Política de Segurança da Informação

PL-SI-001 | Versão 1.6 | Revisão da versão 1.5 — retenção de chamados técnicos

Situação: VERSÃO 1.6 RATIFICADA EM TERMO DE APROVAÇÃO CONJUNTA ASSINADO EM 03/07/2026.
Classificação: PÚBLICA — GRUPO CPA.

1. OBJETIVO

Estabelecer diretrizes para proteger informações, sistemas corporativos, credenciais de acesso e ambientes tecnológicos utilizados pelo Grupo CPA, preservando confidencialidade, integridade e disponibilidade, reduzindo riscos e orientando colaboradores quanto às suas responsabilidades.

2. ABRANGÊNCIA

Aplica-se a colaboradores e profissionais autorizados que utilizam computadores, estações de trabalho, e-mail corporativo, sistemas de atendimento, ferramentas de gestão, cofres de credenciais, VPN, informações técnicas e comerciais, documentos e ambientes tecnológicos dos clientes.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- Confidencialidade: acesso somente por pessoas autorizadas
- Integridade: proteção contra alterações indevidas
- Disponibilidade: acesso aos recursos pelos profissionais autorizados conforme a necessidade
- Necessidade de acesso: permissões limitadas às atividades atribuídas
- Responsabilidade: uso adequado dos recursos e comunicação de situações suspeitas

4. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

Para orientação interna, propõe-se classificar as informações como:

- Públicas: conteúdos institucionais autorizados para divulgação
- Internas: procedimentos e comunicações de uso da empresa
- Confidenciais: contratos, dados pessoais, registros de clientes e informações comerciais
- De acesso restrito: senhas, credenciais administrativas, chaves e configurações críticas

O compartilhamento deverá observar a finalidade e a autorização correspondente.

5. GERENCIAMENTO DE USUÁRIOS E SENHAS

O Grupo CPA utiliza o software KeePass para armazenamento criptografado de credenciais fornecidas pelos clientes, inclusive para manutenção de servidores, redes e equipamentos de impressão. Diretrizes de utilização:

- Armazenar credenciais dos clientes no cofre digital autorizado
- Utilizar credenciais somente em atividades técnicas legítimas

- Não divulgar senhas a pessoas não autorizadas
- Evitar registros de credenciais em meios não aprovados
- Comunicar suspeitas de exposição ou comprometimento
- Solicitar revisão de permissões em mudanças de responsabilidade

6. CONTROLE DE ACESSO POR CLIENTE

As permissões são concedidas conforme a carteira de clientes e as responsabilidades de cada técnico. Cada profissional acessa somente as credenciais dos clientes que está autorizado a atender. Quando deixa de atender determinado cliente, suas permissões correspondentes são revogadas.

7. ACESSO REMOTO E VPN

Os recursos internos utilizados para consulta às credenciais dos clientes não são publicados diretamente na internet. O acesso remoto a esses recursos ocorre mediante VPN autorizada. As permissões são concedidas conforme a necessidade operacional e revogadas quando deixam de ser necessárias.

8. DESLIGAMENTO DE COLABORADORES

No desligamento, o Grupo CPA revoga os acessos corporativos disponibilizados ao colaborador, incluindo:

- E-mail corporativo
- Login e autenticação no ambiente Windows
- Acesso ao KeePass
- Acesso à VPN
- Demais sistemas e recursos internos

O procedimento deve ser coordenado entre a gestão e os responsáveis pela administração dos sistemas.

9. ALTERAÇÃO DE RESPONSABILIDADES

Quando um colaborador permanece na empresa, mas deixa de atender determinado cliente, as permissões relacionadas àquele cliente são retiradas. A gestão deverá comunicar as mudanças aos responsáveis pelo controle de acessos.

10. UTILIZAÇÃO DOS EQUIPAMENTOS E SISTEMAS CORPORATIVOS

Os recursos corporativos deverão ser utilizados prioritariamente em atividades profissionais autorizadas. Os colaboradores deverão:

- Preservar credenciais individuais e evitar compartilhamento de contas
- Bloquear estações de trabalho quando ausentes
- Não instalar softwares não autorizados
- Evitar armazenamento desnecessário de informações dos clientes
- Comunicar falhas e comportamentos suspeitos
- Respeitar as normas de segurança dos ambientes dos clientes

11. SEGURANÇA DURANTE O ATENDIMENTO TÉCNICO

Os técnicos devem respeitar as normas e autorizações dos clientes. O acesso a servidores, equipamentos, sistemas de gerenciamento e redes deve limitar-se ao necessário para o serviço. É proibido utilizar credenciais para finalidades particulares. Documentos, arquivos, filas de impressão e dados visualizados durante a manutenção são confidenciais.

12. DOCUMENTOS, ARQUIVOS E DISPOSITIVOS DE ARMAZENAMENTO

Equipamentos de impressão e digitalização podem conter arquivos, registros e filas de impressão. Deve-se evitar acesso, cópia, transferência ou retenção de informações desnecessárias. Intervenções em unidades de armazenamento, bem como retirada, substituição, reutilização ou descarte de componentes que possam conter dados, deverão observar as instruções do cliente e os procedimentos de segurança aplicáveis.

13. PROTEÇÃO DE DADOS PESSOAIS

Os dados pessoais deverão ser utilizados somente para finalidades profissionais legítimas. Nos registros rotineiros de atendimento, serão coletadas apenas informações necessárias. O tratamento deverá observar a Política de Privacidade do Grupo CPA, a LGPD e as condições contratuais aplicáveis.

14. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Qualquer suspeita de incidente deverá ser comunicada à gerência ou ao responsável designado. Exemplos:

- Divulgação ou comprometimento de senhas
- Acesso não autorizado a sistemas
- Perda de equipamentos contendo informações
- Envio indevido de documentos ou dados
- Comprometimento de contas corporativas
- Exposição de informações de clientes
- Utilização indevida de credenciais

A ocorrência deverá ser avaliada para contenção, correção, recuperação e eventuais comunicações. Recomenda-se manter registro das ocorrências e providências adotadas.

15. RELACIONAMENTO COM CLIENTES E FORNECEDORES

Os colaboradores deverão respeitar requisitos contratuais e normas de segurança dos clientes. Informações técnicas, comerciais, credenciais e documentos não deverão ser compartilhados sem autorização ou justificativa legítima. O envolvimento de fabricantes e parceiros deve limitar-se às informações necessárias ao atendimento.

16. ORIENTAÇÃO E CONSCIENTIZAÇÃO DOS COLABORADORES

O Grupo CPA deverá promover orientações sobre confidencialidade, senhas, KeePass, controle de acesso por cliente, VPN, proteção de dados, cuidados na manutenção e comunicação de incidentes. A ciência desta política poderá ser registrada por termo, treinamento ou mecanismo definido pela empresa.

17. RESPONSABILIDADES

- Direção: aprovar a política, apoiar sua implementação e avaliar recursos
- Gerência: acompanhar diretrizes, organizar responsabilidades e receber comunicações
- Responsáveis pelos sistemas: administrar permissões e executar revogações
- Colaboradores: cumprir orientações, proteger credenciais e comunicar incidentes

18. DESCUMPRIMENTO DA POLÍTICA

O descumprimento poderá resultar em medidas administrativas compatíveis com a gravidade da ocorrência, observadas normas internas, contratos e legislação aplicável. Situações envolvendo clientes também serão avaliadas sob as obrigações contratuais e de confidencialidade.

19. REVISÃO E ATUALIZAÇÃO

Esta política deverá ser revisada periodicamente ou diante de mudanças relevantes em processos, sistemas, riscos ou exigências legais e contratuais. As atualizações deverão ser aprovadas pela direção e comunicadas aos profissionais abrangidos.

20. REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS (ROPA)

O Grupo CPA manterá inventário das operações de tratamento de dados pessoais, com identificação de atividades, finalidades, categorias de dados e titulares, sistemas, compartilhamentos, retenção, controles e responsáveis, conforme aplicável.

A aprovação formal do ROPA caberá conjuntamente à Diretoria e à Gerência Técnica. A Gerência Técnica coordenará sua manutenção com apoio dos setores responsáveis pelas atividades registradas.

O inventário será revisado ao menos anualmente e sempre que ocorrerem mudanças relevantes em processos, sistemas, contratos, finalidades, categorias de dados, destinatários ou controles de segurança.

O histórico de revisões será mantido em aba específica da planilha ROPA, registrando versão, data, alteração, responsável e aprovação. A manutenção do inventário não substitui a avaliação de bases legais, contratos e obrigações aplicáveis.

Os procedimentos de retenção de chamados no Qualitor observarão o item 21 desta política. O tratamento de dados de colaboradores e a exclusão de arquivos digitalizados terão procedimentos específicos, sujeitos a validação técnica, contratual e jurídica, conforme aplicável.

As solicitações de privacidade poderão ser encaminhadas a privacidade@cpagrupo.com, com triagem inicial pela Gerência Técnica e participação do gestor responsável designado.

21. RETENÇÃO E DESCARTE DE DADOS PESSOAIS

21.1. Critério geral

O Grupo CPA conservará dados pessoais pelo período necessário ao cumprimento das finalidades do tratamento e das obrigações legais e contratuais aplicáveis. A conservação deverá observar os princípios da necessidade, finalidade e segurança previstos na LGPD.

21.2. Chamados técnicos no Qualitor

Os registros de atendimento técnico e históricos de manutenção mantidos no Qualitor terão prazo-padrão de retenção de 5 (cinco) anos, contados do encerramento de cada chamado. A manutenção desse prazo deverá ser validada quanto à necessidade, proporcionalidade e fundamentos legais e contratuais.

21.3. Exceções ao prazo-padrão

A conservação por prazo superior poderá ocorrer quando houver obrigação legal ou contratual específica, exercício regular de direitos ou outra hipótese legal aplicável, mediante justificativa documentada. Dados desnecessários à finalidade do chamado não deverão ser mantidos apenas em razão do prazo-padrão.

21.4. Outras categorias de informações

Dados de colaboradores, registros comerciais, credenciais de clientes, solicitações de privacidade e documentos digitalizados observarão critérios próprios registrados no ROPA e em procedimentos específicos. Arquivos temporários de digitalização deverão ser eliminados após confirmação de entrega e conferência, ressalvadas instruções contratuais ou obrigações legais.

21.5. Eliminação e evidências

Após o término do prazo aplicável, os registros elegíveis serão avaliados para eliminação segura ou anonimização, ressalvadas as hipóteses legais de conservação. A Gerência de TI deverá verificar a viabilidade técnica no Qualitor, definir método, periodicidade operacional e registro das eliminações, com apoio da Gerência Técnica.

21.6. Revisão e responsabilidades

A Gerência de TI coordenará os controles técnicos de armazenamento e descarte, com apoio das áreas responsáveis pelos dados. Os critérios de retenção serão revistos anualmente ou diante de alterações relevantes na legislação, nos contratos e nos processos. O ROPA deverá refletir os prazos aprovados e suas exceções.

CONTROLE DE APROVAÇÃO

Campo	Registro
Versão	1.6 — aprovada
Aprovação — Diretoria	Ratificação da versão 1.6 conforme Termo de Aprovação Conjunta assinado em 03/07/2026.
Aprovação — Gerência Técnica	Ciência e apoio à implementação conforme Termo de Aprovação Conjunta assinado em 03/07/2026.
Vigência	03/07/2026 — conforme Termo de Aprovação Conjunta assinado
Próxima revisão	Anualmente, ou antes por mudança relevante