AVIG360 · PROGRAMA DE INTEGRIDADE E COMPLIANCE

Política de Segurança da Informação, Privacidade e Proteção de Dados

Governança de dados sensíveis na gestão psicossocial

EMPRESA	AVIG – Avaliação & Vigilância Integrada da Gestão Psicossocial Ltda. (AVIG360)		
CNPJ	53.012.185/0001-10	CÓDIGO	AVIG-COMP-003
VERSÃO	2.1	DATA DE EMISSÃO	14 de novembro de 2026
PRÓXIMA REVISÃO	Novembro de 2027	CLASSIFICAÇÃO	Público · Uso externo
APROVAÇÃO	Adriana Gomes Silva Dias Ribeiro, CEO		

1. Governança de dados sensíveis na gestão psicossocial

1.1 Objeto e fundamentação

A AVIG – Avaliação & Vigilância Integrada da Gestão Psicossocial Ltda. (AVIG360) oferece, em modelo SaaS (software como serviço), uma plataforma de monitoramento contínuo dos fatores de risco psicossocial relacionados ao trabalho. A atividade apoia as organizações no cumprimento da Norma Regulamentadora nº 1 (NR-1), no Gerenciamento de Riscos Ocupacionais (GRO) e no Programa de Gerenciamento de Riscos (PGR), e se baseia na literatura científica de saúde ocupacional e psicologia organizacional, que trata o adoecimento no trabalho como fenômeno de natureza coletiva e organizacional.

Sob o ponto de vista jurídico, as respostas individuais podem revelar informações sobre saúde física e mental e, por isso, são tratadas como **dados pessoais sensíveis** (art. 5º, II, e art. 11 da Lei nº 13.709/2018, a LGPD). A base legal do tratamento é, em regra, o cumprimento de obrigação legal e regulatória pelo controlador (art. 11, II, "a"), decorrente do GRO e do PGR previstos na NR-1. Quando a avaliação integrar procedimento conduzido por profissional ou serviço de saúde do controlador, aplica-se também a tutela da saúde (art. 11, II, "f"). A definição da base legal aplicável cabe ao controlador. O tratamento é regido pelos princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção e não discriminação (art. 6º). A AVIG360 atua como **operadora** dos dados em nome da organização contratante, que é a **controladora**, e segue as instruções documentadas do contrato.

1.2 Princípio estruturante

O diagnóstico psicossocial que interessa à gestão é coletivo: o objetivo é identificar fatores de risco em setores, funções e unidades, e não avaliar ou rotular pessoas. Por isso, a plataforma opera em **dois níveis de acesso, separados por design**:

Nível de gestão

Lideranças, gestores e a área de recursos humanos do cliente acessam **somente indicadores agregados e anonimizados**. Nenhuma resposta individual chega a esses perfis.

Nível de cuidado individual

O dado individual fica em área de acesso restrito, liberada apenas às pessoas **designadas formalmente pelo controlador**, sob dever de sigilo, para finalidades de cuidado e acompanhamento.

As finalidades do nível individual são o acolhimento, o encaminhamento em saúde ocupacional, o acompanhamento das pendências do Plano de Ação e o tratamento de emergências e denúncias. O dado individual nunca é usado para avaliação de desempenho, promoção, punição ou desligamento.

1.3 Fluxo do dado, da coleta aos painéis

1. **Informação ao titular e coleta individual.** O trabalhador responde ao instrumento diretamente no ambiente da plataforma, pelo próprio celular (por QR Code ou link) ou por credencial individual. Antes da coleta, o controlador informa o titular sobre a finalidade, o caráter sigiloso, as pessoas que podem acessar suas respostas individuais, o armazenamento dos dados fora do Brasil e o canal do Encarregado. A AVIG360 fornece ao controlador o modelo de aviso de privacidade com essas informações.
2. **Separação entre identificação e resposta.** Os dados que identificam o respondente são armazenados separados do conteúdo das respostas e vinculados apenas por identificadores técnicos (pseudonimização).
3. **Validação e tratamento em ambiente restrito.** As respostas são validadas e tratadas em ambiente isolado, acessível apenas por processos automatizados e por perfis técnicos autorizados.
4. **Agregação estatística.** O sistema calcula indicadores por grupo (setor, unidade, função, faixa de tempo de casa e semelhantes). **Grupos com menos de 10 respondentes não geram indicador numérico próprio**: a plataforma apresenta apenas a faixa de risco do grupo, sinalizada como **"indicativa"**, sem acesso às respostas que a compõem. A faixa indicativa orienta ações preventivas coletivas e não deve ser usada para conclusões sobre pessoas.
5. **Anonimização dos indicadores de gestão.** Os indicadores entregues no nível de gestão são gerados sem identificador direto ou indireto que permita, com meios técnicos razoáveis, reidentificar o titular. A base individual pseudonimizada continua sendo dado pessoal sensível e permanece sob todos os controles desta Política até o descarte.
6. **Entrega em dois níveis na Control Tower.**
   - *Painéis de gestão:* mapas de risco, níveis de exposição, faixas indicativas e planos de ação, sempre agregados.

- *Área de Acesso Individual Restrito:* páginas Colaboradores, Emergências e Denúncias, detalhe individual e relação nominal de pendências do Plano de Ação. Além do login individual com MFA, a área exige uma senha adicional de acesso restrito, gerida pelo Encarregado e entregue somente às pessoas designadas pelo controlador. A senha é armazenada em formato de hash e rotacionada pelo Encarregado. O desbloqueio expira após 15 minutos de inatividade, e nenhum perfil é isento, inclusive os administradores da AVIG360.
- *Comentários livres:* quando existirem, passam por revisão para remover informações que possam identificar o autor antes de qualquer exibição no nível de gestão.

7. **Retenção e descarte.** Os dados individuais são mantidos pelo tempo estritamente necessário à finalidade contratada e ao cumprimento de obrigações legais. Depois disso, são eliminados ou anonimizados, conforme o contrato e a instrução do controlador.

1.4 Garantias ao titular

- Lideranças, gestores e a área de recursos humanos não têm acesso a respostas individuais.
- O acesso individual é restrito às pessoas designadas por escrito pelo controlador, sujeitas a dever de sigilo. A área só é alcançada por usuário identificado, com login individual e MFA, e a senha adicional é rotacionada sempre que uma pessoa designada deixa a função.
- O titular é informado, antes de responder, sobre quem pode acessar suas respostas individuais e para quê.
- Os resultados não são utilizados para avaliação de desempenho, promoção, punição ou desligamento.
- O titular pode exercer seus direitos pelo canal descrito na seção 5.
- Cabe ao controlador definir a base legal, designar as pessoas com acesso individual e informar os titulares. Cabe à AVIG360 apoiar essas obrigações tecnicamente.

2. Infraestrutura, hospedagem e transferência internacional

2.1 Hospedagem

O ambiente de produção da plataforma é hospedado na **Render** (Render Services, Inc.), provedora de plataforma em nuvem com certificação **ISO/IEC 27001:2022** e relatório **SOC 2 Type II**, que atua como suboperadora da AVIG360. A Render não oferece região de hospedagem no Brasil. Por isso, os dados são armazenados em data center localizado no exterior, e a região de produção utilizada é informada ao controlador no contrato.

2.2 Transferência internacional de dados

O armazenamento no exterior configura transferência internacional de dados pessoais, realizada nos termos do **art. 33 da LGPD** e do Regulamento de Transferência Internacional de Dados aprovado pela **Resolução CD/ANPD nº 19/2024**:

- o tratamento pela provedora é regido pelo seu acordo de tratamento de dados (DPA). A incorporação das cláusulas-padrão contratuais aprovadas pela ANPD ao instrumento com a provedora está em formalização;

- o controlador é informado da transferência e a autoriza no contrato;
- os dados recebem no exterior o mesmo nível de proteção exigido por esta Política, com criptografia em trânsito e em repouso;
- o titular é informado, antes da coleta, de que seus dados são armazenados fora do Brasil.

2.3 Suboperadores

A AVIG360 mantém a relação atualizada dos suboperadores que tratam dados pessoais em seu nome e a informa ao controlador, com a localização do tratamento. Nenhum suboperador é contratado sem a avaliação prévia de maturidade em segurança da informação e proteção de dados prevista na Política Corporativa Anticorrupção e Antissuborno (item 5.1), e sem cláusulas contratuais de confidencialidade e proteção de dados. A relação vigente é:

SUBOPERADOR	FINALIDADE	DADOS TRATADOS
Render Services, Inc.	Hospedagem da aplicação e do banco de dados	Todos os dados da plataforma
Anthropic, PBC	Geração de textos analíticos e relatórios com inteligência artificial	Indicadores agregados, sem identificação de respondentes
Resend, Inc.	Envio de e-mails transacionais de acesso e recuperação de conta	Nome e e-mail dos usuários da Control Tower
Reprogramar (plataforma EAD)	Consulta de certificados das capacitações do Plano de Ação	CPF e nome dos participantes designados

3. Segurança por design e controles lógicos

A plataforma foi concebida segundo o conceito de *privacy by design* e *privacy by default*, com as diretrizes da ISO/IEC 27001 e da ISO/IEC 27701 como referência para a gestão da segurança e da privacidade da informação.

CONTROLE	MEDIDA ADOTADA
Criptografia em trânsito	Toda comunicação entre usuários, aplicações e serviços usa HTTPS obrigatório, com TLS 1.2 ou superior.
Criptografia em repouso	Bancos de dados, cópias de segurança e segredos são criptografados com padrão mínimo AES-256, com gestão controlada de chaves.
Controle de acesso	Acesso baseado em perfis, com o mínimo de privilégio necessário, autenticação obrigatória em todas as áreas restritas, MFA para os perfis de gestão e senha adicional para a Área de Acesso Individual Restrito.

Segregação de ambientes	Desenvolvimento, homologação e produção são separados, e a base de cada cliente é logicamente isolada das demais. Quando o diagnóstico de uma falha exige reproduzir dados reais fora da produção, o uso ocorre em cópia restrita à equipe técnica autorizada, sob dever de sigilo e com os mesmos controles de acesso, e a cópia é descartada ao fim da atividade.
Segregação de dados	Dados de identificação, respostas individuais e indicadores anonimizados ficam em camadas separadas, com permissões distintas.
Logs de auditoria	Acessos, alterações, exportações e ações administrativas são registrados com data, hora e usuário. Os registros são protegidos contra alteração, têm acesso restrito e são analisados periodicamente.
Cópias de segurança	Backups periódicos e criptografados, com testes de restauração e plano de continuidade.
Gestão de vulnerabilidades	Atualizações regulares, correção de falhas e testes de segurança periódicos nas aplicações e na infraestrutura.
Desenvolvimento seguro	Revisão de código, controle de versões e avaliação de privacidade obrigatória antes de qualquer nova funcionalidade que trate dados pessoais.

3.1 Minimização

Só são coletados os dados necessários ao diagnóstico contratado. Dados de identificação, como nome, CPF, telefone e e-mail, são usados para o controle de acesso e a participação. Eles não aparecem nos painéis de gestão e só são exibidos na Área de Acesso Individual Restrito.

3.2 Incidentes de segurança

Incidentes são tratados conforme plano de resposta, que inclui detecção, contenção, análise de causa, correção, registro e comunicação. A AVIG360 notifica o cliente controlador de forma imediata. Quando o incidente puder acarretar risco ou dano relevante aos titulares, o controlador e a AVIG360 comunicam a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares nos prazos e na forma da regulamentação vigente.

4. Governança de sistemas e perfis de acesso

4.1 Princípio do menor privilégio

Cada pessoa recebe apenas os acessos indispensáveis à sua função, pelo período necessário. Os perfis internos são definidos por função e aprovados pela diretoria. Contas de login são individuais e intransferíveis, e o compartilhamento de credenciais de login é proibido. A senha da Área de Acesso Individual Restrito não substitui o login individual: é uma camada adicional, comum às pessoas designadas, aplicada sobre contas que já são individuais e protegidas por MFA.

PERFIL	ALCANCE DO ACESSO
Titular (respondente)	Apenas ao seu próprio instrumento de resposta.
Liderança e gestores do cliente	Indicadores agregados e anonimizados da sua área de gestão e faixas indicativas, sem acesso a respostas individuais nem à relação nominal de pendências.
Administrador do cliente	Gestão de usuários e configurações da conta, sem acesso a respostas individuais.
Acesso Individual Restrito (designado pelo controlador)	Páginas Colaboradores, Emergências e Denúncias, detalhe individual e relação nominal de pendências do Plano de Ação, mediante a senha adicional gerida pelo Encarregado. São pessoas como o médico responsável pela saúde ocupacional e a área jurídica ou de compliance do cliente, conforme designação escrita do controlador.
Equipe técnica da AVIG360	Acesso limitado, sob demanda justificada e registrada, para suporte e manutenção.
Encarregado de dados (DPO)	Gestão e rotação da senha da Área de Acesso Individual Restrito, consulta aos registros de auditoria e aos relatórios de conformidade.

4.2 Autenticação e gestão de credenciais

- **Autenticação multifator (MFA) obrigatória** para todo perfil com acesso a dados de gestão ou a dados individuais, para administradores, para a equipe técnica e para o console da nuvem. Na Control Tower, o MFA é obrigatório para todos esses perfis desde setembro de 2026.
- A interface legada de administração (painel.avig360.com) está em migração para o mesmo padrão de autenticação da Control Tower. O respondente acessa o aplicativo com identificação própria e alcança apenas o seu instrumento de resposta.
- Na Control Tower, senhas com requisitos mínimos de complexidade e bloqueio após tentativas falhas, armazenadas com técnica de hash seguro.
- Tempo máximo de sessão ociosa, após o qual é exigida nova autenticação.
- Credenciais de serviço e chaves técnicas guardadas em cofre próprio, sem inclusão em código-fonte, e renovadas periodicamente.

4.3 Ciclo de vida do acesso

1. A concessão de acesso interno exige solicitação formal e aprovação da diretoria.
2. O Acesso Individual Restrito exige designação escrita do controlador, com nome, função e justificativa. O Encarregado entrega a senha adicional somente às pessoas designadas.
3. Alterações de função são seguidas de ajuste imediato do perfil.
4. O desligamento ou fim de contrato de colaborador ou prestador provoca a revogação de todos os acessos no mesmo dia. O controlador é orientado a comunicar a AVIG360 no mesmo prazo quando uma pessoa designada deixar a função, e o Encarregado rotaciona a senha adicional.
5. Acessos privilegiados são temporários e registrados, com justificativa.

4.4 Revisão periódica

Os acessos e perfis são revisados ao menos a cada seis meses, e sempre que houver mudança relevante no sistema ou na equipe, para identificar privilégios excessivos e contas inativas ou órfãs. A revisão inclui a confirmação, com cada controlador, da lista de pessoas com Acesso Individual Restrito. O resultado é registrado, e as correções são executadas em prazo definido. Todos os colaboradores e prestadores assinam termo de confidencialidade e recebem treinamento em segurança da informação e proteção de dados na admissão e anualmente.

5. Canal do titular e atuação do Encarregado (DPO)

5.1 O Encarregado pelo Tratamento de Dados Pessoais

A AVIG360 designou como Encarregado pelo Tratamento de Dados Pessoais, nos termos do art. 41 da LGPD, **Douglas da Silva Mota**, Engenheiro de Software e Analista de Dados. Contato: **dpo@avig360.com**.

Cabe ao Encarregado:

- receber e responder às solicitações dos titulares e às comunicações da ANPD;
- orientar colaboradores e prestadores sobre as práticas de proteção de dados;
- coordenar a elaboração e a atualização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para operações de alto risco, como o tratamento de dados sensíveis na avaliação psicossocial;
- gerir e rotacionar a senha da Área de Acesso Individual Restrito e entregá-la somente às pessoas designadas;
- conduzir a resposta a incidentes de segurança, com apoio da área técnica e da diretoria;
- acompanhar auditorias, revisões de acesso e a conformidade das medidas desta Política;
- apoiar os clientes controladores em suas obrigações perante os titulares e a ANPD.

O Encarregado atua com autonomia técnica e acesso direto à diretoria.

5.2 Direitos dos titulares (art. 18 da LGPD)

O titular pode solicitar, a qualquer momento e mediante requisição:

1. confirmação da existência de tratamento;
2. acesso aos dados;
3. correção de dados incompletos, inexatos ou desatualizados;
4. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
5. portabilidade dos dados;
6. eliminação dos dados tratados com consentimento, ressalvadas as hipóteses legais de conservação;
7. informação sobre as entidades públicas e privadas com as quais os dados foram compartilhados;
8. informação sobre a possibilidade de não fornecer consentimento e suas consequências;
9. revogação do consentimento, quando for a base legal do tratamento.

5.3 Como exercer os direitos

1. O titular envia a solicitação ao e-mail **dpo@avig360.com**, com nome completo e meio de contato. A AVIG360 pode pedir informações adicionais para confirmar a identidade, a fim de evitar acesso indevido.
2. A solicitação é registrada e o recebimento é confirmado.
3. A resposta é dada de forma imediata, em formato simplificado, ou, quando se tratar de declaração completa, no prazo de até 15 dias, conforme o art. 19 da LGPD.
4. Como a AVIG360 atua como operadora, a solicitação é encaminhada ao controlador (empresa contratante), que decide sobre o atendimento, e a AVIG360 apoia tecnicamente. O titular é informado do encaminhamento.
5. Indicadores já anonimizados não podem ser vinculados a um titular e, por isso, ficam fora do alcance de solicitações individuais, conforme o art. 12 da LGPD. A base individual pseudonimizada permanece sujeita a todos os direitos acima.

5.4 Relatório de Impacto e resposta a incidentes

O RIPD descreve as operações de tratamento, sua necessidade e proporcionalidade, os riscos aos titulares e as medidas de mitigação. Ele contempla expressamente o modelo de Acesso Individual Restrito, os suboperadores e a transferência internacional de dados, e é revisado a cada alteração relevante da plataforma. Em caso de incidente, o Encarregado coordena as ações de contenção, a avaliação do risco, o registro do evento e as comunicações ao controlador, à ANPD e aos titulares, conforme a regulamentação.

5.5 Vigência, revisão e chancela

Esta Política entra em vigor na data de sua assinatura, é revisada ao menos uma vez por ano e sempre que houver mudança legal, tecnológica ou nos riscos da operação, e é de cumprimento obrigatório por todos que tratam dados em nome da AVIG360. A versão 2.1 substitui a versão 2.0, de 13 de novembro de 2026.

Barueri/SP, 14 de novembro de 2026.

ADRIANA G S D RIBEIRO

Adriana Gomes Silva Dias Ribeiro

CEO – Chief Executive Officer · AVIG360

avig360.com · +55 11 94739-5288 · compliance@avig360.com · dpo@avig360.com