DAVID CANASSA STRATEGY & ADVISORY

POLÍTICA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

Diretrizes de Proteção de Dados, Governança e Conformidade Normativa

05 de agosto de 2026

---

1. IDENTIFICAÇÃO DO DOCUMENTO

Este documento constitui o corpo normativo oficial da **David Canassa Strategy & Advisory** no que tange à segurança da informação e à privacidade de dados. A presente política reflete o compromisso da consultoria com a excelência na governança de ativos informacionais e o estrito cumprimento das legislações vigentes.

Título: Política de Segurança e Privacidade da Informação
Empresa: David Canassa Strategy & Advisory
Versão: 1.0
Data: 05 de agosto de 2026
Aprovado por: Sócios
Classificação: Confidencial

2. OBJETIVO

A presente Política tem por objetivo estabelecer as diretrizes, princípios e controles fundamentais para assegurar a proteção da confidencialidade, integridade e disponibilidade das informações geridas pela **David Canassa Strategy & Advisory**. Busca-se garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (**LGPD**), o Regulamento Geral de Proteção de Dados da União Europeia (**GDPR**) e demais normas de segurança cibernética, adequando tais exigências ao perfil de consultoria estratégica boutique e à sua atuação em ambientes de alta complexidade e relevância internacional.

3. ABRANGÊNCIA

Esta Política aplica-se integralmente às seguintes pessoas e entidades:

3.1 Sócios
Todos os sócios da **David Canassa Strategy & Advisory**, em sua capacidade de administradores, gestores e operadores da consultoria.

3.2 Funcionários Próprios e Terceirizados
Eventuais funcionários contratados diretamente pela empresa, bem como profissionais terceirizados, estagiários, consultores associados e prestadores de serviço que tenham acesso, ainda que temporário, às informações da empresa ou de seus clientes.

3.3 Parceiros de Negócios
Pessoas físicas e jurídicas que mantenham relação comercial, técnica ou estratégica com a **David Canassa Strategy & Advisory**, incluindo consultores independentes, firmas parceiras, fornecedores de tecnologia e prestadores de serviços profissionais que, em virtude de sua relação com a empresa, tenham acesso a informações corporativas ou de clientes.

3.4 Ativos Tecnológicos

A abrangência estende-se a todos os dispositivos, sistemas, aplicativos e ambientes de computação utilizados pela empresa, incluindo a infraestrutura **Microsoft 365** (**OneDrive**, **SharePoint**, **Teams**), computadores pessoais e corporativos, dispositivos móveis e redes de comunicação utilizadas para o exercício das atividades profissionais.

4. BASE LEGAL E NORMATIVA

A fundamentação desta Política baseia-se nos seguintes diplomas legais e normativos:

- **LGPD (Lei nº 13.709/2018)**
- **GDPR (Regulamento UE 2016/679)**
- **Marco Civil da Internet (Lei nº 12.965/2014)**
- **ISO/IEC 27001:2022 e 27002:2022**
- **Resoluções da ANPD**

5. PRINCÍPIOS DA SEGURANÇA E PROTEÇÃO DE DADOS

5.1 Princípios de Segurança da Informação

A gestão da informação na consultoria é regida pelos seguintes pilares:

- **Confidencialidade:** Garantia de que a informação seja acessível apenas por pessoas explicitamente autorizadas.
- **Integridade:** Salvaguarda da exatidão e completude da informação e dos métodos de processamento.
- **Disponibilidade:** Garantia de que os usuários autorizados tenham acesso à informação sempre que necessário.
- **Necessidade de Conhecer (Need-to-know):** O acesso à informação deve ser restrito ao mínimo necessário para a execução de uma tarefa específica.
- **Menor Privilégio:** Concessão apenas das permissões de acesso essenciais para as funções desempenhadas.
- **Responsabilização (Accountability):** Capacidade de identificar e responsabilizar agentes por suas ações nos sistemas.

5.2 Princípios de Proteção de Dados Pessoais

Em conformidade com o **Art. 6º da LGPD** e preceitos do **GDPR**, o tratamento de dados pessoais observará:

- **Finalidade e Adequação:** Realização do tratamento para propósitos legítimos, específicos e informados ao titular.
- **Necessidade:** Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.
- **Livre Acesso e Qualidade:** Garantia de consulta facilitada e exatidão dos dados aos titulares.
- **Transparência:** Informações claras e precisas sobre a realização do tratamento.
- **Segurança e Prevenção:** Utilização de medidas técnicas para proteger os dados e prevenir danos.
- **Não Discriminação:** Impossibilidade de tratamento para fins discriminatórios ilícitos ou abusivos.
- **Responsabilização:** Demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são classificadas em quatro níveis, determinando seu manuseio e proteção conforme a tabela abaixo:

Nível	Definição	Exemplos	Acesso	Armazenamento	Transmissão	Descarte
Pública	Informações destinadas ao conhecimento externo.	Materiais institucionais.	Livre.	Áreas públicas do site ou redes sociais.	Sem criptografia obrigatória.	Descarte comum.
Interna	Dados operacionais da consultoria.	Fluxos de trabalho.	Restrito aos sócios.	**SharePoint** corporativo.	E-mail corporativo.	Lixeira eletrônica.
Confidencial	Informações que podem causar danos se divulgadas.	Propostas e contratos.	Restrito aos envolvidos no projeto.	Pastas específicas com permissão limitada.	Links protegidos.	Exclusão permanente.
Restrita	Dados de altíssima sensibilidade.	Estratégias C-level, dados financeiros, dados pessoais sensíveis.	Exclusivo aos sócios.	Diretórios com criptografia adicional.	Obrigatoriamente criptografada.	Destruição segura de dados.

7. PAPEIS E RESPONSABILIDADES

7.1 Sócios (Conjuntamente)

Compete aos sócios a aprovação final desta Política, a garantia de recursos para sua implementação e a revisão anual das diretrizes de segurança, além da tomada de decisão em incidentes críticos.

7.2 Encarregado de Proteção de Dados (DPO)

O sócio designado atuará como interface com a **ANPD** e titulares, orientando a consultoria sobre as melhores práticas e mantendo o registro das operações de tratamento de dados.

7.3 Terceiros e Prestadores de Serviço

Devem obrigatoriamente assinar Termos de Confidencialidade (**NDA**), cumprir esta Política e reportar qualquer suspeita de incidente imediatamente.

8. CONTROLES DE ACESSO

8.1 Gestão de Identidade

É obrigatório o uso de contas individuais no **Microsoft 365**. A Autenticação Multifator (**MFA**) deve estar ativa em todos os acessos. As senhas devem possuir no mínimo **12 caracteres**, incluindo complexidade alfanumérica e símbolos, sendo vedada a reutilização de credenciais.

8.2 Controle Lógico e Acesso Remoto

O acesso a dados de clientes é restrito ao sócio responsável pelo projeto. O bloqueio de tela automático é configurado para **5 minutos**. Conexões em redes Wi-Fi públicas são terminantemente proibidas sem o uso de **VPN segura**.

9. SEGURANÇA DE DISPOSITIVOS

Todos os computadores e notebooks devem operar com sistemas atualizados, antivírus ativo e criptografia de disco (**BitLocker**) habilitada. Dispositivos móveis devem possuir bloqueio biométrico ou **PIN forte**, além de capacidade de apagamento remoto de dados em caso de extravio.

10. USO DO MICROSOFT 365

10.1 OneDrive e SharePoint

O armazenamento deve ser centralizado nestas plataformas. É proibido o compartilhamento de links públicos; deve-se utilizar links para destinatários específicos com prazo de expiração máximo de **30 dias**.

10.2 Teams e Outlook

O **Teams** deve ser utilizado para comunicações profissionais, evitando-se dados restritos em canais abertos. O **Outlook** deve utilizar criptografia de mensagem para o envio de documentos confidenciais. O uso de e-mail pessoal para fins corporativos é proibido.

11. PROTEÇÃO DE DADOS PESSOAIS (LGPD E GDPR)

11.1 Bases Legais e Direitos

Todo tratamento de dados deve estar vinculado a uma base legal (Execução de Contrato, Legítimo Interesse ou Consentimento). A consultoria garante aos titulares o exercício de seus direitos (acesso, correção, exclusão) em até **15 dias úteis** para demandas de **LGPD**.

11.2 Transferência Internacional

Dada a atuação global, transferências internacionais de dados observarão o **Art. 33 da LGPD** e o **Capítulo V do GDPR**, utilizando Cláusulas Contratuais Padrão (**SCC**) para garantir que o nível de proteção não seja comprometido.

12. GESTÃO DE TERCEIROS

A contratação de fornecedores de tecnologia ou consultores associados depende de prévia avaliação de suas práticas de segurança e da inclusão de cláusulas específicas de proteção de dados em contrato.

13. RESPOSTA A INCIDENTES DE SEGURANÇA

Em caso de incidente (vazamento, perda de dispositivo ou acesso não autorizado), o procedimento padrão inclui: contenção imediata, avaliação de impacto e, se houver risco aos titulares, notificação à **ANPD** em até **3 dias úteis**, conforme legislação vigente.

14. CONTINUIDADE, MONITORAMENTO E AUDITORIA

14.1 Continuidade do Negócio

A resiliência operacional é garantida pelo backup automático em nuvem **Microsoft**. Testes de recuperação de dados e integridade de arquivos serão realizados anualmente pelos sócios.

14.2 Monitoramento e Auditoria

Os sócios realizarão revisões trimestrais nas configurações de segurança do **Microsoft 365** e auditorias anuais de conformidade para assegurar a eficácia dos controles estabelecidos.

15. DISPOSIÇÕES FINAIS

15.1 Contato do Encarregado (DPO)

E-mail: adm@davidcanassa.com

15.2 Termo de Confidencialidade (Pontos Essenciais)

Todo **NDA** com terceiros deve conter: (i) Definição de Informação Confidencial; (ii) Prazo de sigilo (mínimo **5 anos** pós-contrato); (iii) Obrigatoriedade de devolução/exclusão de dados; (iv) Proibição de subcontratação sem anuência.

15.3 O descumprimento destas normas sujeita o infrator às sanções legais e contratuais cabíveis. Esta política entra em vigor imediatamente após sua aprovação.

15.4 Esta Política será revisada anualmente pelos sócios ou sempre que houver alterações significativas na operação da empresa ou no cenário regulatório. Alterações serão comunicadas a todos os envolvidos e o histórico de versões incluído abaixo:

15.5 Histórico de Versões

Versão	Data	Descrição	Autor
1.0	05/08/2026	Emissão inicial da Política de Segurança	Sócios

---

DAVID CANASSA:10595221874

Assinado de forma digital por DAVID CANASSA:10595221874
Dados: 2026.08.05 15:48:31 -03'00'

SÓCIO ADMINISTRADOR

Araçoiaba da Serra, 05 de agosto de 2026