Guia de Boas Práticas da Política de Segurança da Informação

Protegendo os Dados da Cidade de Pompeia

Prefeitura Municipal de Pompeia | Tecnologia da Informação

Nossa Missão: Proteger o Maior Ativo de Pompeia – a Informação.

Este guia não é apenas um conjunto de regras. É o nosso compromisso compartilhado para proteger as informações que nos são confiadas pelos cidadãos e garantir o bom funcionamento da nossa cidade. A segurança da informação protege contra vazamentos, fraudes e paralisações de serviços, assegurando a conformidade com leis como a LGPD (Lei Geral de Proteção de Dados - Lei nº 13.709/2018).

Cidadão Protegido

Serviços Públicos Ativos

Conformidade Legal

A segurança da informação é uma responsabilidade de todos nós: servidores, estagiários, prestadores de serviços e fornecedores.

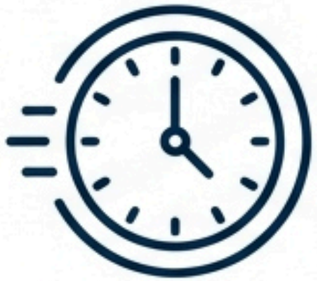
Os 6 Princípios que Guiam Nossas Ações

Confidencialidade

A informação certa, apenas para as pessoas autorizadas.

Integridade

Garantir que a informação seja sempre precisa e completa, sem alterações indevidas.



Disponibilidade

A informação acessível e pronta para uso sempre que necessário.

Rastreabilidade

Registrar quem fez o quê e quando, garantindo a transparência e a auditoria.

Conformidade

Seguir rigorosamente as leis e normas, como a LGPD e o Marco Civil da Internet.

Responsabilização

Cada um de nós é responsável pelo uso correto e seguro das informações.

Um Pacto de Segurança: Nosso Papel e o Seu Papel

Nosso Papel (A Prefeitura)

O que nós garantimos

A Prefeitura de Pompeia se compromete a fornecer a estrutura, as ferramentas e os processos para um ambiente digital seguro.

Seu Papel (O Colaborador)

O que esperamos de você

Sua atenção e suas ações diárias são a linha de frente da nossa defesa. Você é um guardião essencial das nossas informações.

Nosso Compromisso: A Estrutura de Proteção da Prefeitura

Investimos continuamente em tecnologia e processos para proteger nossos ativos de informação.

Controle de Acesso

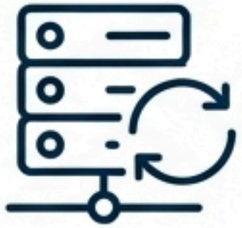
Acesso liberado apenas ao que é necessário para sua função (princípio do menor privilégio).

Defesas de Rede

Firewalls, segmentação de rede e sistemas de detecção de intrusão (IDS/IPS).

Segurança Física

Controle de acesso e monitoramento de áreas críticas, como salas de servidores.



Backups e Recuperação

Cópias de segurança diárias e testes de restauração trimestrais.

Criptografia

Proteção de dados em trânsito (TLS 1.2+) e em dispositivos.

Atualizações e Softwares

Manutenção de sistemas atualizados e uso exclusivo de softwares licenciados e homologados.

Sua Missão: Suas Responsabilidades Diárias na Segurança

- **Proteger suas credenciais:** Suas senhas são intransferíveis. Nunca as compartilhe.
- **Comunicar imediatamente:** Viu algo suspeito? Reporte na hora para a equipe de TI.
- **Respeitar a confidencialidade:** Trate as informações da Prefeitura com sigilo, mesmo após seu desligamento.
- **Manter a mesa limpa:** Documentos sensíveis não devem ficar expostos em sua mesa de trabalho.
- **Seguir as regras de uso:** Utilize e-mail, internet e sistemas apenas para fins institucionais.
- **Não compartilhar dados sem permissão:** Dados pessoais ou confidenciais só podem ser compartilhados com autorização explícita.

Senhas Fortes e Estações de Trabalho Seguras: Nossa Primeira Barreira

Criando Senhas Fortes

Sua senha deve ter:

No mínimo 7 caracteres.

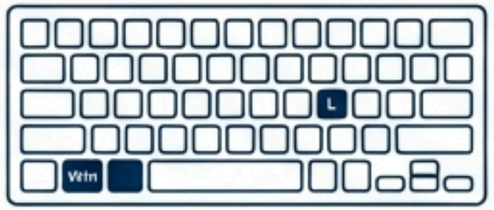
Troca obrigatória a cada 90 dias.

Use **autenticação de dois fatores (2FA)** sempre que disponível.

Protegendo sua Estação

Lembre-se sempre:

Seu computador será **bloqueado** automaticamente após **10 minutos** de inatividade.



Sempre bloqueie sua tela (**Win + L**) ao se ausentar da sua mesa, mesmo que por um instante.

Navegação Segura: O Uso Consciente de E-mail, Internet e Softwares

As ferramentas de trabalho da Prefeitura são para uso exclusivo institucional. O uso inadequado abre portas para ataques.

Cuidado com a Engenharia Social!

Desconfie de e-mails, mensagens ou ligações que pedem informações urgentes ou parecem boas demais para ser verdade. Isso é **Phishing.**

É proibido o uso de software pirata, não autorizado, e o acesso a sites ilícitos ou de risco.

WhatsApp e Telegram

O uso de aplicativos de mensagens em equipamentos da Prefeitura para fins de trabalho requer autorização e o máximo cuidado com a confidencialidade dos dados compartilhados.

Segurança Fora da Prefeitura: Regras Essenciais para Teletrabalho e BYOD

Se você trabalha remotamente ou usa seu dispositivo pessoal (Bring Your Own Device), estas regras são **obrigatórias**:

VPN Obrigatória

Todo acesso à rede da Prefeitura deve ser feito através da nossa Rede Privada Virtual (VPN).

Antivírus e Firewall Ativos

Seu dispositivo deve ter antivírus licenciado e firewall sempre atualizados.

Proibido Wi-Fi Público Aberto

Nunca utilize redes abertas (de cafés, aeroportos) para acessar dados da Prefeitura.

BYOD Seguro

Seu dispositivo pessoal só é permitido se tiver criptografia ativada, softwares licenciados e antivírus ativo. A responsabilidade pela segurança dos dados nele é sua.

Identificou uma Ameaça?
Aja Rápido e Comunique.

O que é um **Incidente de Segurança**?
Qualquer evento que comprometa ou ameace nossos dados, sistemas ou serviços. Exemplos: um e-mail de phishing que você clicou, a perda de um pendrive com dados de trabalho, ou um comportamento estranho no seu computador.

NÃO TENTE RESOLVER SOZINHO. NÃO TENHA MEDO DE REPORTAR.

Sua ação mais importante é **NOTIFICAR IMEDIATAMENTE** a equipe de Tecnologia da Informação e o Encarregado de Proteção de Dados (DPO).

Nosso Protocolo de Resposta: O que Acontece Após o Seu Alerta

1 Detecção e Notificação
Você reporta o incidente.

2 Contenção
A equipe de TI age para isolar o problema e impedir que se espalhe.

3 Investigação
Analisamos a causa e a extensão do incidente.

4 Recuperação
Restauramos os sistemas e dados para a normalidade.

5 Comunicação
Notificamos os órgãos competentes (como a ANPD) em até 72 horas, se necessário.

6 Relatório e Melhoria
Documentamos o que aconteceu e o que aprendemos para evitar que se repita.

Prevenção é o Melhor Remédio: Nosso Programa de Educação Contínua

A segurança da informação é um aprendizado constante. Por isso, mantemos um programa ativo de conscientização.

Treinamento Anual Obrigatório

- LGPD e tratamento de dados
- Como identificar Phishing e Engenharia Social
- Uso seguro de senhas e credenciais
- Procedimentos em caso de incidente

Simulações e Auditorias

Realizamos **simulações semestrais** de ataques (como e-mails de phishing falsos) para testar nossa atenção, além de **auditorias periódicas** para garantir a conformidade.

Nosso Pacto Formal: Responsabilidade e Consequências

O cumprimento desta política é uma condição para o trabalho na Prefeitura. O não cumprimento pode resultar em sanções administrativas, civis e criminais, aplicadas após Processo Administrativo Disciplinar, garantindo o contraditório e a ampla defesa.

O desconhecimento da política não é uma justificativa válida para seu descumprimento.

Ação Necessária

Todos os colaboradores deverão assinar o **Termo de Confidencialidade** e o **Termo de Responsabilidade do Usuário**, formalizando seu compromisso com a segurança da informação de Pompeia.

Dúvidas ou Incidentes? Fale Conosco.

A equipe de Segurança da Informação está aqui para ajudar.

E-mail: seguranca.ti@pompeia.sp.gov.br

Telefone: 34505-1530

A segurança é uma jornada, não um destino. Esta política é revisada a cada 2 anos para se adaptar a novas tecnologias e desafios. Contamos com você para manter Pompeia segura.