Governo do Estado de São Paulo
Fundação Centro de Atendimento Socioeducativo ao Adolescente
ATI - Assessoria de Tecnologia da Informação

INSTRUÇÃO

Nº do Processo: 161.00063663/2025-11

Interessado: FUNDACAO CASA, ATI - Assessoria de Tecnologia da Informação

Assunto: Política de Serviços de Mensageria e Telefonia

Responsável	Assessoria de Tecnologia da Informação - ATI
Aprovado por:	Gabinete da Presidência.
Políticas Relacionadas	Política de Governança de TI, Política de Segurança da Informação, Política de Uso Aceitável de TI, Política de Backup e Recuperação de Dados
Localização de armazenamento	Processo SEI 161.00063663/2025-11
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

1. OBJETIVO

1.1. Esta política tem por finalidade estabelecer as diretrizes e os procedimentos para o uso adequado dos serviços de mensageria e telefonia disponibilizados pela organização, assegurando uma comunicação segura, eficiente e em conformidade com as exigências legais e as melhores práticas de TI.

1.2. Objetiva-se, ainda, definir as responsabilidades dos usuários, administradores e demais envolvidos, bem como orientar as ações preventivas e corretivas relacionadas a incidentes e abusos na utilização das ferramentas oficiais (Outlook, Teams, Rainbow e telefonia VoIP).

1.3. Por meio desta política, busca-se garantir a integridade, confidencialidade e disponibilidade das informações, promovendo um ambiente de comunicação que contribua para a continuidade operacional e o alinhamento estratégico da organização.

---

2. Abrangência

2.1. Esta política aplica-se a todos os colaboradores, terceirizados, prestadores de serviços e

demais usuários autorizados que utilizem as ferramentas de mensageria e telefonia fornecidas pela organização.

2.2. Compreende todas as modalidades de acesso e utilização dos serviços, incluindo, mas não se limitando, aos ambientes físico e virtual, bem como aos dispositivos corporativos e pessoais previamente autorizados.

2.3. Abrange todas as atividades relacionadas ao envio, recebimento e gerenciamento de mensagens, e à realização de chamadas telefônicas via VoIP, devendo ser observadas as diretrizes aqui estabelecidas por todos os envolvidos.

3. TERMOS E CONDIÇÕES

Conta de e-mail departamental – Conta institucional destinada à comunicação compartilhada entre os membros de um departamento ou setor.

Conta de e-mail pessoal – Conta individual fornecida ao colaborador para a comunicação oficial e o gerenciamento de correspondência.

Mensageria – Conjunto de serviços de comunicação eletrônica, que inclui e-mail, mensagens instantâneas e outros recursos de troca de informações.

Outlook – Cliente de e-mail corporativo utilizado para o gerenciamento de contas pessoais, calendário e tarefas.

Rainbow – Ferramenta de comunicação corporativa que oferece recursos de mensagens instantâneas, videoconferências e colaboração em tempo real.

Teams – Plataforma de colaboração e comunicação da Microsoft, utilizada para reuniões, chats e compartilhamento de arquivos.

Telefonia VOIP – Sistema de comunicação telefônica que utiliza a tecnologia de Voz sobre Protocolo de Internet para a realização de chamadas.

4. REFERÊNCIAS LEGAIS E BOAS PRÁTICAS

Referência	Descrição
COBIT	**Framework de governança de TI que orienta o alinhamento entre estratégias de negócio e investimentos em tecnologia, contribuindo para a mitigação de riscos.**
ITIL	**Conjunto de melhores práticas para gerenciamento e entrega de serviços de TI, promovendo a eficiência operacional e a melhoria contínua dos processos.**
LGPD (Lei Geral de Proteção de Dados)	**Regula o tratamento de dados pessoais, garantindo a proteção, a privacidade e os direitos dos titulares no ambiente digital.**

NIST	**Conjunto de diretrizes e práticas para segurança cibernética, controle de acesso e proteção contra ameaças, que serve de referência para a implementação de medidas de segurança.**
ISO/IEC 27001	**Norma internacional que especifica os requisitos para a implementação e manutenção de um Sistema de Gestão de Segurança da Informação (SGSI), assegurando a confidencialidade, integridade e disponibilidade dos dados.**

5. PRINCÍPIOS GERAIS

5.1. **Legalidade e Conformidade**

Assegurar que o uso dos serviços esteja em conformidade com a legislação vigente, normas internas e melhores práticas.

5.2. **Segurança e Proteção das Informações**

Garantir a proteção das comunicações e dados por meio de medidas preventivas e corretivas.

5.3. **Transparência e Rastreabilidade**

Assegurar a rastreabilidade das comunicações com definição clara de responsabilidades para facilitar auditorias.

5.4. **Uso Responsável e Ético**

Promover o uso dos serviços exclusivamente para fins profissionais, com condutas éticas que preservem a segurança e a reputação da organização.

5.5. **Continuidade e Eficiência Operacional**

Garantir a disponibilidade contínua dos serviços e a eficiência no uso dos recursos tecnológicos.

5.6. **Privacidade e Proteção de Dados**

Assegurar o respeito à privacidade dos usuários e a proteção adequada dos dados pessoais e sensíveis.

CAPÍTULO I – DISPOSIÇÕES GERAIS

Seção I – Finalidade e Escopo da Política

Art. 1º Esta política tem por finalidade estabelecer as diretrizes, normas e procedimentos para a utilização dos serviços de mensageria e telefonia disponibilizados pela Fundação CASA-SP, visando assegurar a comunicação segura, eficiente e em conformidade com as disposições legais e regulamentares aplicáveis.

§ 1º Para os fins desta política, consideram-se como ferramentas oficiais os sistemas de mensageria (Outlook, Teams e Rainbow) e o serviço de telefonia via VoIP.

§ 2º O escopo desta política abrange todas as atividades relacionadas ao envio, recebimento, armazenamento e gerenciamento de informações transmitidas por meio dos serviços

mencionados.

Seção II – Aplicabilidade e Responsabilidades

Art. 2º Esta política é aplicável a todos os colaboradores, terceirizados, prestadores de serviços e demais usuários autorizados a utilizar os serviços de mensageria e telefonia da organização.

I - Dos Usuários:

a) Utilizar os serviços de acordo com as diretrizes estabelecidas nesta política;

b) Zelar pela confidencialidade, integridade e disponibilidade das informações;

c) Reportar, de forma imediata, quaisquer incidentes, irregularidades ou suspeitas de uso indevido para a Seção de Segurança da Informação.

II - Dos Gestores dos usuários:

a) Supervisionar a aplicação desta política nas respectivas áreas de atuação;

b) Adotar medidas corretivas e preventivas em caso de descumprimento das disposições aqui estabelecidas.

III – Da Gerência de Infraestrutura e Segurança da Informação:

a) Implementar e manter os controles de segurança e os mecanismos de monitoramento dos serviços;

b) Promover treinamentos e orientações acerca do uso adequado das ferramentas oficiais;

c) Realizar auditorias periódicas para verificar o cumprimento desta política.

Parágrafo Único: O descumprimento das disposições desta política implicará na aplicação de penalidades administrativas, civis e penais, em conformidade com a legislação vigente e as normas internas da organização.

CAPÍTULO II – DIRETRIZES PARA USO DOS SERVIÇOS DE MENSAGERIA

Seção I – Uso do Outlook

Art. 3º – Das Regras Gerais de Uso

I. O Outlook deverá ser utilizado exclusivamente para atividades profissionais, limitando-se à comunicação e ao gerenciamento de informações essenciais para o desempenho das funções;

II. O acesso à conta de e-mail pessoal é intransferível, sendo vedado o compartilhamento de credenciais;

III. As contas de e-mail departamentais, destinadas ao uso coletivo dos membros do respectivo setor, poderão ser compartilhadas entre os usuários autorizados, sendo o acesso gerenciado e monitorado pelo gestor responsável, que manterá registros dos usuários autorizados e das atividades realizadas.

IV. É imperativo que o uso do Outlook observe os princípios da ética, da integridade e da responsabilidade, preservando a confidencialidade das informações corporativas.

Art. 4º – Do Envio e Recebimento de E-mails

I. O envio e o recebimento de e-mails devem ser realizados com clareza, objetividade e precisão.

II. Para o envio de mensagens, devem ser observados os seguintes critérios:

a) O conteúdo deve ser estritamente relacionado ao contexto profissional, apresentando informações relevantes e necessárias para a execução das atividades;

b) É proibido o envio de mensagens contendo termos ou expressões ofensivas, discriminatórias ou que possam comprometer a reputação da organização;

c) É obrigatória a utilização da assinatura padrão disponibilizada pela Fundação CASA-SP, devidamente preenchida e configurada no cliente de e-mail, a fim de assegurar a padronização e a identificação correta dos remetentes;

d) O envio de e-mails deverá observar o uso adequado do idioma português, com correção gramatical e formalidade compatível à comunicação corporativa.

III. A seleção dos destinatários deverá ser feita com critério, garantindo que as informações sejam encaminhadas somente aos indivíduos diretamente envolvidos nas atividades ou expressamente autorizados a receber tais dados.

IV. O usuário deve configurar a resposta automática em caso de férias, licença ou abonada, indicando o e-mail ao qual as mensagens devem ser encaminhadas nesse período.

Art. 5º – Da Segurança e Proteção contra Ameaças

I. O Outlook deverá ser configurado pela contratada com mecanismos de segurança, dentre os quais filtros de spam e outras soluções de proteção.

II. São medidas obrigatórias para a segurança do serviço:

a) A utilização de senhas robustas, que deverão ser alteradas periodicamente;

b) implementação de autenticação multifator para reforçar o controle de acesso.

III. As atividades realizadas por meio do Outlook poderão ser monitoradas com o intuito de identificar comportamentos suspeitos ou tentativas de acesso não autorizado, devendo quaisquer incidentes ser imediatamente comunicados à Seção de Segurança da Informação.

IV. Em caso de bloqueio ou esquecimento de senha, deverá ser aberto chamado no Tarefas para atendimento.

Art. 6º – Da Política de Retenção e Arquivamento

I. As mensagens eletrônicas enviadas e recebidas pelo Outlook são armazenadas na nuvem até a capacidade estabelecida para a conta.

II. Em caso de desligamento, descomissionamento ou transferência do servidor, o gestor da área poderá ter acesso ao conteúdo armazenado, conforme necessidade de conhecimento do registro das atividades de trabalho.

III. É responsabilidade do usuário monitorar o espaço de armazenamento disponível em sua conta de e-mail, adotando medidas preventivas para evitar que a capacidade atinja 100%.

IV. A regras de backup estão definidas na Política de Backup e Recuperação de Dados.

Seção II – Uso do Teams e Rainbow

Art. 7º – Das Regras Gerais de Uso

I. As ferramentas Teams e Rainbow deverão ser utilizadas única e exclusivamente para finalidades profissionais

II. O acesso às referidas plataformas é restrito aos usuários devidamente autorizados, sendo vedado o compartilhamento de credenciais ou qualquer informação de acesso.

III. Os usuários deverão empregar as funcionalidades das plataformas com ética e responsabilidade, zelando pela integridade e segurança das informações corporativas.

Art. 8º – Do Uso de Grupos e Bolhas

I. A criação e a gestão de grupos ou bolhas de comunicação nas plataformas Teams e Rainbow deverão ser efetuadas conforme as necessidades operacionais e com a autorização do gestor responsável.

II. Os grupos deverão ser configurados com níveis de acesso compatíveis com a sensibilidade das informações compartilhadas, garantindo que somente membros autorizados tenham acesso ao conteúdo.

III. Compete à administração dos grupos a moderação do conteúdo e a realização de revisões periódicas, assegurando a conformidade com as políticas internas e a segurança dos dados.

Art. 9º – Da Comunicação Corporativa e Videoconferências

I. As videoconferências e demais formas de comunicação corporativa realizadas por meio das plataformas Teams e Rainbow deverão obedecer aos padrões de clareza, objetividade e segurança estabelecidos pela organização.

II. É obrigatória a identificação dos participantes, que deverão utilizar suas credenciais institucionais para assegurar a responsabilidade e a rastreabilidade das interações.

Art. 10 – Da Disponibilidade e Substituição do Rainbow

I. Havendo disponibilidade da tecnologia no ramal, o servidor deverá efetuar o primeiro acesso para definição da senha, possibilitando o uso da ferramenta.

II. É obrigatório que o servidor permaneça logado no Rainbow e disponível para atendimento de chamadas durante o expediente enquanto em teletrabalho.

III. Não havendo disponibilidade do Rainbow ou mediante avaliação da conveniência dos trabalhos executados, o gestor poderá optar por outras ferramentas tecnológicas, devendo seguir as mesmas diretrizes dessa política.

CAPÍTULO III – DIRETRIZES PARA USO DA TELEFONIA VOIP

Art. 11 – Das Regras Gerais de Uso

I. A utilização do sistema de telefonia VoIP destina-se exclusivamente à realização de comunicações corporativas, estando vedado o uso para fins pessoais ou que não estejam alinhados com as atividades institucionais.

II. O número de telefone corporativo deve ser fornecido externamente apenas para fins das atividades profissionais.

Art. 12 – Da Segurança e Registro de Chamadas

I. Todos os registros de chamadas efetuadas por meio do sistema VoIP deverão ser armazenados de forma segura.

II. As informações coletadas por meio do registro das chamadas serão utilizadas única e exclusivamente para fins de controle, segurança e melhoria contínua dos serviços, respeitando os direitos à privacidade e a legislação aplicável.

Capítulo IV – Da Distribuição de Licenças

Art. 13 – Dos Tipos de Licenças

I. Básico completo: licença do Outlook com e-mail de 100 Gb de armazenamento, OneDrive 5Tb, Office 365 Online e instalado, Planner, Teams e Power BI Pro.

II. E1: licença do Outlook com e-mail de 50 Gb de armazenamento, OneDrive 1Tb, Office online, Planner e Teams.

III. Exchange: licença do Outlook com e-mail de 50Gb de armazenamento.

IV. Rainbow: telefonia VOIP, serviço web e aplicativo.

Art. 14 – Da Distribuição das Licenças

I. Básico completo: Presidente, Chefe de Gabinete, Diretores e Diretores Adjuntos (DGAR e DGA), Superintendentes, Gerentes (Administrativos e Técnicos), Assessores, Ouvidor, Corregedor, Assessor Jurídico, Assessor de Imprensa, Chefes de Seção das Divisões Regionais (Seção Técnica e Administrativa), Núcleo de Inteligência Organizacional – NIO e Núcleo de Apoio Tecnológico – NAT.

II. E1: Gestores, e 3 contas de e-mail departamentais principais de cada centro de atendimento.

III. Exchange: contas departamentais e demais servidores.

IV. Rainbow: disponibilidade contratual exclusivamente no prédio da sede, sendo disponibilizado para todos os servidores.

§ 1º – A distribuição poderá ser limitada conforme disponibilidade de licenças.

§ 2º – As contas de e-mail departamentais terão como padrão “@fundacaocasa.sp.gov.br” e as contas de e-mail pessoais “@sp.gov.br”.

§ 3º – Casos excepcionais deverão passar por análise e aprovação do Gabinete da Presidência e poderão ser revisados periodicamente.

CAPÍTULO V – DAS DISPOSIÇÕES FINAIS

Art. 15 – O compartilhamento de arquivos deverá obedecer aos protocolos da **Política de Segurança da Informação** e da **Política de Dados Pessoais e Privacidade**.

Art. 16 – Esta política será revisada periodicamente, conforme a necessidade e evolução das melhores práticas de governança de TI, segurança da informação e mudanças na legislação aplicável.

Art. 17 – Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

São Paulo, na data da assinatura digital.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 13/03/2025, às 16:31, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Raelen Bego Luiz**, **Chefe de Gabinete**, em 18/03/2025, às 22:30, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0059159599** e o código CRC **56300E34**.