

1. INTRODUÇÃO

Esta Política estabelece as diretrizes para o gerenciamento do ciclo de vida de contas de *e-mail* institucionais e de repositórios de arquivos a elas relacionados após o desligamento de empregados ou de colaboradores da SPTrans.

2. OBJETIVOS

- 2.1. Racionalizar o uso de licenças e otimizar os custos associados;
- 2.2. Prezar, como regra, pela exclusão de contas institucionais após o desligamento de empregados e de colaboradores, e considerar a manutenção uma exceção para garantir a preservação de informações institucionais; e
- 2.3. Assegurar a conformidade do gerenciamento e da retenção de contas de *e-mail* institucionais e de repositórios de arquivos relacionados com obrigações legais e regulatórias.

3. BASE LEGAL E NORMATIVA

- 3.1. Constituição da República Federativa do Brasil de 1988;
- 3.2. Lei Federal nº 12.527, de 18/11/2011 – Lei de Acesso à Informação (LAI);
- 3.3. Lei Federal nº 12.965, de 23/04/2014 – Marco Civil da Internet (MCI);
- 3.4. Lei Federal nº 13.709, de 14/08/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- 3.5. Decreto Municipal nº 49.914, de 14/08/2008, que dispõe sobre a proibição de acesso a sites da Internet com conteúdos relacionados a sexo, drogas, pornografia, pedofilia, violência e armamento, no âmbito dos órgãos integrantes da Administração Municipal Direta e Indireta;
- 3.6. Decreto Municipal nº 59.767, de 15/09/2020, que regulamenta a aplicação da LGPD no âmbito da Administração Municipal Direta e Indireta;
- 3.7. Política de Segurança da Informação da SPTrans;
- 3.8. Código de Conduta e Integridade da SPTrans; e
- 3.9. Normas ABNT NBR ISO 31000:2018, sobre Gestão de Riscos, e NBR ISO 27001:2022, 27002:2022, 27003:2020 e 27005:2023, sobre Segurança da Informação.

4. AMPLITUDE

Aplica-se a todos os empregados, Diretores, membros dos Conselhos de Administração e Fiscal, membros do Comitê de Auditoria Estatutário, jovens aprendizes, estagiários e prestadores de serviço, assim como qualquer pessoa que utilize ou venha a ter acesso a contas institucionais.

5. DEFINIÇÕES

5.1. Log

É o registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação.

5.2. Backup

É o conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação.

5.3. Legal Hold

É o pedido de retenção de dados, por prazo determinado ou indeterminado, realizado pela Área Jurídica à Área de Tecnologia da Informação e Comunicação

6. DIRETRIZES E CRITÉRIOS

➤ Gerais

- 6.1. A interpretação desta Política observará os termos da Lei Geral de Proteção de Dados Pessoais – LGPD e dos demais atos normativos nacionais e municipais que tratem dos direitos à privacidade, à proteção de dados pessoais e à autodeterminação informativa.
- 6.2. A interpretação desta Política também deverá observar as Políticas e as Normas e Procedimentos da SPTrans referentes à segurança da informação.
- 6.3. Exceções aos termos desta Política deverão ser analisados caso a caso, com aplicação entre as partes interessadas, nos limites que a motivem.

- 6.4.** O acesso ou qualquer outra operação de tratamento, por empregados da SPTrans, a dados presentes em contas de *e-mail* institucionais vinculadas a ex-empregados e a ex-colaboradores, será restrito a empregados autorizados pelo Responsável da Área de Tecnologia da Informação e Comunicação, justificado apenas para a preservação de informações institucionais, para o cumprimento de obrigações legais e/ou para o cumprimento de ordens judiciais.
- 6.5.** O “*backup*” de contas institucionais, quando aplicável, deverá permanecer armazenado em repositório seguro gerenciado pela Área de Tecnologia da Informação e Comunicação e de acesso, também, restrito a empregados autorizados pelo Responsável da Área referida.
- 6.6.** Qualquer acesso, cópia ou visualização do conteúdo do “*backup*” deverá gerar “*logs*” que garantam integridade e rastreabilidade.

➤ **Controle de Acessos**

- 6.7.** O acesso do ex-empregado ou do ex-colaborador à conta de *e-mail* institucional a ele anteriormente vinculada deverá ser suspensa, imediatamente, após a cessação de seu vínculo com a SPTrans.
- 6.8.** A decisão motivada entre a eliminação e a retenção (“*backup*”), por prazo determinado ou indeterminado, de conta de *e-mail* institucional e do repositório de arquivos a ela relacionado, anteriormente vinculado a ex-empregado ou a ex-colaborador, será tomada, preliminarmente, pelo Responsável de Área, após notificação da Área de Tecnologia da Informação e Comunicação.
- 6.8.1.** Se a decisão tomada for a de eliminação ou a de retenção (“*backup*”) por prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com questionamento à Área Jurídica quanto a eventuais prejuízos que impossibilitem a eliminação, conforme segue:
- a.** Se a Área Jurídica entender pela impossibilidade da eliminação, mesmo após o decurso de prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com a retenção (“*backup*”) por prazo indeterminado, salvo disposição em contrário da Área Jurídica que possibilite retenção (“*backup*”) por prazo determinado e posterior eliminação;
 - b.** Se a Área Jurídica entender pela possibilidade da eliminação, inclusive após o decurso de prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com a sua realização.

6.9. Excetuam-se ao disposto no item 6.8. os casos em que o ex-empregado tenha cessado o seu vínculo na condição de Diretor ou de Responsável de Área da estrutura organizacional, hipóteses nas quais haverá, de imediato, a retenção (“*backup*”), pelo prazo de 6 (seis) meses, da conta de *e-mail* institucional e do repositório de arquivos a ela relacionado.

6.9.1. Antes do decurso do prazo disposto no item 6.9., a decisão motivada entre a eliminação e a retenção (“*backup*”), por prazo determinado ou indeterminado, de conta de *e-mail* institucional e do repositório de arquivos a ela relacionado, anteriormente vinculada a Diretor ou Responsável de Área da estrutura organizacional, será tomada, preliminarmente, pelo atual titular da Área, após notificação da Área de Tecnologia da Informação e Comunicação, conforme segue:

- Se a decisão tomada for a de eliminação ou a de retenção (“*backup*”) por prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com questionamento à Área Jurídica quanto a eventuais prejuízos que impossibilitem a eliminação, procedendo da seguinte forma:
 - a. Se a Área Jurídica entender pela impossibilidade da eliminação, mesmo após o decurso de prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com a retenção (“*backup*”) por prazo indeterminado, salvo disposição em contrário da Área Jurídica que possibilite retenção (“*backup*”) por prazo determinado e posterior eliminação;
 - b. Se a Área Jurídica entender pela possibilidade da eliminação, inclusive após o decurso de prazo determinado, a Área de Tecnologia da Informação e Comunicação procederá com a sua realização.

6.10. A omissão do Responsável de Área quanto às tomadas de decisões a que se referem os itens 6.8. e 6.9.1. resultará na retenção (“*backup*”) da conta de *e-mail* institucional e do repositório de arquivos a ela relacionada, anteriormente vinculada a ex-empregado ou a ex-colaborador, até que decisão a respeito seja tomada pelo superior hierárquico do referido Responsável de Área.

6.11. A retenção de conta de *e-mail* institucional e do repositório de arquivos a ela relacionada, anteriormente vinculada a ex-empregado ou a ex-colaborador, poderá ser requerida, por prazo indeterminado, a qualquer tempo e por qualquer motivo, pela Área Jurídica (“*legal hold*”).

7. COMPETÊNCIAS

7.1. Responsável pela Área de Recursos Humanos

Garantir a imediata comunicação à Área de Tecnologia da Informação e Comunicação a respeito do desligamento de empregado ou de colaborador que se utilize de conta de *e-mail* institucional e de repositório de arquivos a ela relacionada, identificando-lhe a partir de nome, cargo/função, prontuário, Área de lotação e Responsável de Área ao qual esteja subordinado.

7.2. Responsável de Área

Decidir, motivadamente, entre a eliminação e a retenção ("*backup*"), por prazo determinado ou indeterminado, de *e-mail* institucional e do repositório de arquivos a ele relacionado, anteriormente vinculado a ex-empregado ou a ex-colaborador, no prazo de 10 (dez) dias úteis após notificação da Área de Tecnologia da Informação e Comunicação.

7.3. Responsável pela Área de Tecnologia da Informação e Comunicação

7.3.1. Garantir o cumprimento da tomada de decisão dos Responsáveis de Área, nos termos dos itens 6.9. e 6.9.1.

7.3.2. Garantir a possibilidade da execução do procedimento ("*legal hold*") disposto no item 6.11.

7.4. Responsável pela Área Jurídica

Garantir a elaboração de pareceres relativos aos questionamentos realizados nos termos dos itens 6.8.1. e 6.9.1., alíneas "a" e "b", bem como a possibilidade da execução do procedimento ("*legal hold*") disposto no item 6.11.

7.5. Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO)

7.5.1. Acompanhar o cumprimento dos termos desta Política quanto à proteção de dados pessoais.

7.5.2. Elaborar pareceres referentes a casos específicos, quanto ao tratamento de dados pessoais, em casos de dúvidas quanto aos procedimentos necessários à harmonia entre a proteção de dados pessoais e o acesso a contas institucionais de ex-empregados e ex-colaboradores por agentes autorizados pelo Responsável pela Área de Tecnologia da Informação e Comunicação.

7.6. Comitê de Governança em Privacidade, em Proteção de Dados Pessoais e em Segurança da Informação

Acompanhar o cumprimento dos termos desta Política.

8. VIOLAÇÕES

A não observância dos dispositivos desta Política sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, trabalhistas, cíveis e penais previstas em legislação e em regulamentação vigentes, assegurados aos envolvidos o direito ao contraditório e à ampla defesa.

9. DISPOSIÇÕES FINAIS

9.1. Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação, o usuário deverá solicitar os esclarecimentos necessários para a Área de Tecnologia da Informação e Comunicação.

9.2. A presente Política deverá ser revista e atualizada em intervalo não superior a três anos ou sempre que se julgar necessário.

10. APROVAÇÕES

Esta Política foi aprovada pelo Comitê de Governança em Privacidade, em Proteção de Dados Pessoais e em Segurança da Informação (CPD) da SPTrans em 21 de janeiro de 2026.

HISTÓRICO DE REVISÕES		
REVISÃO	DATA	ALTERAÇÃO
0	05.02.2026	Emissão inicial.