade de ocorrência de cada risco com base em histórico de incidentes, nível de exposição e controles existentes.

Etapa 4 – Determinação do Nível de Risco

Combinar probabilidade e impacto para determinar o nível de risco (baixo, moderado, alto ou crítico), utilizando matriz padronizada de risco definida pela unidade de TI.

Etapa 5 – Tratamento do Risco

Definir as ações adequadas:

a) Mitigar: implementar controles que reduzam o risco;

b) Transferir: compartilhar o risco com terceiros (por exemplo, contratos e seguros);

c) Aceitar: aceitar riscos residuais, mediante aprovação da Alta Administração;

d) Evitar: eliminar o risco pela interrupção da atividade que o gera.

Etapa 6 – Monitoramento e Revisão

Monitorar continuamente os riscos, atualizar controles e revisar o plano de gestão conforme mudanças tecnológicas, organizacionais ou legais.

4.5 Responsabilidades pela Gestão de Riscos

I. Alta Administração: aprovar os resultados da avaliação de riscos e prover recursos necessários à mitigação.

II. Comitê Municipal de Segurança da Informação: acompanhar o processo de gestão de riscos, revisar a matriz e propor medidas de controle.

III. Coordenador de TI: implementar controles técnicos, monitorar vulnerabilidades e manter atualizada a base de ativos.

IV. Encarregado de Dados (DPO): acompanhar os riscos relacionados ao tratamento de dados pessoais e elaborar Relatórios de Impacto à Proteção de Dados (RIPD).

V. Gestores de Diretorias: identificar riscos em processos sob sua responsabilidade e adotar medidas preventivas.

VI. Servidores e Colaboradores: reportar incidentes, irregularidades ou suspeitas que possam indicar vulnerabilidades.

4.6 Integração com Outras Políticas Municipais

A gestão de riscos da informação deve estar alinhada a:

- Plano Diretor de Tecnologia da Informação (PDTI);
- Plano de Continuidade de Negócios (PCN);
- Política de Proteção de Dados Pessoais;
- Plano de Transformação Digital;
- Gestão de Riscos Institucionais (em conformidade com orientações do Tribunal de Contas e da Controladoria).

Essa integração assegura coerência entre a proteção de dados, a segurança da informação e os objetivos estratégicos da Prefeitura.

4.8 Revisão e Melhoria Contínua

O processo de gestão de riscos será revisado anualmente, ou sempre que ocorrerem mudanças significativas na infraestrutura tecnológica, no arcabouço legal ou nos processos administrativos.

As revisões deverão considerar:

- Resultados de auditorias internas e externas;
- Ocorrência de incidentes e falhas identificadas;
- Novas ameaças cibernéticas ou tecnológicas;
- Recomendações de órgãos de controle e da ANPD.

Capítulo 5 – Classificação e Tratamento da Informação

5.1 Conceito e Finalidade

A classificação e o tratamento adequado das informações têm como finalidade assegurar a proteção proporcional ao valor, à sensibilidade e ao impacto que o uso, a divulgação, a modificação ou a perda dessas informações possam causar à Prefeitura Municipal de Bocaina/SP, aos cidadãos ou a terceiros.

Toda informação produzida, recebida, armazenada ou transmitida no âmbito da Prefeitura é considerada ativo informacional público e deve ser protegida conforme seu grau de sigilo, valor estratégico e obrigações legais de guarda.

➡ Base normativa:

- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Decreto nº 7.724/2012 – Regulamenta a LAI;
- Lei nº 13.709/2018 – LGPD (arts. 6º, 46 e 50);
- ABNT NBR ISO/IEC 27002:2023 – seção 5.12 (Classificação da Informação);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação (PNSI).

5.2 Princípios de Classificação da Informação

A classificação da informação observará os seguintes princípios:

I. Proporcionalidade: o nível de proteção deve ser compatível com a sensibilidade da informação e o impacto de sua divulgação indevida;

II. Legalidade: a classificação deve respeitar as normas legais sobre transparência, sigilo e proteção de dados pessoais;

III. Temporalidade: as restrições de acesso devem ter prazo definido e revisão periódica;

IV. Rastreabilidade: todo processo de classificação deve ser documentado e identificável quanto à sua origem e responsável;

V. Minimização: apenas as informações estritamente necessárias deverão ser classificadas em níveis restritivos.

5.3 Categorias de Classificação da Informação

As informações sob guarda da Prefeitura Municipal serão classificadas conforme o grau de sigilo e nível de proteção requerido, observando as normas da LAI e do Decreto nº 7.724/2012:

Nível	Denominação	Descrição e Exemplo	Acesso
1. Pública	Informação de livre acesso	Dados e documentos que podem ser divulgados sem restrição. Ex: Relatórios públicos, atas, leis, orçamentos, dados abertos.	Acesso irrestrito.
2. Restrita	Informação interna	Dados cujo acesso é limitado a servidores e gestores da unidade. Ex: memorandos internos, planejamento estratégico, relatórios de TI.	Acesso mediante credencial institucional.
3. Confidencial	Informação sensível ou estratégica	Dados que, se expostos, podem causar danos à segurança institucional, à imagem da administração ou aos interesses públicos. Ex: pareceres jurídicos em andamento, dados financeiros, contratos em fase de licitação.	Acesso restrito a autoridades e servidores autorizados.
4. Sigilosa	Informação classificada em grau de sigilo, conforme LAI	Dados cujo conhecimento não autorizado pode comprometer a segurança da sociedade ou do Estado. Ex: investigações, informações estratégicas, dados de segurança pública.	Acesso controlado e autorizado por autoridade competente, com prazos definidos de restrição (5 a 25 anos).

➡ Observação: o nível "sigiloso" deve ser formalmente designado pela autoridade máxima da Prefeitura, conforme arts. 24 a 27 da LAI e art. 31 do Decreto nº 7.724/2012.

5.4 Tratamento da Informação por Natureza

Além do nível de sigilo, o tratamento da informação deve observar sua natureza e finalidade, em especial no que se refere aos dados pessoais e dados sensíveis, conforme a LGPD:

Tipo de Informação	Tratamento Específico
Dados pessoais	Devem ser tratados com base em uma hipótese legal (art. 7º da LGPD), garantindo segurança, confidencialidade e acesso controlado.
Dados pessoais sensíveis	Exigem proteção reforçada (art. 11 da LGPD), com controles adicionais, registro de acesso e medidas de segurança específicas.
Dados de crianças e adolescentes	O tratamento deve respeitar o melhor interesse da criança (art. 14 da LGPD), com consentimento e controles adicionais de sigilo.
Informações públicas	Devem ser publicadas de forma clara, precisa e acessível, observando o princípio da publicidade e o direito de acesso à informação.
Informações estratégicas ou críticas	Devem ter gestão controlada, uso restrito e plano de contingência em caso de incidente.

5.5 Rotulagem e Identificação da Informação

Toda informação classificada como restrita, confidencial ou sigilosa deve ser devidamente rotulada, identificada e protegida.

A rotulagem deverá conter, no mínimo:

- Grau de sigilo ("Restrita", "Confidencial" ou "Sigilosa");
- Data da classificação;
- Nome e cargo da autoridade classificadora;
- Prazo de revisão da classificação;
- Unidade responsável pela guarda.

Nos documentos eletrônicos, a classificação deve ser registrada no sistema de gestão documental, com controle de permissões e logs de acesso.

➡ Referência técnica: ISO/IEC 27002, controle 5.13 (Rotulagem de informação).

5.6 Armazenamento e Acesso à Informação

I. O armazenamento das informações deverá ser feito em ambientes seguros, com controle físico e lógico de acesso;

II. Sistemas de informação deverão possuir autenticação individual, criptografia e logs de auditoria;

III. Os acessos devem ser concedidos conforme o princípio do menor privilégio e revisados periodicamente;

IV. Documentos físicos classificados devem ser armazenados em armários trancados, salas seguras ou arquivos com controle de acesso;

V. É vedado o transporte de mídias, *pendrives* ou dispositivos com informações institucionais sem autorização formal.

5.7 Compartilhamento e Transferência de Informações

O compartilhamento interno ou externo de informações deve obedecer às seguintes regras:

I. Ser limitado ao mínimo necessário para a execução da atividade pública;

II. Observar as bases legais previstas no art. 7º e art. 26 da LGPD;

III. Nos casos de compartilhamento com outros entes públicos, observar o Decreto nº 10.046/2019;

IV. No caso de envio de dados a operadores (empresas contratadas), exigir contrato específico contendo cláusulas de sigilo e segurança;

V. Toda transferência de informações deve ser registrada, documentada e, quando possível, criptografada.

5.8 Retenção e Descarte de Informações

O descarte de informações deve ocorrer de forma segura, controlada e documentada, observando a legislação arquivística e de proteção de dados.

I. O prazo de guarda das informações seguirá o Plano de Classificação e a Tabela de Temporalidade Documental do Município;

II. Informações com dados pessoais devem ser eliminadas após o término da finalidade, salvo obrigação legal de guarda;

III. O descarte de documentos físicos deverá ser feito por fragmentação, trituração ou incineração controlada;

IV. O descarte de informações digitais deverá ocorrer por eliminação segura de mídias ou sobrescrição de dados (wipe).

➡ Fundamentação: art. 15, III da LGPD; art. 25, §1º da LAI; ISO/IEC 27002, controle 5.14 (Descarte de informações).

5.9 Auditoria e Revisão da Classificação

O Comitê de Segurança da Informação, com apoio da Controladoria e da TI, deverá realizar auditorias periódicas sobre a classificação e o tratamento das informações, verificando:

- Adequação dos níveis de sigilo aplicados;
- Correta rotulagem e armazenamento;
- Conformidade com as legislações aplicáveis;
- Ocorrência de acessos indevidos ou incidentes.

As revisões das classificações deverão ocorrer, no mínimo, a cada 24 meses, ou sempre que houver alteração significativa no contexto, na legislação ou na sensibilidade da informação.

Capítulo 6 – Controle de Acesso à Informação e aos Sistemas

6.1 Conceito e Finalidade

O controle de acesso é o conjunto de políticas, procedimentos e mecanismos destinados a garantir que apenas pessoas devidamente autorizadas possam acessar informações, sistemas, redes e ativos tecnológicos da Prefeitura Municipal de Bocaina – Estado de São Paulo.

O objetivo deste capítulo é assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações, prevenindo acessos indevidos, fraudes, vazamentos e incidentes que possam comprometer os dados públicos e pessoais tratados pela administração municipal.

➡ Base normativa:

- Lei nº 13.709/2018 – LGPD (arts. 6º, VII e 46);
- Lei nº 12.527/2011 – LAI (art. 7º);
- ABNT NBR ISO/IEC 27002:2023 – Controles 5.15 a 5.18;
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Lei do Governo Digital (art. 15, incisos II e IV).

6.2 Princípios do Controle de Acesso

O controle de acesso da Prefeitura Municipal é regido pelos seguintes princípios:

I. Necessidade de saber (Need to Know): o acesso às informações é concedido somente a quem necessita delas para executar suas atividades;

II. Menor privilégio: cada usuário deve possuir apenas as permissões mínimas indispensáveis ao desempenho de suas funções;

III. Autenticidade e rastreabilidade: toda ação sobre os sistemas deve ser vinculada a um usuário identificado e autenticado;

IV. Segregação de funções: funções críticas devem ser separadas para evitar conflito de interesses ou fraudes;

V. Temporalidade: os acessos devem ser concedidos por prazo determinado, sendo periodicamente revisados e revogados quando cessada a necessidade.

6.3 Perfis e Tipos de Acesso

Os acessos aos sistemas e informações da Prefeitura serão classificados em três categorias principais:

Tipo de Acesso	Descrição	Exemplos de Aplicação
Administrador	Permite gerenciar sistemas, usuários e configurações.	Coordenador de TI e Ténicos de TI designados.
Administrativo	Permite gerenciar sistemas.	Coordenadores de Deptos Administrativos.
Operacional	Permite executar funções relacionadas à rotina de trabalho, sem modificar configurações críticas.	Servidores de departamento, agentes públicos.

Tipo de Acesso	Descrição	Exemplos de Aplicação
Consulta (Leitura)	Permite visualizar informações sem alterar dados.	Gestores, auditores, controladores internos.

O Coordenador de TI deverá manter um cadastro atualizado de perfis de acesso, contendo identificação do usuário, data de criação, tipo de acesso e responsável pela autorização.

6.4 Procedimentos de Concessão e Revogação de Acesso

I. Todo acesso deverá ser solicitado formalmente pelo gestor da unidade e autorizado pela autoridade competente;

II. O Coordenador de TI deverá registrar a data de criação e o motivo do acesso concedido;

III. O acesso de usuários desligados, transferidos ou com alteração de função deverá ser imediatamente revogado;

IV. Contas inativas por mais de 90 dias deverão ser bloqueadas;

V. O Comitê de Segurança da Informação deverá revisar trimestralmente os perfis de acesso e as permissões concedidas.

➡ Referência: ISO/IEC 27002:2023, controles 5.16 e 8.2.

6.5 Autenticação de Usuários

A autenticação de usuários deve garantir a identidade de quem acessa os sistemas, utilizando mecanismos de segurança proporcionais ao nível de risco.

I. Requisitos mínimos:

- Utilização obrigatória de login individual e intransferível;
- Senhas com no mínimo 8 caracteres, contendo letras maiúsculas, minúsculas, números e símbolos;
- Troca obrigatória de senha a cada 90 dias;
- Bloqueio automático após 5 tentativas incorretas consecutivas;
- Proibição de reutilização das últimas 3 senhas.

II. Mecanismos complementares (conforme disponibilidade):

- Autenticação multifator (MFA) para acessos administrativos ou sensíveis;
- Tokens ou certificados digitais para assinatura e autenticação de servidores;
- Controle de acesso baseado em grupos ou funções (RBAC – Role Based Access Control).

➡ Referência técnica: ISO/IEC 27002, controle 8.3 (Gestão de credenciais de autenticação).

6.6 Controle de Acesso Físico

I. O acesso físico a áreas que contenham equipamentos críticos (datacenter, servidores,

arquivos, armários de backup) será restrito e autorizado pelo Coordenador de TI;

II. Visitantes e prestadores de serviço deverão ser acompanhados e registrados em livro ou sistema de controle;

III. Portas e janelas de áreas sensíveis devem permanecer trancadas fora do horário de expediente;

IV. Equipamentos portáteis (notebooks, HDs externos, *pendrives*) devem ser armazenados de forma segura;

V. Deve ser implementado sistema de rastreabilidade de entrada e saída de equipamentos.

➡ Base: ISO/IEC 27002, seção 7 (Segurança física e ambiental).

6.7 Acesso Remoto e Dispositivos Móveis

I. O acesso remoto aos sistemas da Prefeitura será permitido apenas mediante autorização prévia do Coordenador de TI;

II. Todo acesso remoto deverá ocorrer por conexão segura (VPN ou canal criptografado);

III. É vedada a utilização de redes públicas não seguras para acesso a informações institucionais;

IV. Equipamentos pessoais (BYOD – Bring Your Own Device) não poderão ser utilizados na rede administrativa da prefeitura em hipótese alguma; quer sejam de servidores, prestadores de serviços ou visitantes;

V. Equipamentos pessoais (BYOD – Bring Your Own Device), só poderão ser utilizados em redes fisicamente separadas da rede administrativas (convidados), caso existam, e como cadastro obrigatório para uso;

VI. Deve ser implementado controle de logs para monitorar acessos remotos e conexões externas.

➡ Referência: ISO/IEC 27002, controles 8.23 e 8.24.

6.8 Registro, Auditoria e Rastreabilidade de Acessos

Todos os acessos a sistemas, internet e informações críticas deverão ser registrados e auditáveis, contemplando:

- Identificação do usuário;
- Data e hora de acesso;
- Sistema ou recurso acessado;
- Ações executadas;
- Resultado (sucesso ou falha).

Esses registros deverão ser:

- Mantidos por prazo mínimo de 12 meses;

- Armazenados de forma protegida contra alterações;
- Analisados periodicamente pelo Coordenador de TI e pela Controladoria.

➡ Fundamentação: art. 6º, X da LGPD (responsabilização e prestação de contas); ISO/IEC 27002, controle 8.15.

6.9 Revogação e Suspensão de Acesso

Os acessos deverão ser suspensos ou revogados imediatamente nas seguintes situações:

I. Desligamento, férias ou afastamento do servidor;

II. Término de contrato de prestador de serviço;

III. Alteração de função ou setor;

IV. Constatação de uso indevido, compartilhamento de credenciais ou descumprimento da política;

V. Identificação de incidente de segurança ou violação de dados.

➡ A revogação deverá ser documentada e comunicada ao Comitê de Segurança da Informação.

6.10 Termo de Responsabilidade de Acesso

Todo usuário com acesso aos ativos tecnológicos da Prefeitura deverá assinar Termo de Responsabilidade de Acesso (Termo de Uso dos Sistemas e Termo de Uso da Internet), comprometendo-se a:

- Utilizar os recursos apenas para fins institucionais, no exercício de suas funções;
- Manter sigilo sobre senhas e informações;
- Respeitar esta PSI (Política de Segurança da Informação), respeitar as normas contidas na Instrução Normativa 001/2013 (e suas atualizações) e as demais normas complementares;
- Comunicar imediatamente incidentes ou suspeitas de violação.

➡ Este termo deverá ser arquivado pelo setor de Recursos Humanos e revisado anualmente.

Capítulo 7 – Segurança Física, Ambiental e de Infraestrutura Tecnológica

7.1 Conceito e Finalidade

A Segurança Física e Ambiental compreende o conjunto de medidas destinadas a proteger os equipamentos, instalações, documentos e ativos tecnológicos da Prefeitura Municipal de Bocaina – Estado de São Paulo contra ameaças físicas, ambientais e tecnológicas que possam comprometer a confidencialidade, integridade e disponibilidade das informações.

O objetivo é minimizar riscos de danos, interrupções ou perdas causadas por acesso físico não autorizado, incêndios, falhas elétricas, inundações, furtos, sabotagem, ou desastres naturais.

➡ Base normativa:

- ABNT NBR ISO/IEC 27002:2023 – Seção 7 (Segurança física e ambiental);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 13.709/2018 – LGPD (art. 46);
- Lei nº 14.129/2021 – Governo Digital (art. 15);
- Instrução Normativa GSI/PR nº 01/2019.

7.2 Princípios de Proteção Física e Ambiental

As medidas de segurança física e ambiental devem observar os seguintes princípios:

I. Prevenção: adotar medidas para evitar o acesso físico indevido e minimizar a probabilidade de incidentes;

II. Detecção: identificar de forma rápida tentativas de intrusão, incêndios, falhas elétricas e outras anomalias;

III. Resposta: possuir procedimentos claros para reagir adequadamente a eventos e restaurar a normalidade;

IV. Continuidade: assegurar que os ambientes e equipamentos essenciais possam ser restabelecidos sem prejuízo ao funcionamento da administração;

V. Proporcionalidade: as medidas devem ser compatíveis com o valor da informação e com a criticidade do serviço prestado.

7.3 Áreas e Instalações Críticas

Consideram-se áreas críticas para a segurança da informação da Prefeitura:

- Sala de servidores e datacenter municipal (se houver);
- Ambientes que abrigam equipamentos de rede, roteadores e switches;
- Arquivos físicos e salas de documentos sigilosos;
- Estações de trabalho de setores sensíveis (como saúde, finanças e recursos humanos);
- Locais de armazenamento de mídias de backup.

➡ Essas áreas deverão ter controle de acesso físico restrito, registro de entrada e saída de pessoas e monitoramento contínuo, conforme sua importância.

7.4 Controle de Acesso Físico

I. O acesso a áreas críticas deve ser permitido somente a servidores e prestadores devidamente autorizados;

II. Visitantes e técnicos externos deverão ser acompanhados por servidor responsável e registrados em livro ou sistema de controle;

III. As portas e janelas das áreas de TI e arquivos devem permanecer trancadas fora do horário

de expediente;

IV. As chaves e cartões de acesso devem ter controle formal de entrega, devolução e substituição;

V. Câmeras de vigilância e sistemas de alarme devem ser utilizados quando possível, respeitando a legislação de proteção de dados e privacidade (art. 7º, II da LGPD).

➡ Referência: ISO/IEC 27002, controle 7.4 (Controles de entrada física).

7.5 Proteção de Equipamentos e Instalações

I. Os equipamentos devem estar dispostos em áreas com ventilação adequada, livres de poeira e calor excessivo;

II. Servidores e nobreaks devem estar posicionados em locais secos, sobre plataformas elevadas, para evitar danos por inundação;

III. Os cabos de energia e dados devem ser protegidos e identificados;

IV. Os equipamentos devem estar conectados a sistemas de proteção elétrica (estabilizadores, filtros de linha e nobreaks);

V. O desligamento dos sistemas críticos deve seguir procedimentos formais de desligamento seguro.

➡ Referência: ISO/IEC 27002, controle 7.6 (Proteção de equipamentos).

7.6 Segurança Elétrica e de Climatização

I. Os ambientes de TI devem dispor de sistema de energia ininterrupta (UPS) e de aterramento elétrico adequado;

II. O sistema elétrico deve ser inspecionado periodicamente;

III. A climatização dos ambientes críticos deve manter temperatura entre 18°C e 24°C e umidade relativa entre 45% e 60%, conforme recomendações técnicas;

IV. Equipamentos de ar-condicionado e ventilação devem receber manutenção preventiva;

V. Em caso de falha elétrica ou oscilação de energia, devem existir procedimentos para desligamento controlado dos servidores.

➡ Referência: ISO/IEC 27002, controle 7.7 (Energia elétrica e climatização adequadas).

7.7 Proteção Contra Incêndios, Inundações e Outras Ameaças

I. As áreas críticas deverão possuir extintores adequados ao tipo de risco (CO_2 ou pó químico seco) e sinalização visível de emergência;

II. IAs instalações devem manter saídas de emergência desobstruídas, iluminação de emergência e plantas de evacuação;

III. É vedado o armazenamento de materiais inflamáveis ou líquidos próximos aos equipamentos de TI;

IV. Equipamentos e documentos importantes devem ser mantidos acima do nível do piso para reduzir riscos de inundação;

V. Os sistemas de backup devem prever cópia externa (off-site) armazenada em local seguro e distante da sede principal.

➡ Referência: ISO/IEC 27002, controles 7.8 e 7.9.

7.8 Transporte e Remoção de Equipamentos

I. Nenhum equipamento, mídia ou ativo de informação poderá ser retirado das dependências da Prefeitura sem autorização formal da autoridade competente;

II. O transporte de notebooks, pendrives ou HDs externos deverá ocorrer mediante Termo de Responsabilidade;

III. As mídias que contiverem dados sensíveis deverão ser criptografadas ou fisicamente protegidas durante o transporte;

IV. Equipamentos desativados deverão ser armazenados de forma segura até o descarte definitivo;

V. A movimentação de equipamentos deve ser autorizada e registrada pelo Depto de TI.

➡ Referência: ISO/IEC 27002, controle 8.26 (Remoção de ativos).

7.9 Proteção de Documentos Físicos

I. Documentos impressos classificados como restritos, confidenciais ou sigilosos devem ser mantidos em armários trancados ou salas seguras;

II. O acesso físico deve ser limitado aos servidores responsáveis pela unidade;

III. É vedado o abandono de documentos sobre mesas, impressoras ou locais de circulação pública;

IV. Impressões sigilosas devem ser retiradas imediatamente após emissão;

V. O descarte deve ser feito por fragmentação, trituração ou incineração controlada.

➡ Referência: ISO/IEC 27002, controle 5.14 (Descarte seguro de informações).

7.10 Limpeza, Manutenção e Suporte de Instalações

I. Empresas terceirizadas responsáveis por limpeza, manutenção predial ou elétrica devem ser supervisionadas durante o acesso a áreas críticas;

II. Tais empresas deverão assinar termos de confidencialidade e segurança;

III. Ferramentas e materiais utilizados deverão ser inspecionados antes e após o serviço;

IV. É proibido o uso de dispositivos pessoais de armazenamento em ambientes restritos;

V. Toda manutenção deverá ser registrada em relatório e arquivada.

➡ Base: ISO/IEC 27002, controle 7.10 (Segurança durante manutenção e suporte).

7.11 Continuidade Operacional e Recuperação de Desastres

I. O Coordenador de TI deverá manter um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) documentados e testados periodicamente;

II. O plano deve contemplar: cópias de segurança, contatos de emergência, locais alternativos de operação e procedimentos de restauração;

III. Os testes de restauração deverão ocorrer pelo menos uma vez ao ano;

IV. O resultado dos testes deve ser reportado ao Comitê de Segurança da Informação;

V. O PCN e o PRD devem integrar o Plano Diretor de TI e estar alinhados à estratégia da administração municipal.

➡ Base: ISO/IEC 22301 e ISO/IEC 27031.

Capítulo 8 – Cópias de Segurança (Backup) e Recuperação de Dados

8.1 Conceito e Finalidade

As cópias de segurança (backups) são medidas essenciais para garantir a disponibilidade e integridade das informações, assegurando que dados e sistemas da Prefeitura Municipal de Bocaina – Estado de São Paulo, possam ser restaurados em caso de falhas, exclusões acidentais, incidentes de segurança, ataques cibernéticos ou desastres naturais.

A finalidade deste capítulo é estabelecer diretrizes, responsabilidades e procedimentos padronizados para o planejamento, execução, armazenamento e verificação de backups, bem como a recuperação de informações e sistemas críticos.

➡ Base normativa:

- ABNT NBR ISO/IEC 27002:2023 – controles 8.13 (backup) e 8.14 (recuperação de dados);
- Lei nº 13.709/2018 – LGPD (art. 46, §2º);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Lei do Governo Digital;
- Portaria SGD/ME nº 9.907/2022 – Diretrizes de segurança e privacidade para órgãos públicos.

8.2 Objetivos Específicos

I. Assegurar a recuperação tempestiva de dados e sistemas em caso de falha, sinistro ou incidente de segurança;

II. Minimizar o impacto de interrupções sobre os serviços públicos e atividades administrativas;

III. Garantir a continuidade operacional e a preservação do patrimônio informacional;

IV. Cumprir as obrigações legais de guarda, sigilo e proteção de dados pessoais e sensíveis;

V. Estabelecer a rastreabilidade de todas as cópias e restaurações de dados realizadas.

8.3 Escopo e Abrangência

Esta política de backup aplica-se a todos os sistemas, bancos de dados, documentos eletrônicos e informações institucionais sob responsabilidade da Prefeitura, incluindo:

- Servidores locais e em nuvem;
- Sistemas administrativos e financeiros;
- Sistemas de saúde, educação e assistência social;
- Arquivos eletrônicos e documentos oficiais;
- Bases de dados contendo informações pessoais ou sensíveis;
- Equipamentos e mídias de armazenamento utilizados para backup.

8.4 Tipos de Backup Adotados

A Prefeitura deverá adotar estratégia combinada de backup, conforme a criticidade das informações:

Tipo	Descrição	Aplicação Recomendada
Completo (Full)	Cópia integral de todos os dados selecionados.	Realizado semanalmente em todos os sistemas principais.
Incremental	Cópia apenas dos dados alterados desde o último backup (completo ou incremental).	Realizado diariamente.
Diferencial	Cópia dos dados alterados desde o último backup completo.	Utilizado como redundância de segurança.
Off-site (externo)	Armazenamento de cópia em local físico distinto da sede principal.	Realizado semanalmente.
Em nuvem (Cloud Backup)	Armazenamento criptografado em plataforma segura de nuvem.	Recomendado para sistemas administrativos e financeiros.

➡ Referência: ISO/IEC 27002, controle 8.13 (Backups de informações).

8.5 Periodicidade e Retenção de Backups

I. O backup diário deve contemplar as bases de dados de sistemas operacionais e documentos críticos;

II. O backup semanal completo deve ser realizado para todos os servidores e sistemas principais;

III. O backup mensal consolidado deve ser preservado por, no mínimo, 12 meses;

IV. Backups relacionados a dados fiscais, contábeis e financeiros devem seguir os prazos de guarda determinados por lei (mínimo de 5 anos, conforme legislação tributária);

V. O tempo de retenção dos backups deve respeitar o princípio da minimização da LGPD,

eliminando dados pessoais quando cessar a finalidade do tratamento.

8.6 Armazenamento e Proteção das Cópias

I. As cópias de segurança devem ser armazenadas em ambientes fisicamente seguros, com acesso restrito;

II. O local de armazenamento (sala-cofre, datacenter, ou armário seguro) deve ser protegido contra umidade, poeira, calor excessivo e risco elétrico;

III. Deve haver redundância geográfica, com cópia externa armazenada em local físico ou serviço de nuvem distinto da sede principal;

IV. Os arquivos de backup devem ser criptografados e protegidos por senha forte;

V. A guarda das mídias físicas (HDs externos, fitas, pendrives) deve seguir controle de registro, rastreabilidade e assinatura de termo de responsabilidade;

VI. O transporte de mídias entre locais deve ser feito de forma controlada e documentada.

➡ Referência: ISO/IEC 27002, controles 8.13.4 e 8.26.

8.7 Testes de Restauração e Validação

I. Os backups deverão ser testados periodicamente para verificar sua integridade e capacidade de restauração;

II. Os testes devem ocorrer pelo menos uma vez por trimestre;

III. O Gestor de TI deverá manter relatório dos testes realizados, contendo data, sistema testado, resultado e responsável;

IV. Falhas de restauração deverão ser imediatamente comunicadas ao Comitê de Segurança da Informação e ao DPO;

V. A restauração de dados pessoais deverá ser feita de forma controlada, garantindo que somente usuários autorizados tenham acesso.

➡ Referência: ISO/IEC 27002, controle 8.14 (Testes de restauração de dados).

8.8 Responsabilidades

I. Gestor de Tecnologia da Informação:

- Planejar e implementar a rotina de backups;
- Garantir a integridade, rastreabilidade e documentação das cópias;
- Gerenciar o armazenamento, testes e restaurações;
- Reportar periodicamente os resultados ao Comitê de Segurança da Informação.

I. Comitê Municipal de Segurança da Informação:

- Acompanhar o cumprimento das rotinas de backup;
- Definir prioridades de recuperação e níveis de serviço;

- Avaliar riscos e propor melhorias contínuas.

I. Demais Secretarias e Unidades:

- Informar à TI sobre alterações em sistemas, bases de dados ou processos críticos;
- Apoiar o planejamento da recuperação em caso de falha;
- Respeitar as diretrizes sobre guarda e eliminação de dados.

8.9 Recuperação de Dados e Continuidade Operacional

I. Em caso de incidente ou desastre, a recuperação dos dados deverá seguir o Plano de Recuperação de Desastres (PRD) e o Plano de Continuidade de Negócios (PCN);

II. A restauração deverá priorizar sistemas essenciais ao funcionamento da Prefeitura (como contabilidade, folha de pagamento, saúde e arrecadação);

III. Toda restauração deve ser documentada e validada pelo responsável técnico;

IV. Após a restauração, os sistemas deverão ser submetidos a verificação de integridade e funcionalidade;

V. Quando envolver dados pessoais, a operação deverá ser registrada para fins de prestação de contas (accountability), conforme o art. 6º, X da LGPD.

8.10 Eliminação Segura de Backups Antigos

I. Backups fora do prazo de retenção deverão ser eliminados de forma segura e documentada;

II. A exclusão deve impedir a recuperação dos dados por qualquer meio (técnicas de wipe ou destruição física da mídia);

III. Deve ser lavrado termo ou relatório de descarte contendo data, tipo de mídia e responsável técnico;

IV. O descarte deve observar as regras da Política de Descarte de Informações e as exigências da LGPD quanto à eliminação de dados pessoais.

➡ Referência: ISO/IEC 27002, controle 5.14.

Capítulo 9 – Gestão de Incidentes de Segurança da Informação

9.1 Conceito e Finalidade

Incidente de segurança da informação é qualquer evento adverso, confirmado ou suspeito, que possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações, sistemas ou serviços da Prefeitura Municipal de Bocaina – Estado de São Paulo.

A gestão de incidentes tem por finalidade detectar, registrar, analisar e responder rapidamente a esses eventos, reduzindo seus impactos, restaurando a normalidade operacional e promovendo a melhoria contínua dos controles de segurança.

➡ Base normativa:

- LGPD, art. 48 (Comunicação de incidentes à ANPD e aos titulares);
- ABNT NBR ISO/IEC 27035:2023 – Gestão de Incidentes de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2023 – Controles 8.16 a 8.18;
- Decreto nº 9.637/2018 – PNSI;
- Lei nº 14.129/2021 – Governo Digital.

9.2 Objetivos Específicos

I. Estabelecer um fluxo padronizado para identificação, comunicação e tratamento de incidentes;

II. Minimizar o impacto técnico, jurídico e reputacional decorrente de falhas ou vazamentos;

III. Assegurar a rastreamento e documentação de todos os eventos;
IV – Atender às obrigações legais de notificação previstas na LGPD;

IV. Promover a cultura de segurança entre servidores, gestores e prestadores de serviço.

9.3 Abrangência

Aplica-se a todos os órgãos, diretorias, departamentos, autarquias e fundações municipais, bem como a todos os servidores, estagiários, terceirizados e fornecedores que tratem informações ou dados pessoais em nome da Prefeitura.

9.4 Exemplos de Incidentes de Segurança

- Perda, roubo ou furto de equipamento contendo dados institucionais;
- Acesso não autorizado a sistemas ou pastas compartilhadas;
- Envio indevido de documentos ou informações sigilosas;
- Infecção por malware, ransomware ou vírus;
- Exclusão ou alteração não intencional de dados;
- Vazamento ou divulgação indevida de dados pessoais;
- Interrupção de serviços críticos ou falha prolongada de sistemas;
- Tentativas de phishing, engenharia social ou fraudes eletrônicas.

9.5 Princípios da Gestão de Incidentes

I. Imediatismo: todo incidente deve ser comunicado assim que detectado;

II. Responsabilidade: cada agente público é responsável por relatar irregularidades observadas;

III. Sigilo: informações sobre incidentes devem ser tratadas de forma confidencial até sua resolução;

IV. Rastreabilidade: todos os registros e decisões devem ser documentados;

V. Aprendizado Contínuo: cada incidente deve gerar lições para aperfeiçoamento dos controles e políticas.

9.6 Fluxo de Gestão de Incidentes

O processo de gestão seguirá as cinco fases preconizadas pela ISO/IEC 27035, adaptadas à realidade municipal:

1. Identificação e Registro

- O usuário que detectar anomalia ou evento suspeito deve comunicar imediatamente à unidade de TI ou ao Encarregado (DPO).
- O Gestor de TI registra o incidente em formulário próprio, contendo: data/hora, descrição, sistema afetado, tipo de dado, pessoa que reportou e ações iniciais.
- O registro deve ser numerado e arquivado em banco de dados ou planilha oficial.

2. Classificação e Análise

- O Gestor de TI e o Comitê de Segurança avaliam a gravidade, a abrangência e o tipo de incidente (baixo, médio, alto ou crítico).
- Quando envolver dados pessoais ou sensíveis, o Encarregado (DPO) participa obrigatoriamente da análise.

3. Resposta e Contenção

- Adotar medidas imediatas para conter o incidente e impedir sua propagação (bloqueio de conta, desconexão de rede, isolamento de equipamento, etc.);
- Registrar todas as ações adotadas e autoridades envolvidas;
- Preservar evidências digitais e logs para eventual investigação.

4. Comunicação e Notificação

- O Encarregado de Dados deve avaliar a necessidade de notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados, conforme o art. 48 da LGPD;
- A notificação deve ser imediata e conter: natureza do incidente, dados afetados, medidas técnicas adotadas e ações corretivas;
- O Comitê de Segurança poderá comunicar outros órgãos competentes (Controladoria, Polícia Civil, Ministério Público, etc.), conforme o caso.

5. Encerramento e Ações Corretivas

- Após a resolução, deve ser elaborado Relatório de Encerramento do Incidente, contendo causa raiz, impactos, medidas preventivas e responsáveis;
- O Comitê de Segurança revisará o caso e proporá ajustes de processo, treinamento ou infraestrutura;
- O relatório será arquivado por mínimo de 5 anos e poderá subsidiar auditorias ou

processos administrativos.

9.7 Responsabilidades

I. Coordenador de TI:

- Receber, registrar e tratar tecnicamente o incidente;
- Adotar medidas de contenção e restauração de serviços;
- Preservar evidências digitais;
- Emitir relatório técnico e encaminhar ao Comitê.

II. Encarregado de Dados (DPO):

- Analisar o impacto sobre dados pessoais e sensíveis;
- Avaliar a necessidade de notificação à ANPD e aos titulares;
- Documentar o incidente no Relatório de Impacto à Proteção de Dados (RIPD);
- Orientar a comunicação institucional em caso de vazamento.

III. Comitê Municipal de Segurança da Informação:

- Acompanhar os incidentes registrados;
- Definir prioridades e recursos de resposta;
- Analisar relatórios de encerramento e recomendar melhorias.

IV. Servidores e Usuários:

- Comunicar imediatamente qualquer ocorrência suspeita;
- Não apagar, alterar ou divulgar informações sobre o incidente;
- Cooperar com a equipe de TI e o Comitê na apuração dos fatos.

9.8 Comunicação com a ANPD e Outros Órgãos

Em conformidade com o art. 48 da LGPD, a Prefeitura deverá comunicar a ANPD e os titulares dos dados quando o incidente puder acarretar risco ou dano relevante aos direitos dos titulares.

A notificação deverá conter:

- Descrição do incidente;
- Dados pessoais afetados;
- Medidas de contenção e correção;
- Possíveis riscos e impactos;
- Contatos do Encarregado de Dados.

A Prefeitura também deverá comunicar, quando necessário, a Controladoria, o Ministério Público

ou a Polícia Civil, caso haja indícios de crime, dano patrimonial ou violação de sigilo funcional.

9.9 Treinamento e Conscientização

I. Todos os servidores e colaboradores devem receber orientação anual sobre prevenção e comunicação de incidentes;

II. As capacitações devem incluir simulações de ataques cibernéticos, políticas de senhas, engenharia social e boas práticas no uso de e-mail e internet;

III. As lições aprendidas em incidentes reais deverão ser incorporadas aos programas de treinamento e aos procedimentos operacionais padrão (POPs).

9.10 Documentação e Auditoria

I. Todos os incidentes, relatórios e notificações deverão ser registrados em sistema ou planilha oficial;

II. Os registros devem ser preservados por prazo mínimo de 5 anos;

III. O Comitê de Segurança deverá realizar auditorias anuais sobre o processo de gestão de incidentes;

IV. Os resultados serão encaminhados à Alta Administração e à Controladoria Interna.

Capítulo 10 – Treinamento, Conscientização e Cultura de Segurança

10.1 Conceito e Finalidade

A conscientização e a capacitação em segurança da informação são pilares fundamentais para garantir que os servidores públicos, colaboradores e prestadores de serviço compreendam suas responsabilidades e adotem comportamentos seguros e éticos no tratamento de dados e informações públicas.

Este capítulo tem por finalidade instituir diretrizes e mecanismos permanentes de treinamento e educação voltados à segurança da informação e à proteção de dados pessoais, criando uma cultura organizacional de segurança em toda a Prefeitura Municipal de Bocaina/SP.

➡ Base normativa:

- Lei nº 13.709/2018 – LGPD (arts. 46 e 50);
- Lei nº 14.129/2021 – Lei do Governo Digital (art. 15, incisos IV e V);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2023 – controles 6.3 e 6.4 (Conscientização, educação e treinamento em segurança da informação).

10.2 Objetivos

I. Promover o entendimento institucional sobre os princípios e boas práticas de segurança da informação;

II. Sensibilizar servidores e terceiros quanto à importância da proteção de dados pessoais e sigilosos;

III. Reduzir a probabilidade de incidentes causados por erro humano ou negligência;

IV. Disseminar orientações sobre uso ético e responsável de recursos tecnológicos;

V. Estimular a participação ativa dos servidores na prevenção, identificação e reporte de incidentes;

VI. Cumprir o dever de adoção de medidas administrativas preventivas exigido pelo art. 46 da LGPD.

10.3 Princípios de Conscientização

Os programas de conscientização deverão seguir os seguintes princípios:

1. Periodicidade: as ações devem ser contínuas e planejadas, não se limitando a eventos pontuais;

2. Acessibilidade: o conteúdo deve ser claro, compreensível e adequado ao perfil dos públicos (administrativo, técnico e operacional);

3. Relevância: os temas devem abordar situações reais e riscos concretos vivenciados pela administração pública;

4. Praticidade: devem incluir exemplos, casos reais e orientações aplicáveis à rotina de trabalho;

5. Evidência e registro: toda ação de treinamento deve ser documentada, registrando data, conteúdo, instrutor e participantes.

10.4 Públicos-Alvo

A política de conscientização abrangerá os seguintes grupos:

Público-Alvo	Conteúdo Focado
Servidores efetivos e comissionados	Princípios da LGPD, sigilo funcional, uso ético de sistemas, identificação de ameaças e boas práticas digitais.
Estagiários e terceirizados	Condutas básicas de segurança, acesso controlado e confidencialidade de informações.
Gestores e Diretores	Governança da informação, gestão de riscos, incidentes e responsabilidades administrativas.
Prestadores de serviços de TI	Segurança de redes, backups, incidentes cibernéticos e cláusulas contratuais de confidencialidade.
DPO (Encarregado de Dados) e Comitê	Atualização legal, relatórios de impacto e procedimentos de notificação à ANPD.

10.5 Temas Prioritários de Treinamento

Os programas de capacitação em segurança da informação e proteção de dados deverão abranger, no mínimo, os seguintes temas:

1. Fundamentos da Segurança da Informação (confidencialidade, integridade, disponibilidade e autenticidade);
2. Boas práticas no uso de e-mail, senhas e internet corporativa;
3. Identificação de fraudes digitais, *phishing* e engenharia social;
4. Proteção de dados pessoais e sensíveis (conforme a LGPD);
5. Política de uso de dispositivos móveis e armazenamento em nuvem;
6. Procedimentos em caso de incidentes ou suspeitas de vazamento;
7. Regras de acesso e confidencialidade de informações públicas e restritas;
8. Classificação e descarte seguro de informações;
9. Responsabilidade administrativa e sanções em caso de descumprimento;
10. Ética digital e dever de sigilo funcional.

➡ Referência técnica: ISO/IEC 27002, controle 6.4.

10.6 Formas de Execução e Ferramentas

I. Os treinamentos poderão ser realizados presencialmente ou em formato on-line (EAD), preferencialmente com apoio de vídeos, manuais, cartilhas e plataformas de capacitação;

II. A Secretaria de Administração e o Gestor de TI deverão manter calendário anual de capacitações;

III. Poderão ser utilizadas campanhas temáticas periódicas, como "Mês da Segurança da Informação" ou "Semana da Proteção de Dados";

IV. A comunicação interna poderá utilizar murais, e-mails, infográficos e avisos eletrônicos com lembretes e boas práticas;

V. O conteúdo deverá ser revisado anualmente, incorporando novas ameaças, legislações e recomendações da ANPD.

10.7 Integração com Programas Municipais

As ações de conscientização deverão estar integradas a outros programas da Prefeitura, tais como:

- Programa de Integridade e Ética Pública;
- Plano Diretor de Tecnologia da Informação (PDTI);
- Política de Proteção de Dados Pessoais;
- Gestão de Riscos Institucionais;
- Capacitações da Escola de Governo Municipal (quando houver).

Essa integração garante coerência entre as políticas de transparência, governança e proteção de dados.

10.8 Responsabilidades

I. Comitê Municipal de Segurança da Informação:

- Planejar e supervisionar as ações de conscientização;
- Propor temas e materiais educativos;
- Avaliar resultados e propor melhorias.

II. Gestor de TI:

- Apoiar tecnicamente as ações de capacitação;
- Incluir conteúdos práticos sobre segurança digital;
- Registrar as evidências de participação e frequência.

III. Encarregado de Dados (DPO):

- Orientar a capacitação em proteção de dados pessoais;
- Atualizar os conteúdos conforme orientações da ANPD;
- Elaborar relatórios de conformidade com base nas ações realizadas.

IV. Servidores e Colaboradores:

- Participar obrigatoriamente dos treinamentos;
- Aplicar as orientações aprendidas no cotidiano de trabalho;
- Reportar dúvidas ou situações de risco identificadas.

10.9 Registro, Evidências e Auditoria

I. Toda ação de capacitação deverá gerar registro formal contendo data, conteúdo, público-alvo, instrutor e carga horária;

II. Os registros deverão ser arquivados pela Secretaria de Administração ou pelo Comitê de Segurança da Informação;

III. As evidências serão utilizadas para comprovar adoção de medidas preventivas, conforme o art. 46 da LGPD;

IV. A Controladoria Interna poderá auditar as ações de conscientização, verificando a participação e eficácia dos programas.

10.10 Cultura Organizacional de Segurança

A segurança da informação é uma responsabilidade coletiva e contínua. A Prefeitura deve promover uma cultura institucional baseada em:

- Exemplo da liderança: os gestores devem adotar e demonstrar boas práticas;
- Engajamento permanente: os servidores devem compreender que segurança é parte de suas funções;
- Valorização da ética e da transparência: equilíbrio entre proteção e acesso à informação;
- Reconhecimento de boas práticas: estímulo a servidores e equipes que se destacarem na aplicação da política.

➡ Essa cultura deve ser incorporada aos valores institucionais da Prefeitura, consolidando a confiança da sociedade na gestão pública.

Capítulo 11 – Auditoria, Monitoramento e Melhoria Contínua

11.1 Conceito e Finalidade

A auditoria e o monitoramento da Política de Segurança da Informação (PSI) têm por objetivo avaliar a conformidade, a eficácia e a aderência das práticas de segurança da Prefeitura Municipal de Bocaina – Estado de São Paulo, em relação às diretrizes estabelecidas nesta política e às legislações vigentes.

A melhoria contínua busca garantir que os processos, controles e procedimentos relacionados à segurança da informação evoluam de forma constante, acompanhando as mudanças tecnológicas, legais e organizacionais.

➡ Base normativa:

- ABNT NBR ISO/IEC 27001:2022 – Cláusulas 9.1 a 10.2 (Monitoramento, auditoria e melhoria);
- ABNT NBR ISO/IEC 27002:2023 – Controles 5.35 a 5.37;
- ABNT NBR ISO/IEC 27004:2022 – Avaliação de desempenho da segurança da informação;
- Lei nº 13.709/2018 – LGPD (art. 50 – boas práticas e governança);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Governo Digital (art. 15).

11.2 Objetivos Específicos

I. Avaliar periodicamente a aplicação efetiva das políticas, normas e controles de segurança da informação;

II. Identificar falhas, vulnerabilidades e oportunidades de melhoria;

III. Comprovar a conformidade com a LGPD, a LAI e demais regulamentos aplicáveis;

IV. Fornecer subsídios para a tomada de decisão da Alta Administração e do Comitê de Segurança;

V. Garantir a transparência e a prestação de contas (accountability) das ações de segurança da informação;

VI. Manter o ciclo de melhoria contínua (PDCA) ativo: Planejar → Executar → Verificar → Agir.

11.3 Princípios da Auditoria e Monitoramento

A execução das auditorias e do monitoramento deverá respeitar os seguintes princípios:

1. Independência: a auditoria deve ser conduzida de forma imparcial, sem interferência dos auditados;

2. Evidência: as conclusões devem se basear em registros, relatórios e fatos comprováveis;

3. Objetividade: as avaliações devem ser técnicas, fundamentadas e livres de juízo pessoal;

4. Rastreabilidade: todas as constatações e recomendações devem ser documentadas;

5. Transparência: os resultados devem ser compartilhados com a Alta Administração e o Comitê;

6. Periodicidade: o processo deve ocorrer de forma planejada e recorrente.

11.4 Escopo das Auditorias

As auditorias internas e externas deverão abranger, no mínimo, os seguintes aspectos:

- Cumprimento das diretrizes da PSI e políticas complementares (backup, controle de acesso, incidentes etc.);
- Conformidade com as leis e regulamentos aplicáveis (LGPD, LAI, Governo Digital);
- Segurança física e lógica de ambientes e sistemas;
- Controle de acessos e gestão de credenciais;
- Procedimentos de backup, restauração e descarte de dados;
- Registros de incidentes e plano de resposta;
- Conscientização e treinamento de servidores;
- Eficiência das medidas de mitigação de riscos;
- Gestão de contratos e cláusulas de confidencialidade com terceiros.

11.5 Tipos de Auditoria

Tipo	Descrição	Periodicidade Recomendada
Auditoria Interna de Segurança da Informação	Realizada pelo Comitê de Segurança ou pela Controladoria Interna, avaliando o cumprimento das normas e controles internos.	Anualmente.

Prefeitura Municipal de Bocaina
Estado de São Paulo

Tipo	Descrição	Periodicidade Recomendada
Auditoria Técnica de TI	Avalia infraestrutura, vulnerabilidades, sistemas, redes, backups e logs. Pode envolver apoio externo.	A cada 12 a 18 meses.
Auditoria de Conformidade LGPD	Verifica a aderência à LGPD, incluindo relatórios de impacto, controles de privacidade e medidas administrativas.	Anualmente ou conforme atualização legal.
Auditoria de Terceiros e Fornecedores	Avalia o cumprimento das cláusulas contratuais de segurança por empresas prestadoras de serviço.	Durante ou após o contrato.

➡ Referência: ISO/IEC 27002, controle 5.35 (Auditoria de segurança da informação).

11.6 Monitoramento Contínuo

I. O Coordenador de TI deverá manter mecanismos de monitoramento automatizado para detectar incidentes, falhas ou acessos não autorizados;

II. Logs de acesso e eventos críticos deverão ser revisados periodicamente;

III. O Comitê de Segurança deverá consolidar relatórios semestrais sobre o desempenho da PSI;

IV. Os resultados das auditorias e monitoramentos deverão subsidiar o Plano de Ação e Melhoria Contínua (PAMC) da Prefeitura;

V. O monitoramento deverá considerar indicadores-chave (KPIs), conforme item 11.7.

➡ Referência: ISO/IEC 27002, controle 5.36 (Monitoramento da segurança da informação).

11.7 Indicadores de Desempenho (KPIs)

A eficácia da PSI e dos controles de segurança será avaliada por meio de indicadores mensuráveis, tais como:

Indicador	Descrição	Periodicidade
Taxa de incidentes de segurança	Número de incidentes reportados x mês.	Mensal
Tempo médio de resposta a incidentes	Tempo entre a detecção e a contenção.	Trimestral
Taxa de sucesso de backup/restauração	Percentual de testes de backup bem-sucedidos.	Trimestral
Percentual de servidores treinados	Relação entre servidores capacitados e total de ativos.	Semestral
Nível de conformidade com a LGPD	Grau de aderência às exigências da lei.	Anual
Conclusão de auditorias planejadas	% de auditorias realizadas no período	Anual

Indicador	Descrição	Periodicidade
	previsto.	

➡ Esses indicadores devem ser acompanhados pelo Comitê e apresentados em relatório anual à Alta Administração.

11.8 Relatórios e Comunicação dos Resultados

I. Os relatórios de auditoria devem conter achados, evidências, recomendações e plano de ação corretivo;

II. O Comitê de Segurança analisará os relatórios e encaminhará à Alta Administração;

III. As recomendações deverão ter prazos e responsáveis designados;

IV. O acompanhamento das correções deverá constar em relatórios de progresso trimestrais;

V. Resultados relevantes podem ser comunicados à Controladoria Interna e ao Tribunal de Contas, quando aplicável.

11.9 Melhoria Contínua (PDCA)

O processo de melhoria contínua da PSI deve seguir o ciclo PDCA (Plan–Do–Check–Act):

1. Planejar (Plan): identificar riscos, definir objetivos e atualizar controles;
2. Executar (Do): implementar políticas, treinamentos e procedimentos;
3. Verificar (Check): monitorar e auditar resultados e conformidade;
4. Agir (Act): corrigir falhas, revisar políticas e promover ajustes.

➡ O ciclo deve ocorrer anualmente, com base nos resultados das auditorias, nos relatórios de incidentes e nos indicadores de desempenho.

11.10 Revisão da Política de Segurança da Informação

I. A PSI deverá ser revisada anualmente ou sempre que houver alterações significativas em leis, tecnologia ou estrutura organizacional;

II. A revisão será coordenada pelo Comitê Municipal de Segurança da Informação, com apoio do Gestor de TI e do Encarregado de Dados (DPO);

III. As versões revisadas deverão ser submetidas à aprovação da Alta Administração Municipal e publicadas no portal institucional;

IV. As alterações devem ser comunicadas a todos os servidores e prestadores de serviço, com treinamento quando necessário.

➡ Referência: ISO/IEC 27002, controle 5.37 (Revisão da política e melhoria contínua).

Capítulo 12 – Disposições Finais e Vigência

Prefeitura Municipal de Bocaina
Estado de São Paulo

12.1 Integração com Outras Políticas e Normativos

Esta Política de Segurança da Informação (PSI) integra o conjunto de políticas e normas internas da Prefeitura Municipal de Bocaina – Estado de São Paulo, devendo ser interpretada de forma complementar às seguintes diretrizes e instrumentos institucionais:

I. Política de Proteção de Dados Pessoais, editada em conformidade com a Lei nº 13.709/2018 (LGPD);

II. Plano Diretor de Tecnologia da Informação (PDTI);

III. Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD);

IV. Política de Backup e Recuperação de Dados;

V. Regulamento Interno de Uso de Recursos Tecnológicos e Comunicação Eletrônica;

VI. Código de Ética e Conduta dos Servidores Públicos Municipais;

VII. Demais normas administrativas e regulamentares editadas pela Administração Municipal.

Parágrafo único. Em caso de conflito entre esta política e outros instrumentos internos, prevalecerão as disposições que garantam maior nível de proteção à informação e aos dados pessoais.

12.2 Cumprimento e Fiscalização

I. O cumprimento desta política é obrigatório para todos os servidores públicos, estagiários, colaboradores, prestadores de serviços e fornecedores que, de qualquer forma, tratem informações ou dados sob responsabilidade da Prefeitura;

II. O Comitê Municipal de Segurança da Informação e Proteção de Dados será o órgão responsável por fiscalizar, orientar e propor melhorias contínuas na aplicação desta política;

III. As Diretorias e Unidades Administrativas deverão cooperar com o Comitê, fornecendo informações e relatórios sempre que solicitados;

IV. A Controladoria Interna poderá realizar auditorias específicas para verificar o cumprimento desta política e das normas correlatas.

12.3 Sanções e Responsabilidades

I. O descumprimento das normas estabelecidas nesta política sujeitará o infrator às sanções administrativas, civis e penais previstas em lei, conforme a gravidade da conduta;

II. Configuram infrações, entre outras:

- a) acesso ou uso indevido de informações sigilosas;
- b) compartilhamento de credenciais, senhas ou chaves de acesso;
- c) omissão na comunicação de incidentes;
- d) descarte inadequado de documentos ou mídias;
- e) negligência no cumprimento das orientações técnicas da área de TI.

III. As penalidades aplicáveis podem incluir:

- advertência;
- suspensão;
- responsabilização civil ou penal, conforme legislação vigente;
- rescisão contratual, no caso de fornecedores e prestadores de serviço.

➡ Fundamentação: art. 46 e 52 da LGPD; art. 116 da Lei nº 8.112/1990 (aplicável por analogia); e Decreto nº 9.637/2018 (PNSI).

12.4 Divulgação e Acesso Público

I. Esta política deverá ser publicada integralmente no portal institucional da Prefeitura e divulgada amplamente entre servidores e colaboradores;

II. A versão atualizada deverá estar disponível para consulta pública, respeitando o princípio da transparência previsto na Lei de Acesso à Informação (Lei nº 12.527/2011);

III. Sempre que revisada, a nova versão deverá ser comunicada formalmente a todas as Secretarias e setores municipais.

12.5 Responsabilidade da Alta Administração

A Alta Administração é responsável por:

I. Garantir o apoio institucional e financeiro necessário à implementação e manutenção das medidas de segurança da informação;

II. Aprovar esta política e suas atualizações;

III. Assegurar a integração da PSI aos instrumentos de planejamento e gestão pública, como o PDTI, o PPA, a LOA e o Plano de Governo Digital.

➡ Base legal: art. 15, incisos I e IV da Lei nº 14.129/2021 (Lei do Governo Digital).

12.6 Revisão e Atualização

I. Esta Política deverá ser revisada anualmente, ou sempre que houver:

- a) alteração nas legislações aplicáveis (como atualizações da LGPD, ANPD ou normas técnicas);
- b) mudanças tecnológicas significativas;
- c) recomendações de auditorias internas, externas ou do Tribunal de Contas;
- d) incidentes de segurança relevantes que indiquem necessidade de revisão.

II. A revisão será coordenada pelo Comitê Municipal de Segurança da Informação e Proteção de Dados, com apoio da área de Tecnologia da Informação e da Assessoria Jurídica.

III. A versão revisada deverá ser submetida à aprovação da Alta Administração Municipal e registrada formalmente por decreto ou portaria.

Prefeitura Municipal de Bocaina
Estado de São Paulo

12.7 Vigência

I. Esta Política entra em vigor na data de sua aprovação e publicação oficial, passando a integrar o conjunto normativo da Prefeitura Municipal de Bocaina/SP;

II. Sua aplicação é obrigatória e imediata a todos os servidores, colaboradores e prestadores de serviço vinculados à administração municipal;

III. Ficam revogadas as disposições internas anteriores que tratem de segurança da informação em sentido diverso.

12.8 Disposição Final

A Política de Segurança da Informação da Prefeitura Municipal de Bocaina – Estado de São Paulo, tem por finalidade fortalecer a governança pública digital, garantir a continuidade dos serviços, proteger o patrimônio informacional e assegurar o cumprimento dos princípios constitucionais da legalidade, moralidade, eficiência, publicidade e segurança jurídica, promovendo uma administração pública moderna, confiável e transparente.

Bocaina, em 29 de dezembro de 2025.

Caio Augusto Crepaldi
Prefeito Municipal

Prefeitura Municipal de Bocaina
Estado de São Paulo

PLANO DE CONTINUIDADE DE SERVIÇOS (PCS)

Prefeitura Municipal de Bocaina – Estado de São Paulo

1. Finalidade

O Plano de Continuidade de Serviços (PCS) tem por objetivo garantir a manutenção ou rápida retomada das atividades essenciais da Prefeitura Municipal de Bocaina em caso de interrupções, incidentes, falhas técnicas, desastres naturais, ataques cibernéticos ou qualquer evento que comprometa a disponibilidade dos serviços públicos.

O PCS assegura a resiliência organizacional, a continuidade das operações críticas e o cumprimento das obrigações legais, minimizando impactos sobre cidadãos, servidores e parceiros institucionais.

2. Base Legal e Normativa

- Lei nº 14.129/2021 (Lei do Governo Digital) – art. 15, incisos II e IV;
- Lei nº 13.709/2018 (LGPD) – art. 46 (segurança e continuidade de dados pessoais);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- ABNT NBR ISO 22301:2020 – Sistema de Gestão da Continuidade de Negócios;
- ABNT NBR ISO/IEC 27031:2022 – Continuidade de serviços de tecnologia da informação;
- Portaria SGD/ME nº 9.907/2022 – Diretrizes de segurança e continuidade para órgãos públicos.

3. Escopo

O PCS abrange:

- Todos os órgãos, secretarias, departamentos e autarquias da Prefeitura;
- Sistemas, bancos de dados e serviços digitais essenciais;
- Infraestruturas críticas (datacenter, rede municipal, energia, comunicações);
- Atividades administrativas e operacionais indispensáveis à execução das funções públicas.

4. Objetivos Específicos

I. Proteger as operações críticas da Prefeitura contra interrupções;

II. Assegurar a retomada rápida dos serviços essenciais;

III. Reduzir perdas financeiras, operacionais e reputacionais;

IV. Cumprir as exigências legais de continuidade e segurança da informação;

V. Definir responsabilidades, fluxos e procedimentos de recuperação.

5. Estrutura de Governança

A execução e manutenção do PCS serão coordenadas por:

Função	Responsabilidade
Comitê de Continuidade de Serviços (CCS)	Aprova e supervisiona o PCS.
Coordenador de Tecnologia da Informação (TI)	Implementa medidas de contingência e recuperação dos sistemas.
Encarregado de Dados (DPO)	Garante que os processos de continuidade respeitem a LGPD.
Gestores de Diretorias	Identificam processos críticos e planos alternativos de execução.
Controladoria Interna	Fiscaliza a aplicação do PCS.

6. Identificação dos Serviços Críticos

Os serviços considerados essenciais à continuidade administrativa e social do Município são:

Serviço / Sistema	Órgão Responsável	Impacto da Interrupção	Tempo Máximo de Interrupção Tolerável (RTO)
Folha de Pagamento	Diretoria de Administração / RH	Alto	48 horas
Sistema Contábil e Financeiro	Tesouraria / Contabilidade	Alto	24 horas
Sistema de Arrecadação Tributária	Finanças / Tributação	Alto	24 horas
Sistema da Saúde (Prontuários e E-SUS)	Diretoria de Saúde	Alto	12 horas
Sistema Educacional	Diretoria de Educação	Médio	72 horas
Sistema de Protocolo e Documentos	Diretoria de Administração	Médio	48 horas
E-mail Institucional	TI	Médio	48 horas
Portal da Transparência	Controladoria / TI	Baixo	72 horas

7. Análise de Riscos e Impactos

Os principais riscos à continuidade dos serviços incluem:

Tipo de Risco	Exemplo	Impacto	Probabilidade	Ação Preventiva
Falha elétrica	Queda de energia na sede	Alto	Média	Nobreaks, gerador e pontos alternativos de energia
Ataque cibernético	Ransomware ou phishing	Alto	Média	Firewall, antivírus, backup e treinamento de servidores
Desastre natural	Enchente ou incêndio	Alto	Baixa	Cópias off-site e plano de evacuação
Falha de sistema	Erro em servidor ou software	Médio	Alta	Backup diário e redundância de sistemas
Erro humano	Exclusão ou alteração indevida	Médio	Alta	Treinamento e revisão de acessos
Interrupção de internet	Queda de provedor	Médio	Média	Contrato com provedor secundário

8. Estratégias de Continuidade

1. Redundância tecnológica: sistemas críticos hospedados com cópias locais e backup em nuvem;

2. Infraestrutura alternativa: previsão de ponto físico secundário para operação emergencial (ex.: prédio anexo ou escola municipal com rede segura);

3. Procedimentos manuais emergenciais: planilhas e formulários físicos para registros temporários;

4. Comunicação de crise: canal institucional (WhatsApp corporativo, telefone fixo alternativo e e-mail de contingência);

5. Prioridade de restauração: os sistemas da Saúde, Finanças e Administração devem ter prioridade máxima;

6. Equipe de resposta: designar técnicos e gestores para atuar em plantão emergencial durante incidentes.

9. Plano de Ação Imediata (Situações de Crise)

Fase 1 – Detecção e Avaliação

- Confirmar o incidente ou interrupção;
- Registrar ocorrência em formulário padrão;
- Comunicar o Gestor de TI e o Comitê de Continuidade.

Fase 2 – Resposta e Contenção

- Isolar o problema (sistemas afetados, rede, área física);
- Acionar backup mais recente;
- Implementar plano de contingência operacional.

Fase 3 – Recuperação

- Restaurar sistemas e validar integridade dos dados;
- Retomar gradualmente os serviços essenciais;
- Registrar relatório técnico e comunicar a Alta Administração.

Fase 4 – Pós-Incidente

- Avaliar causas e impactos;
- Atualizar o PCS conforme lições aprendidas;
- Realizar comunicação institucional e registro de auditoria.

10. Comunicação e Notificação

Durante incidentes ou interrupções:

I. A comunicação interna será coordenada pela Secretaria de Administração;

II. A comunicação externa será feita somente por autoridade designada (Prefeito ou Assessoria de Comunicação);

III. Em incidentes com dados pessoais, o DPO deverá avaliar a necessidade de notificação à ANPD e aos titulares, conforme art. 48 da LGPD.

11. Testes e Simulações

I. O PCS deverá ser testado anualmente, com simulações de falhas elétricas, indisponibilidade de rede e perda de dados;

II. Os testes devem ser documentados, registrando resultados, falhas e planos de melhoria;

III. O Comitê de Continuidade revisará o plano com base nas evidências dos testes.

12. Atualização e Melhoria Contínua

I. O PCS deverá ser revisado sempre que ocorrer:

- Mudança de infraestrutura ou de sistemas;
- Alteração de responsabilidades;
- Ocorrência de incidentes reais;
- Atualização legal ou normativa.

II. A revisão será coordenada pelo Comitê de Continuidade, com apoio da TI e da

Prefeitura Municipal de Bocaina
Estado de São Paulo

Controladoria.

III. As versões revisadas deverão ser aprovadas pela Alta Administração e publicadas internamente.

13. Vigência

O presente Plano entra em vigor na data de sua aprovação pela Alta Administração Municipal, e deverá ser integrado ao Plano Diretor de Tecnologia da Informação (PDTI) e à Política de Segurança da Informação (PSI), permanecendo em constante atualização e monitoramento.

Bocaina, em 29 de dezembro de 2025.

Caio Augusto Crepaldi
Prefeito Municipal

Prefeitura Municipal de Bocaina

Estado de São Paulo

DECRETO Nº 099/25

Regulamenta a Lei Federal nº 14.129/2021, de 29 de Março de 2021.

O Prefeito do Município de Bocaina, Estado de São Paulo, no uso de suas atribuições legais;

DECRETA:

DISPOSIÇÕES GERAIS

Art. 1º Fica instituído no âmbito da Administração Direta o Programa Municipal de Governo Digital.

Art. 2º O Programa Municipal de Governo Digital terá as seguintes diretrizes:

I – a manutenção dos serviços digitais disponíveis, bem como a garantia da sua evolução tecnológica;

II – ampliação da oferta de serviços digitais;

III - aproximação entre a gestão municipal e o cidadão;

IV – uso da tecnologia e da inovação como habilitadoras da inclusão diminuindo as desigualdades;

V – busca da permanente melhoria dos processos e ferramentas de atendimento ao cidadão;

Art. 3º A Diretoria de Administração e Finanças junto com a Coordenadoria de Tecnologia da Informação, em parceria com os órgãos e entidades da Administração Direta, coordenará o estudo para a ampliação dos serviços digitais públicos.

DA DIGITALIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA E DA PRESTAÇÃO DIGITAL DE SERVIÇOS PÚBLICOS

Art. 4º A Administração Pública Municipal poderá criar instrumentos para desenvolvimento de capacidades individuais e organizacionais necessárias à transformação digital, com o objetivo de:

I - criar e avaliar estratégias e conteúdos para o desenvolvimento de competências para a transformação digital entre servidores municipais;

II - pesquisar, desenvolver e testar métodos, ferramentas e iniciativas para a colaboração entre servidores municipais e cidadãos no desenho de soluções focadas na transformação digital.

Art. 5º As Plataformas de Governo Digital são ferramentas digitais e serviços comuns aos órgãos municipais, ofertados de forma centralizada e compartilhada, necessários para a oferta digital de serviços, devendo possuir pelo menos as seguintes funcionalidades:

I - ferramenta digital de solicitação de atendimento e de acompanhamento da entrega dos serviços públicos;

II - painel de monitoramento do desempenho dos serviços públicos.

§1º As Plataformas de Governo Digital deverão ser acessadas por meio de portal, de aplicativo ou de outro canal digital único e oficial, para a disponibilização de informações institucionais, notícias e prestação de serviços públicos.

§2º As funcionalidades deverão observar padrões de interoperabilidade e a necessidade de integração de dados como formas de simplificação e de eficiência nos processos e no atendimento aos usuários.

Art. 6º Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos deverão, no âmbito de suas respectivas competências:

I - manter atualizadas as informações institucionais e as comunicações de interesse público, principalmente as referentes à Carta de Serviços ao Cidadão;

II - monitorar e implementar ações de melhoria dos serviços públicos prestados, com base nos resultados da avaliação de satisfação dos usuários dos serviços;

III - integrar os serviços públicos às ferramentas de notificação aos usuários, de assinatura eletrônica, quando aplicáveis;

IV - eliminar, inclusive por meio da interoperabilidade de dados, exigências desnecessárias quanto à apresentação, pelo usuário, de informações e de documentos comprobatórios prescindíveis;

V - aprimorar a gestão das suas políticas públicas com base em dados e em evidências por meio da aplicação de inteligência de dados em plataforma digital;

Art. 7º Os órgãos e entidades prestadores de serviços públicos buscarão oferecer aos cidadãos a possibilidade de formular sua solicitação, sempre que possível, por meio eletrônico.

DOS DIREITOS DOS USUÁRIOS DA PRESTAÇÃO DIGITAL DE SERVIÇOS PÚBLICOS

Art. 8º São garantidos os seguintes direitos aos usuários da prestação digital de serviços públicos

I - gratuidade no acesso às Plataformas de Governo Digital;

II - atendimento nos termos da Carta de Serviços ao Cidadão;

III - padronização de procedimentos referentes à utilização de formulários, de guias e de outros documentos congêneres, incluídos os de formato digital;

IV - recebimento de protocolo, físico ou digital, das solicitações apresentadas;

DA INTEROPERABILIDADE DE DADOS ENTRE ÓRGÃOS PÚBLICOS

Art. 9º Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, deverão gerir suas ferramentas digitais, tendo em consideração:

I - a interoperabilidade de informações e de dados sob sua gestão, respeitadas as restrições legais, os requisitos de segurança da informação e comunicação, as limitações tecnológicas e a relação custo benefício da interoperabilidade;

DO USO DE DADOS

Art. 10. Os órgãos e entidades da Administração direta promoverão o uso de dados para a construção e o acompanhamento das políticas públicas, respeitados a Lei Federal nº 13.709, de 2018.

DOS SERVIÇOS DIGITAIS PÚBLICOS DISPONÍVEIS

Art. 11. Os serviços digitais públicos disponíveis e em operação, são os seguintes:

- Carta de Serviços ao Usuário;
- Transparência Municipal;
- e-Sic : Sistema Eletrônico de Informação ao Cidadão;
- Diário Oficial do Município;
- Programa de Dados Abertos;
- Consulta Concursos Públicos e Processos Seletivos;
- Legislação municipal;
- Nota Fiscal Eletrônica;
- Serviços Online Imobiliário e Mobiliário;
- Sistema Web de Ouvidoria;

Prefeitura Municipal de Bocaina

Estado de São Paulo

DISPOSIÇÕES FINAIS

Art. 12. O acesso para o uso de serviços públicos poderão ser garantidos total ou parcialmente pela Administração, com o objetivo de promover o acesso universal à prestação digital dos serviços.

Art. 13. Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Bocaina, em 29 de dezembro de 2.025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrado na Secretaria, na data acima.

Denise Chotti
Agente Administrativo

Prefeitura Municipal de Bocaina

Estado de São Paulo

DECRETO Nº 100/25

Regulamenta a política de acesso às informações públicas no âmbito do Município de BOCAINA, bem como institui regras específicas complementares às normas gerais estabelecidas pela Lei nº 12.527, de 18 de Novembro de 2011 – Lei de Acesso à informação Pública – e dá outras providências.

O Prefeito do Município de Bocaina, Estado de São Paulo, no uso de suas atribuições legais;

DECRETA:

Art. 1º Este Decreto regulamenta, no âmbito do Poder Executivo Municipal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações, previsto no inc. XXXIII do "caput" do art. 5º, no inc. II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Os órgãos e entidades públicas municipais promoverão, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por ele produzidas ou custodiadas, recolhidos ou não a arquivos públicos.

Art. 2º Os procedimentos previstos neste Decreto destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I – observância da publicidade como preceito geral e do sigilo como exceção;

II – observância da política municipal de arquivos e gestão de documentos;

III - divulgação de informações de interesse público, independentemente de solicitações;

IV – utilização de meios de comunicação viabilizados pela tecnologia da informação;

V – fomento ao desenvolvimento da cultura de transparência na administração pública;

VI - contribuição para o desenvolvimento do controle social da administração pública.

Art. 3º Para os efeitos deste Decreto, os termos informação; documento; informação sigilosa; informação pessoal; tratamento da

informação, disponibilidade; autenticidade; integridade e primariedade, seguem as definições do artigo 4º da Lei nº 12.527, de 2011.

Art. 4º Sujeitam-se ao disposto neste Decreto, no âmbito do Município de Bocaina:

I - as Diretorias e Órgãos da Administração Centralizada da Prefeitura Municipal de Bocaina;

II - as entidades privadas sem fins lucrativos, no que couber, que recebam recursos públicos diretamente do orçamento ou mediante auxílios, subvenções sociais, contratos de gestão, termos de parceria, convênios, acordos, ajustes ou outros instrumentos congêneres.

Art. 5º O acesso à informação, conforme regulamentado neste Decreto, não se aplica:

I - às hipóteses de sigilo previstas na legislação, como fiscal, bancário, comercial, profissional, industrial, segredo de justiça; e

II - a garantia das medidas de proteção aos cidadãos em situação de violência, risco de vida ou outro episódio de ameaça grave ou coação.

Art. 6º É dever dos órgãos e entidades promover, independentemente de requerimentos, a divulgação, na rede mundial de computadores ("Internet"), através de sítio eletrônico, de informações de interesse coletivo ou geral por elas produzidas ou custodiadas, devendo constar, no mínimo:

I - registro de suas competências e estrutura organizacional,dos endereços e telefones das respectivas unidades e dos horários de atendimento ao público;

II - registros de quaisquer repasses ou transferências de recursos financeiros;

III - execução orçamentária e financeira detalhada;

IV - informações concernentes a procedimentos licitatórios,inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

V - dados gerais para o acompanhamento de programas,ações, projetos e obras;

VI - remuneração dos Servidores, folha de pagamento e quadro de pessoal; e

VII - respostas a perguntas mais frequentes da sociedade.

§ 1º As informações e documentos deverão permanecer disponíveis na Internet pelo prazo de guarda estabelecido na Tabela de Temporalidade de Documentos.

§ 2º O sítio a que se refere o "caput" deste artigo deverá atender aos seguintes requisitos:

I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;

Prefeitura Municipal de Bocaina
Estado de São Paulo

II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio;

VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei Federal nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008; e

IX - disponibilizar informações de referências e de instrumentos de pesquisa para acesso a documentos originais independente de suporte.

Art. 7º A Diretoria Municipal de Administração é o órgão responsável pela gestão do Portal Transparência e pela monitoria do Serviço de Informações ao Cidadão (SIC).

Art. 8º A Diretoria Municipal de Finanças é responsável por fornecer as informações referentes a receita e despesa, em tempo real; despesa de custeio; balanço das finanças públicas; diárias e passagens aéreas; relatórios da Lei Complementar Federal nº 101, de 4 de maio de 2000 (Lei de responsabilidade Fiscal).

Art. 9º O departamento de Recursos Humanos do Município é responsável pela gestão das informações referentes ao quadro funcional, à folha de pagamento e à contratação de pessoal em caráter emergencial, sendo responsável por fornecer as informações no âmbito de sua competência, bem como promover a articulação e a integração com os demais órgãos da administração também sendo responsável por efetuar a gestão do sistema de documentação da AC, orientando os demais departamentos da administração.

Art. 10. As informações relativas às licitações, a convênios ou instrumentos congêneres e à contratação de serviços terceirizados devem ser fornecidas pelos departamentos no âmbito de sua competência.

Art. 11. Fica criado o SIC no âmbito do Poder Executivo do Município de Bocaina.

Art. 12. O SIC terá como objetivos específicos:

I - atender e orientar o público quanto ao acesso à informação;

II - receber e registrar pedidos de acesso à informação; e

Prefeitura Municipal de Bocaina

Estado de São Paulo

III - informar sobre a tramitação de documentos nas unidades.

Art. 13. Compete ao SIC:

I - o recebimento do pedido de acesso e, sempre que possível, o fornecimento imediato da informação;

II - o registro do pedido de acesso em sistema eletrônico específico e a entrega de número do protocolo, que conterá a data de apresentação do pedido;

III - o encaminhamento do pedido ao órgão e entidade responsável pelo fornecimento da informação, quando couber.

Art. 14º O SIC será oferecido nas modalidades presencial, virtual e telefônica.

§ 1º Na modalidade presencial, o SIC será operacionalizado no setor do Protocolo Municipal.

§ 2º Na modalidade virtual, o SIC será disponibilizado em seção específica no sítio da Municipalidade.

§ 3º Na modalidade telefônica, o SIC será operacionalizado, exclusivamente, através do telefone tronco da Municipalidade.

Art. 15º Qualquer pessoa, natural ou jurídica, poderá formular pedido de acesso à informação por meio de formulário padrão através das modalidades oferecidas pelo SIC e receberá número do registro de protocolo.

Parágrafo único. Em casos presenciais o agente público deverá entregar cópia do pedido protocolado.

Art. 16º O pedido de acesso à informação deverá conter:

I - nome do requerente;

II - número do Cadastro de Pessoa Física (CPF) ou Cadastro Nacional de Pessoa Jurídica (CNPJ) ou número de documento válido, quando estrangeiro;

III - especificação, de forma clara e precisa, da informação requerida; e

IV - endereço físico ou eletrônico do requerente, para recebimento de comunicações ou da informação requerida.

Art. 17º Não serão atendidos os pedidos de acesso à informação:

I - genéricos ou desproporcionais;

II - classificados com o grau de sigilo reservado; ou

III - que exijam trabalhos adicionais de análise e interpretação de dados e informações.

Parágrafo único. Em todas as hipóteses previstas neste Decreto, o SIC responderá ao requerente da impossibilidade de prestar a informação solicitada.

Art. 18º Recebido o pedido e estando a informação disponível, o acesso será imediato.

Parágrafo único. Caso não seja possível o acesso imediato, o órgão ou entidade deverá, no prazo de até 20 (vinte) dias, a contar do 1º dia

Prefeitura Municipal de Bocaina

Estado de São Paulo

útil após recebimento do pedido, realizar os tramites necessários para ter acesso às informações solicitadas de modo a responder o pedido.

Art. 19º O prazo para resposta do pedido poderá ser prorrogado por 10 (dez) dias, mediante justificativa encaminhada ao requerente.

Art. 20º O serviço de busca e fornecimento da informação é gratuito, salvo quando o fornecimento da informação implicar reprodução de documentos.

§ 1º Em casos de reprodução de documentos, o órgão ou entidade, observado o prazo de resposta ao pedido, disponibilizará ao requerente Guia de Documento de Arrecadação Municipal (DAM), para que seja providenciado o ressarcimento dos custos dos serviços e dos materiais utilizados.

§ 2º Fica isento de ressarcir os custos dos serviços e dos materiais utilizados aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da Lei Federal nº 7.115, de 29 de agosto de 1983.

Art. 21º Negado o pedido de acesso à informação, serão enviadas ao requerente, dentro do prazo de resposta, as seguintes informações:

I - razões da negativa de acesso e seu fundamento legal;

II - possibilidade e prazo de recurso, com indicação da autoridade

III - possibilidade de apresentação de pedido de desclassificação que o apreciará;

Art. 22º Este Decreto entrará em vigor na data da sua publicação ficando revogadas as disposições em contrário da informação ou documento com grau de sigilo reservado.

Bocaina, em 29 de dezembro de 2.025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrado na Secretaria, na data acima.

Denise Chotti
Agente Administrativo

Prefeitura Municipal de Bocaina

Estado de São Paulo

DECRETO N° 101/25

Dispõe sobre abertura de Crédito Adicional Suplementar e dá providências correlatas.

Caio Augusto Crepaldi, Prefeito do município de Bocaina, Estado de São Paulo, usando de atribuições que lhe são conferidas pela Lei nº 3178, Art 4°, de 18 de fevereiro de 2025 , resolve:

Art. 1º - Fica aberto, crédito adicional no valor de R$ 36.665,60 (Trinta e Seis Mil, Seiscentos e Sessenta e Cinco Reais e Sessenta Centavos),afim de suplementar a seguinte dotação orçamentária:

02.00.00 – Prefeitura Municipal

02.03.07 – Outras Transf e Convênios do Ensino				
325	4.4.90.51.00	12.365.0006.1029	Obras e Instalações	
			Vínculo 01.210.000	36.665,60
			Subtotal	**36.665,60**
			Total	**36.665,60**

Art. 2º - Os recursos necessários para a pronta execução deste decreto, serão aqueles provenientes de anulação parcial da seguinte dotação orçamentária:

02.03.07 – Outras Transf e Convênios do Ensino				
324	4.4.90.51.00	12.365.0006.1029	Obras e Instalações	
			Vínculo 02.210.022	36.665,60
			Subtotal	**36.665,60**
			Total	**36.665,60**

Art.3º - Esta decreto entrará em vigor na data de sua publicação.

Bocaina, em 29 de dezembro de 2025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrado na Secretaria, na data acima.

Denise Chotti
Agente Administrativo

Prefeitura Municipal de Bocaina

Estado de São Paulo

PORTARIA Nº 194/25

Revoga a Portaria n°116/2025, de 31 de julho de 2025.

CAIO AUGUSTO CREPALDI, Prefeito do município de Bocaina, Estado de São Paulo, usando de atribuições que lhe são conferidas pela lei, Resolve:

Art. 1º - Fica revogada a Portaria nº 116/25, de 31 de julho de 2025, que designou a servidora MARIA AMELIA MAREGA BAROQUELLO, PEB- I Ensino Fundamental, para prestação de serviços nos Órgãos da Diretoria Municipal de Educação, para exercer atividades inerentes ou correlatas ao Magistério, de acordo com a Lei 2874 de 09 de abril de 2020, que dispõe sobre o Plano de Cargos , Carreiras e Remuneração do Magistério da Prefeitura Municipal de Bocaina, SP.

Art. 2º - Esta portaria entrará em vigor na data da sua publicação.

Bocaina, em 29 de dezembro de 2025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrada na Secretaria, na data acima.

Denise Chotti
Agente Administrativo

Prefeitura Municipal de Bocaina

Estado de São Paulo

PORTARIA Nº 195/25

Dispõe sobre a nomeação dos membros do Conselho Municipal de Segurança da Informação.

CAIO AUGUSTO CREPALDI, Prefeito do Município de Bocaina, Estado de São Paulo, usando de atribuições que lhe são conferidas por Lei;

Considerando a necessidade de implementar e manter a Política de Segurança da Informação no âmbito da administração pública municipal;

Considerando a importância de estabelecer diretrizes, normas e procedimentos para garantir a integridade, confidencialidade e disponibilidade das informações;

Considerando o disposto na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº 13.709/2018) e demais normativos aplicáveis;

RESOLVE:

Art. 1º Fica instituído o Conselho Municipal de Segurança da Informação, com a finalidade de planejar, propor, acompanhar e avaliar as ações relacionadas à segurança da informação no âmbito da administração pública municipal.

Art. 2º Ficam nomeados os seguintes membros para compor o Conselho:

I. Camila Aparecida Navegante Pereira: Diretora Municipal de Administração e Finanças

II. Renato Benedito Doretto - Coordenador de Tecnologia da Informação

III. Agnaldo Luiz Navegante - Técnico em Tecnologia da Informação

IV. Rodrigo Tosi Zanutto - Técnico em Tecnologia da Informação (DPO Nomeado)

V. Viviani Bernardo Frare Serra - Procuradora Jurídica

VI. Rita de Cassia Aparecida de Castro - Atendente (ouvidoria)

Art. 3º O Conselho será coordenado pelo servidor Renato Benedito Doretto, Coordenador de Tecnologia da Informação, que também atuará como Autoridade Municipal de Segurança da Informação.

Art. 4º Compete ao Conselho:

I. Estabelecer diretrizes e ações para proteção das informações institucionais;

II. Propor normas e procedimentos relacionados à segurança da

Prefeitura Municipal de Bocaina

Estado de São Paulo

informação e proteção de dados pessoais;

III. Acompanhar e fiscalizar o cumprimento das políticas de segurança da informação no município;

IV. Deliberar sobre incidentes de segurança e recomendar providências.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

Bocaina, em 29 de dezembro de 2025.

Caio Augusto Crepaldi
Prefeito Municipal

Registrado na Secretaria, na data acima.

Denise Chotti
Agente Administrativo