



DIRETRIZES DE BOAS PRÁTICAS DE

PROTEÇÃO DE DADOS



NO ÂMBITO DA SMSA-BH





DIRETRIZES DE BOAS PRÁTICAS DE

PROTEÇÃO DE DADOS



NO ÂMBITO DA SMSA-BH



Elaboração

Grupo de Trabalho LGPD-SMSA (Lei Geral de Proteção de Dados Pessoais - Secretaria Municipal de Saúde):

Helen Maria Ramos de Oliveira Lopes

Isabel Maria Gomes Soares

Janete dos Reis Coimbra

Lídia de Sousa

Luiz Cláudio da Silva Barros

Mariana Reis Giuliani

Mariela Bauer Porto Gonçalves

Marília de Azevedo Jannotti Guerra

Mayra Ferreira Tavares

Moisés Gonçalves de Oliveira

Paulo Roberto Lopes Correa

Ricardo Araújo Morais

Róger Alberto Schwetter Silveira

Salime Cristina Hadad

Sandra Cristina Paulucci Cavalcante de Andrade

Valeria Pinto Fonseca

Wanessa Ferreira da Rocha

Warley Aguiar Simões

Webert Gaioffato Silva

Projeto gráfico

Produção Visual - Assessoria de Comunicação Social

Secretaria Municipal de Saúde

SUMÁRIO

INTRODUÇÃO	3
1. LEI DE ACESSO À INFORMAÇÃO – LAI / DECRETO MUNICIPAL N° 14.906/2012	5
2. DADOS PESSOAIS DE SERVIDORES PÚBLICOS	7
3. GESTÃO DE DOCUMENTOS NA PBH / “TABELA DE TEMPORALIDADE”	8
4. CLÁUSULA DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS NOS INSTRUMENTOS E ADITIVOS CONTRATUAIS / CONVENIAIS	10
5. COMPARTILHAMENTO DE DADOS PESSOAIS	11
6. UTILIZAÇÃO DO CORREIO ELETRÔNICO NO ÂMBITO MUNICIPAL	13
7. UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO NO AMBIENTE COMPUTACIONAL DA PBH.....	14
8. USO DE APLICATIVOS DE MENSAGENS INSTANTÂNEAS E CHAMADAS DE VOZ	16
9. USO DO GOOGLE DRIVE	17
10. UTILIZAÇÃO DE REGISTRO / TRATAMENTO EM REPOSITÓRIOS NÃO ESTRUTURADOS.....	20
11. GESTÃO DO CONHECIMENTO / MUDANÇA	21
REFERÊNCIAS BIBLIOGRÁFICAS.....	23

INTRODUÇÃO

A Lei Geral de Proteção de Dados – LGPD – Lei 13.709, aprovada em 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais*¹ em âmbito nacional. Tem como foco principal oferecer ao titular dos dados maior conhecimento, controle e transparência na coleta, processamento, uso e compartilhamento de suas informações pessoais, tanto aquelas armazenadas em bancos de dados das instituições privadas e de órgãos públicos, como aquelas disponíveis em meios físicos¹.

Inicialmente, a adequação dos órgãos e entidades em relação à LGPD requer uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição, no caso, a Secretaria Municipal de Saúde (SMSA). Esta envolve: considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço (ou produto), até sua execução, assim como promover a sensibilização de todo o corpo funcional de agentes públicos sob sua gestão, visando a incorporação do respeito à privacidade dos dados pessoais nas atividades diárias da instituição².

A SMSA trata dados pessoais a todo momento – recebe e é guardiã de grande volume de informações.

Ao tratar dados dos usuários, a SMSA (assim como os demais órgãos da Administração) deve, sistematicamente, ponderar a real necessidade da solicitação de alguma informação específica para viabilizar a oferta do serviço (ou produto). Alguns dados pessoais*² estão sujeitos a cuidados ainda mais específicos, como os dados sensíveis*³ e os dados sobre crianças e adolescentes.

Os dados sensíveis, por suas características, podem expor o indivíduo social ou profissionalmente, de forma indesejada, dando margem a uma possível discriminação. Em razão disso, exigem a adoção, pelas entidades controladoras, de medidas de segurança mais rígidas, como por exemplo, a anonimização dos dados e camadas de proteção mais extensas¹.

*¹ Tratamento de dados é qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração¹.


*² Dados pessoais – informações relacionadas à pessoa natural identificada ou identificável como nome, data de nascimento, filiação, apelido, CPF, RG, BM, foto, endereço residencial, endereço de e-mail, endereço IP, cookies, hábitos de navegação, posição geolocalacional, formulários cadastrais, números de documentos¹.

*³ Dados sensíveis – informações de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde (prontuários e exames) ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural¹.

Quanto mais dados são coletados, maior a responsabilidade do Poder Público acerca da segurança da informação sob sua guarda.

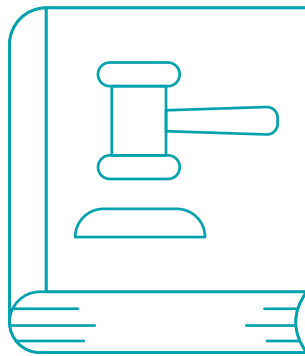
O objetivo deste documento não é esgotar ou abordar todos os aspectos da LGPD, mas dar elementos para uma apropriação do conteúdo da mesma e fornecer orientações de Boas Práticas no âmbito da SMSA para as operações de tratamento de dados pessoais, conforme artigo 50 da referida lei.

Dentre os processos que envolvem o tratamento de dados, alguns aspectos devem ser observados:

- 
- Lei de Acesso à Informação – LAI / Decreto Municipal nº 14.906/2012
 - Dados pessoais de servidores públicos
 - Gestão de documentos na PBH / “Tabela de Temporalidade”
 - Cláusula de adequação à Lei Geral de Proteção de Dados nos instrumentos e aditivos contratuais/conveniais
 - Compartilhamento de dados pessoais
 - Utilização do correio eletrônico no âmbito municipal
 - Utilização das estações de trabalho no ambiente computacional da PBH
 - Uso de aplicativos de mensagens instantâneas e chamadas de voz
 - Uso do Google Drive
 - Utilização de registro/tratamento em repositórios não estruturados
 - Gestão do conhecimento/mudança



1. LEI DE ACESSO À INFORMAÇÃO – LAI / DECRETO MUNICIPAL Nº 14.906/2012



O Decreto Municipal 14.906 de 15 de maio de 2012 que regulamenta a Lei de Acesso à Informação – LAI – no âmbito municipal, apresenta regras específicas com o fim de garantir o acesso à informação conforme previsto na referida Lei Federal, de nº 12.527, de 18 de novembro de 2011. Dessa forma, além da Lei Geral de Proteção de Dados, a Lei de Acesso à Informação e o Decreto Municipal nº 14.906/2012 devem ser sistematicamente interpretados.

Importante destacar que não existe conflito entre a LGPD e a LAI, sendo legislações harmônicas e interativas, visto que garantem os direitos fundamentais do indivíduo.

A LAI veio regulamentar o direito fundamental do cidadão ao acesso à informação previsto no art. 5º, XXXIII da Constituição da República de 1988, aperfeiçoando o controle popular das atividades da Administração Pública, ao passo que a LGPD dispõe sobre o tratamento dos dados pessoais, garantindo a proteção dos direitos fundamentais de liberdade e privacidade do indivíduo assegurados no art. 5º, X, da CR/88.

A proteção da privacidade não rivaliza com o direito à informação, buscando-se, sempre, conciliar o dever de transparência ao que deve ser público e o cuidado ao que é da esfera íntima e pessoal do indivíduo.

A Administração, quando da interpretação e operacionalização dessas legislações, terá que ficar atenta para não utilizar a LGPD sob o argumento de restringir informações obrigatoriamente públicas, haja vista que a principal finalidade da LAI é dar transparência às informações sob a guarda do Estado, cuja regra é a ampla divulgação, sendo o sigilo a exceção.

Ademais, a própria LAI, em seu art. 31, traz instrumentos de proteção à privacidade dos dados pessoais, não havendo, portanto, incompatibilidade com a LGPD. No entanto, podem ocorrer dúvidas, em especial no tocante ao que é considerado dado pessoal cujo acesso é público. Diante, pois, dos casos concretos postos à apreciação, deverá ser realizada uma ponderação de valores para tornar pública ou não uma informação pessoal, realizando uma análise acerca do interesse público que envolve a situação.

Dados pessoais podem e devem ser divulgados quando presente o interesse público e coletivo acerca daquela informação. A LGPD em seu art. 7º, §3º, reforça a publicidade da informação pessoal cujo acesso é público, DESDE QUE respeitadas a finalidade, boa-fé e interesse público na disponibilização desses dados.

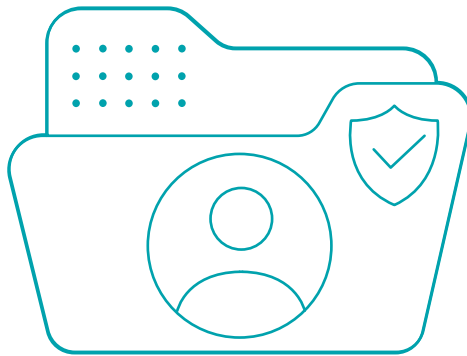
Podemos citar, como exemplo, a veiculação de informações como o nome e CPF dos sócios de empresas contratadas pela Administração, bem como a disponibilização da remuneração percebida pelos servidores públicos. Esses dados, embora pessoais, são de acesso público, cujo conhecimento importa para toda a coletividade, considerando serem informações que asseguram a transparência, o combate a desvios e conflitos de interesses no setor público, sendo, portanto, necessários para o controle social das atividades administrativas, que devem ser acompanhadas por todo e qualquer cidadão.

Nos cenários acima, não há interesse particular que impeça a divulgação dos dados pessoais: uma vez que as informações envolvem recursos públicos, estão revestidas de caráter estatal, estando ausente eventual conflito entre privacidade e publicidade. Considerando o interesse público e a legitimidade da sociedade em conhecer e acompanhar o desempenho dos agentes públicos e a execução dos contratos administrativos, a transparência na ampla divulgação das informações constitui o meio disponível para a fiscalização, o controle social e a viabilização dos princípios da probidade e impessoalidade administrativas.

A LGPD jamais pode ser utilizada para limitar avanços que criaram mecanismos que visam melhorar a transparência na seara pública: o intuito da lei é a proteção dos dados pessoais e não a proibição de sua utilização, que deve respeitar a finalidade e o interesse público quando de sua disponibilização.

Os direitos de privacidade e informação, ambos regulamentados pela LGPD e pela LAI, não se excluem e devem ser objeto de ponderação mediante situações conflituosas, levando em conta, sempre, a consecução do interesse público, sendo este o motivo determinante da possibilidade de eventual divulgação dos dados pessoais.

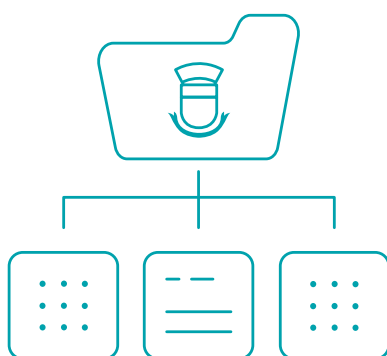
2. DADOS PESSOAIS DE SERVIDORES PÚBLICOS



Nos termos do art. 7º, § 3º da LGPD, o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Desta feita, dados pessoais de servidores públicos são considerados, de forma geral, de acesso público, podendo ser disponibilizados como forma de controle social das atividades e serviços públicos prestados.

Deverão, no entanto, ser sempre analisadas as razões dessa disponibilização. Por exemplo, divulgação nominal de agentes públicos que tiveram custeados com recursos públicos cursos de capacitação profissional, liberação de carga horária (a finalidade é prestar contas dos valores e recursos públicos despendidos). Uma forma de tornar públicos os resultados, neste caso, é a divulgação por meio dos registros funcionais (BM/matricula), por exemplo, sendo recomendável, como boa prática, informar àqueles que optarem pela realização de cursos, que a partir do momento da inscrição, o nome e BM (ou matrícula) serão divulgados para fins de prestação de contas.

3. GESTÃO DE DOCUMENTOS NA PBH / “TABELA DE TEMPORALIDADE”



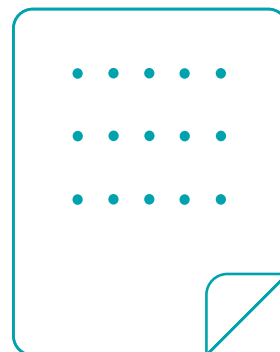
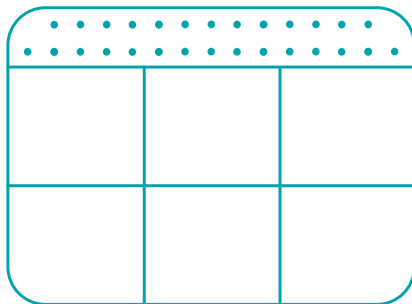
A SMSA é responsável por custodiar grande volume de dados pessoais e sensíveis, os quais se apresentam em diversos formatos, tais como textos não estruturados (em meio físico, em word, pdf, dentre outros), planilhas, páginas web, mensagens de correio eletrônico, imagens (por exemplo, digitalizações), sistemas informatizados mantidos em uma base de dados. Grande parte destes se constitui, ou contém documentos de arquivos*⁴. Assim, além da legislação de proteção de dados pessoais, é preciso também observar as orientações sobre a gestão de documentos na Prefeitura de Belo Horizonte, cujo órgão responsável é o Arquivo Público da Cidade de Belo Horizonte – APCBH. Essas devem ser consideradas conjuntamente na realização das operações com os dados pessoais.

*⁴ Documentos de arquivos são registros de informação em qualquer suporte: papel, plástico, magnético, dentre outros, produzidos e recebidos por um órgão público ou privado no exercício de suas atividades. Os documentos de arquivo possuem valor de prova e informação³.

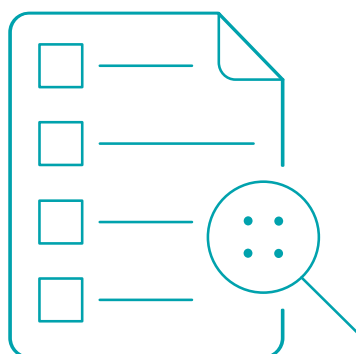
Cabe ressaltar que a gestão de documentos é o conjunto de procedimentos relacionados com:

- a produção de documentos;
- a tramitação dos documentos para outros setores;
- o uso dos documentos;
- a classificação dos documentos;
- a avaliação dos documentos pelo APCBH;
- a eliminação dos documentos após autorização do APCBH;
- a guarda dos documentos de arquivos nos órgãos públicos e no APCBH.

A efetiva gestão documental é fundamental, uma vez que, a ausência de normas, métodos e procedimentos de trabalho provocam o acúmulo desordenado de documentos, transformando os arquivos em meros depósitos de papéis que dificultam o acesso aos documentos e também a recuperação de informações necessárias para a tomada de decisões no âmbito institucional. Para evitar essa situação foi criada, em 1997, a **Tabela de Temporalidade de Destinação de Documentos de Arquivo**. O documento pode ser acessado no portal da Prefeitura de Belo Horizonte (www.pbh.gov.br), dentro de Estrutura de Governo/Fundações/Fundação Municipal de Cultura/Arquivo Público/Tabela de Temporalidade de Documentos.

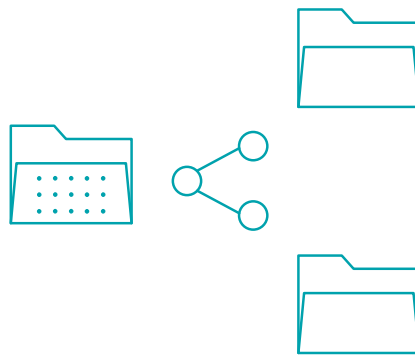


4. CLÁUSULA DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS NOS INSTRUMENTOS E ADITIVOS CONTRATUAIS / CONVENIAIS



Dado o relevante número de contratos sujeitos à adequação LGPD, foi elaborada minuta padrão, bem como o respectivo parecer que a aprova pela Procuradoria-Geral do Município. Caso haja discordância de algum contratado/conveniado com relação às cláusulas pré-aprovadas, ainda que parcialmente, é necessária a apresentação dos contrapontos indicados nos autos do processo administrativo, que deverá ser encaminhado pela Gerência de Contratos e Convênios para análise pela Assessoria Jurídica, que elaborará parecer jurídico prévio à formalização do novo termo aditivo, com a participação e ciência do Grupo de Trabalho LGPD. SMSA sobre tais alterações.

5. COMPARTILHAMENTO DE DADOS PESSOAIS



A LGPD permite o uso compartilhado de dados pessoais e sensíveis dos titulares entre os órgãos do poder público com a finalidade específica para a execução de políticas públicas e atribuição legal. Compartilhamento este autorizado, também, com entidades privadas, desde que estritamente necessário para a execução desta atividade pública e devidamente respaldado em contratos, convênios ou instrumentos congêneres.

Desta forma, a SMSA poderá tratar e compartilhar dados pessoais e de saúde necessários à execução da política de saúde, independentemente do consentimento dos usuários.

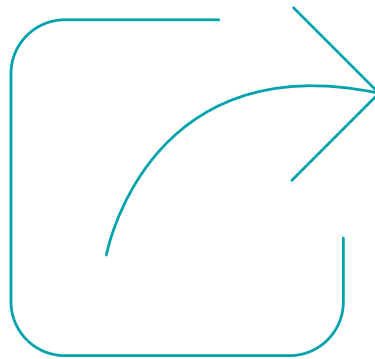
Importante destacar que a LGPD considera que existe compartilhamento de dados quando os mesmos são enviados para outros controladores*⁵ e prestadores de serviços externos, como hospitais ou laboratórios, outras secretarias e entes da PBH e demais órgãos externos (Secretaria de Estado da Saúde, Ministério da Saúde, Ministério Público, Defensoria Pública, Poder Judiciário, dentre outros).

*⁵ Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, sendo as responsáveis pela definição das medidas de segurança que serão aplicadas no tratamento desses dados.

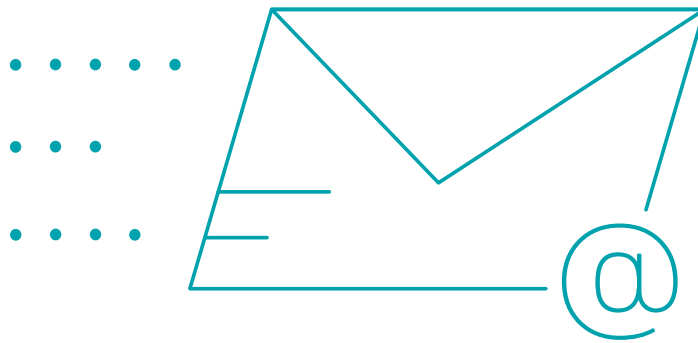
Entre as unidades internas da SMSA, a troca de informações entre as áreas não é considerada compartilhamento de dados e é possível o envio de informações, desde que de forma segura e com respeito à finalidade e necessidade do envio dos dados.

Seja na transmissão entre setores da SMSA, seja no compartilhamento com órgãos externos, as informações enviadas devem, sempre, respeitar o escopo e a finalidade da execução das políticas públicas definidas, sem incluir dados que não sejam os estritamente necessários para a execução e atendimento da política.

Assim, tanto dados pessoais presentes em sistemas informatizados, quanto informações registradas em repositórios não estruturados (planilhas eletrônicas, documentos físicos, dentre outros) podem ser trocadas entre setores internos da SMSA, mas é importante ficar atento quanto à forma como isso é feito: o acesso deve ser restrito apenas a quem de fato precisa acompanhar os casos, com processos bem definidos.



6. UTILIZAÇÃO DO CORREIO ELETRÔNICO NO ÂMBITO MUNICIPAL



O e-mail institucional (domínio@pbh.gov.br) constitui o meio eletrônico oficial de comunicação da PBH. As diretrizes e procedimentos para utilização deste estão elencados na Instrução Normativa nº 010/2015, a qual compõe a Política de Segurança da Informação do Município. A mesma encontra-se disponível na intranet da PBH (intranet.pbh.gov.br/instrucoes).

No que se refere à troca, transmissão ou compartilhamento de dados pessoais e/ou sensíveis por meio de documentos de arquivos digitais*⁶, é recomendado que seja utilizado o e-mail institucional, haja vista a segurança deste por seu caráter corporativo e por estar sob a responsabilidade da PBH e Prodabel, bem como sob as normas de segurança estabelecidas em contrato com a prestadora deste serviço.

*⁶ Exemplo de documentos arquivísticos digitais: planilhas eletrônicas, mensagens de correio eletrônico, sítios na internet, bases de dados e também textos, imagens fixas, imagens em movimento e gravações sonoras, dentre outras possibilidades, em formato digital³.

7. UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO NO AMBIENTE COMPUTACIONAL DA PBH



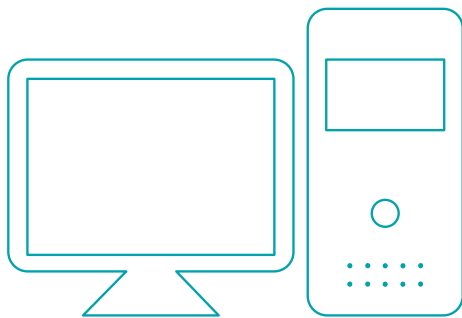
A Instrução Normativa nº 037/2020 dispõe sobre as diretrizes, regras, responsabilidades e procedimentos para a utilização, configuração, manutenção e movimentação das estações de trabalho no ambiente computacional da PBH. Foi elaborada pela Prodabel e pela Secretaria Municipal de Planejamento, Orçamento e Gestão (SMPOG) e é parte integrante da Política de Segurança da Informação do Município (Decreto Municipal nº15.423/13). A mesma encontra-se disponível na intranet da PBH (intranet.pbh.gov.br/instrucoes).

Algumas destas diretrizes merecem destaque por sua relevância na mitigação de riscos de vazamento de dados, dentre elas, as relacionadas às responsabilidades do agente público:

- Utilizar a estação de trabalho de acordo com as regras estabelecidas pela Prodabel, restringindo-se ao desempenho das suas atividades profissionais.
- Desligar de forma adequada e segura a estação de trabalho diariamente, no fim do expediente.
- Bloquear a estação de trabalho, sempre que se ausentar, para impedir o acesso não autorizado.
- Registrar solicitações ou incidentes identificados na estação de trabalho, por meio do SDM (Service Desk Manager).

Salientamos que, em consonância com a Política de Segurança da Informação, é dever do agente público:

- Responsabilizar-se, no âmbito de sua atuação, pela proteção e segurança da informação que lhe é confiada, devendo conhecer, entender e cumprir a Política estabelecida no Decreto, bem como as diretrizes e instruções correlatas, zelando por sua correta aplicação;
- Fazer uso correto e responsável dos recursos tecnológicos, pautando-se pela legalidade e conduta ética, sempre em conformidade com os princípios da Segurança da Informação;
- Comunicar ao seu superior hierárquico qualquer incidente de segurança ou situação de risco no âmbito de sua atuação, cientificando a Prodabel para as devidas providências.



8. USO DE APLICATIVOS DE MENSAGENS INSTANTÂNEAS E CHAMADAS DE VOZ

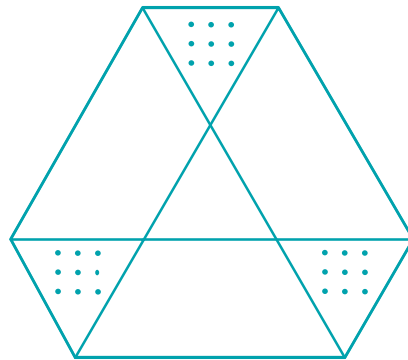


O e-mail institucional é a ferramenta/meio eletrônico oficial de comunicação da PBH. As boas práticas consideram que dados pessoais e/ou dados sensíveis somente devem trafegar em ambiente seguro, no caso, sob a responsabilidade da segurança corporativa dos sistemas e dos endereços eletrônicos institucionais.

Importante ressaltar que mesmo sendo utilizado com frequência, para troca de informações, não só por profissionais e gerências da PBH/SMSA, mas pelo público em geral, os aplicativos de mensagens instantâneas e chamadas de voz não são ferramentas de trabalho ou de comunicação oficial da PBH/SMSA. Não devem, portanto, ser utilizados para envio de documentos ou de informações que contenham dados pessoais e/ou sensíveis.

9.

USO DO GOOGLE DRIVE



A ferramenta Google Drive é uma forma de armazenamento em nuvem que facilita o compartilhamento de informações em tempo real, permitindo que equipes trabalhem em um mesmo documento ao mesmo tempo e de dispositivos diferentes.

Tem sido muito utilizada por ser uma ferramenta que facilita a guarda e construção de documentos, principalmente considerando a modalidade de teletrabalho. Mas é imprescindível estar atento a alguns pontos para aumentar a segurança da mesma, uma vez que documentos sigilosos e importantes podem estar sendo compartilhados na nuvem.

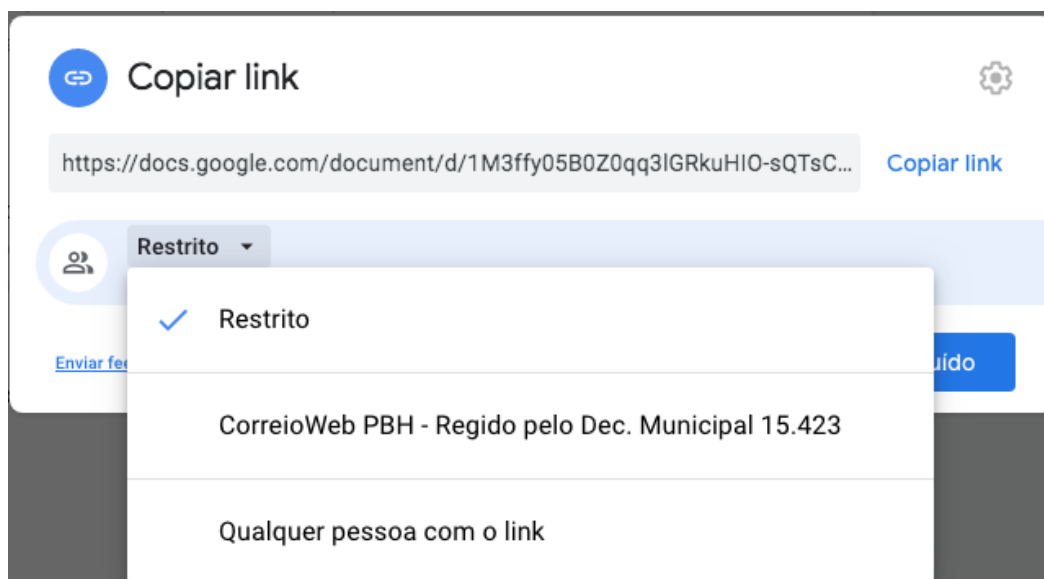
Ao usar o google drive para colaborar em documentos, é preciso se certificar de quais são as permissões que estão sendo concedidas para as pessoas com quem está sendo compartilhado o arquivo. Você pode compartilhar pastas e arquivos convidando pessoas por meio de um link ou e-mail, e para todas as opções é possível escolher quem pode editar o documento, quem pode apenas visualizar ou apenas comentar.

Ainda na configuração do compartilhamento você pode assinalar se permite que os editores possam alterar permissões e compartilhar com outros usuários e se os leitores e comentaristas podem imprimir, fazer download ou copiar. Para configurar essas restrições, basta clicar em compartilhar, em seguida na engrenagem e selecionar a opção conforme *print screen* abaixo.

← Configurações para compartilhar com pessoas

- Os editores podem alterar permissões e compartilhar
- Os leitores e comentaristas podem ver a opção de fazer o download, imprimir e copiar

Quanto ao uso de um link como forma de compartilhar um documento deve-se ter a preocupação em restringir quem pode ter acesso a ele. No processo de compartilhamento é possível restringir o acesso clicando no símbolo de link na janela de compartilhamento. Ao clicar você terá três opções de restrição: restrito - somente ao grupo compartilhado; CorreioWeb PBH - somente para quem estiver nesse domínio; Qualquer pessoa - aberto a qualquer pessoa que tenha o link. Essa última opção deve ser evitada quando se tratar de documentos internos.



Via de regra, como boa prática da governança das informações pessoais e sensíveis tratadas, recomenda-se ao proprietário de documentos que, ao compartilhá-los, utilize as opções de configuração descritas acima para maior segurança dos dados.

Se é um documento que você precisa, por exemplo, que outra pessoa da equipe colabore, selecione a permissão de editor. Caso o documento seja apenas para o conhecimento, é importante assegurar que está compartilhado somente com a opção de visualização.

O maior risco para os dados no google drive está relacionado às credenciais que são utilizadas. Por isso, é recomendado fazer a verificação em duas etapas, um processo de segurança que só permite o acesso à conta após duas comprovações de identidade, ou seja, utilizando uma senha e um token.

Desconectar do seu perfil na ferramenta é uma atitude simples para garantir que os dados não sejam acessados caso um smartphone ou notebook seja extraviado.

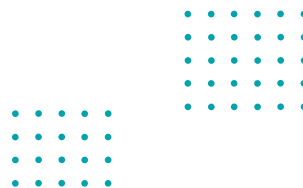
Além da verificação, é importante sempre fazer *logout* das contas (desconectar a conta, sair do sistema operacional). Esse simples ato garante a proteção dos dados em duas situações: no

extravio de algum dispositivo móvel que estiver conectado e no compartilhamento de computadores, o qual não permite definir quem poderá ou não acessar uma determinada conta.

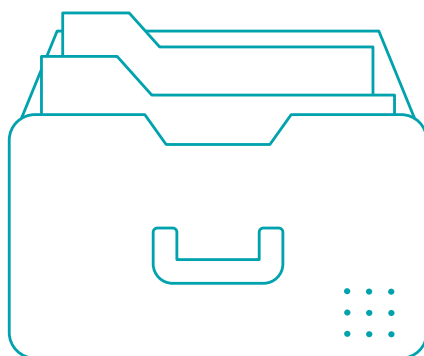
Por último, mesmo considerando todos esses cuidados, é importante ter sempre em mente quais são os arquivos que estão na nuvem. Caso sejam documentos confidenciais, assegure-se de que estará em uma pasta que não é compartilhada com ninguém que não possa ter acesso àqueles dados.

A ferramenta ainda permite que, sendo você o proprietário da pasta ou do arquivo, seja possível gerenciar as opções de compartilhamento para cada perfil. Caso uma pessoa troque de equipe ou mude de lotação ou atividade, é preciso retirar a permissão de acesso desta(s) pessoa(s).

Em suma, é preciso ter uma dedicação e cuidado com o que está sendo compartilhado e sempre rever o que, com quem, se realmente este compartilhamento é imprescindível, e se o documento está sendo compartilhado apenas com os atores essenciais e permitindo tão somente as ações que são necessárias.



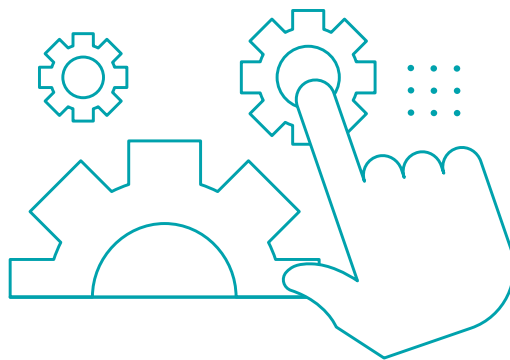
10. UTILIZAÇÃO DE REGISTRO / TRATAMENTO EM REPOSITÓRIOS NÃO ESTRUTURADOS



Sempre ao tratar/cadastrar uma informação pessoal, o agente público deverá, primeiramente, verificar se há um sistema informatizado adequado para o registro do dado, analisando todas as funcionalidades do sistema existente e só recorrendo a outros repositórios se o sistema não apresentar os requisitos necessários para o tratamento da informação.

Ao criar planilhas/registros, manter a uniformidade na forma do tratamento do dado, condensando as informações em uma mesma estrutura (evitar que uma matéria seja registrada em planilha eletrônica e a mesma seja, depois, tratada em dispositivo/formulário em papel ou outros formatos). Evitar, por exemplo, que o registro de dados para busca ativa de faltosos, de controle de entrega de agendamentos de consultas especializadas ou de registros de comunicados a usuários por telefone, seja documentado por alguns serviços em forma de planilhas e por outros em cadernos/ livros de protocolos ou fichas e pastas.

11. GESTÃO DO CONHECIMENTO / MUDANÇA



Considerando todos os tópicos listados como recomendações de boas práticas para a adequada gestão dos dados, é importante ressaltar a necessidade de uma boa gestão do conhecimento e da mudança dentro das equipes, para que seja possível transmitir essas informações a todos e viabilizar o cumprimento do que foi apresentado.

Lembrando que os fluxos de informações, processos, documentos e procedimentos de uma área precisam acontecer com quaisquer pessoas que estejam ocupando a estrutura orgânica institucional no momento; é necessário, portanto, garantir que nenhuma informação relevante seja do conhecimento de apenas uma pessoa.

Mas como controlar isso na prática?

- Criar um e-mail da Unidade (Caixa Postal da Unidade) para que todo documento utilizado na nuvem (Cloud) e localmente seja armazenado neste e-mail e compartilhado com a equipe (mesmo que seja compartilhado com demais e-mails). O ideal é que os documentos não estruturados do setor sejam, preferencialmente, criados na conta da Unidade e não no e-mail individual, para evitar perda de acesso aos mesmos quando da desativação e posterior exclusão do e-mail devido ao desligamento do profissional da instituição. Se o mesmo tiver compartilhado documentos em seu drive com outros usuários, com a desativação da conta

esses documentos perderão o compartilhamento e, logo, não serão mais visíveis aos demais usuários. Assim, é fundamental que antes do desligamento deste, seja feito backup dos documentos administrados e compartilhados por ele, da seguinte forma: transferir a propriedade do documento armazenado na nuvem (Cloud) clicando em compartilhar no e-mail do gestor da unidade, tornando-o proprietário.

- Um e-mail de unidade deve utilizar a delegação para outros e-mails sem necessitar revelar a senha para várias pessoas (Esse procedimento de delegação de contas de e-mail está detalhado no documento: <https://support.google.com/a/answer/7223765?hl=pt-BR>).
- No gerenciamento dos diretórios institucionais para armazenamento de arquivos considerar:
 1. Nome dos arquivos, diretórios e subdiretórios:
 - A. Sempre utilizar nomes curtos ou abreviados para evitar falhas ao movimentar as informações.
 2. Relevância dos arquivos armazenados:
 - A. Sempre questione se os arquivos armazenados realmente precisam ser arquivados.
 - B. Somente arquivar informações que pertençam à organização.
 - C. Observar se arquivos muito antigos realmente necessitam ser mantidos nos diretórios, considerando o contexto de cada setor.
- Sempre que houver mudança de pessoas na equipe, mudar as senhas que eram compartilhadas.
- Criar fluxos de trabalho nas áreas para garantir que todos sejam instruídos da mesma forma, inclusive os novos membros das equipes;
- Organizar e difundir a cultura dos procedimentos para tratamento de dados para todos os membros das equipes.

A conscientização sobre a proteção de dados é imprescindível, uma vez que não é suficiente ter um sistema adequado se os operadores não estiverem atentos e orientados aos riscos e cuidados necessários à proteção de dados. Nesse sentido, sugerimos a leitura da Portaria SMSA/SUS-BH Nº 0272/2021 (<https://dom-web.pbh.gov.br/visualizacao/edicao/3094>), que estabelece as hipóteses de tratamento de dados pessoais e sensíveis no âmbito desse órgão.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Cartilha LGPD PBH (pbh.gov.br).
2. Guia de Boas Práticas para implementação na Administração Pública Federal versão 2.0.
3. Arquivo Público da Cidade de Belo Horizonte – Gestão de Documentos na PBH / Arquivo Público da Cidade de Belo Horizonte. v.4, 2018.

Última atualização em: 27/1/2022.

