VALLUS.GRC

Política de Segurança da Informação (PSI) - Pública

O reforço das suas defesas.

Versão 1.0 - Julho/2026

SUMÁRIO

Política de Segurança da Informação (PSI) - Pública

Versão 1.0 — São Paulo, 5 de julho de 2026. Documento público, destinado ao Trust Center (vallusgrc.com.br). Resumo em linguagem acessível da postura de segurança da Vallus. Para detalhamento técnico completo sob NDA (relatórios de teste de intrusão, *Statement of Applicability*, evidências de auditoria), entre em contato pela Cláusula 10.

01 Nossa Abordagem

1.1. A VALLUS.GRC é construída para organizações que levam governança, risco e conformidade a sério — o que significa que aplicamos à nossa própria operação o mesmo rigor que ajudamos nossos clientes a exigir de si mesmos.

1.2. Nossa abordagem de segurança segue três princípios: **defesa em profundidade** (nenhum controle isolado é o único ponto de proteção), **menor privilégio** (acesso é concedido apenas quando estritamente necessário) e **transparência** (gaps conhecidos são priorizados e tratados, não escondidos).

02 Proteção de Dados e Criptografia

2.1. Dados em trânsito são protegidos com TLS 1.3. Dados em repouso, incluindo cópias de segurança, são criptografados. Segredos de aplicação (chaves de API, credenciais) são armazenados de forma cifrada.

2.2. Cópias de segurança do banco de dados são geradas diariamente, criptografadas antes de saírem do ambiente de produção, e o processo de restauração é testado periodicamente — não apenas configurado e esquecido.

2.3. Seus dados corporativos permanecem de sua titularidade. Tratamos apenas o necessário para operar a Plataforma, nunca vendemos dados pessoais, e detalhamos nossas práticas de privacidade na nossa Política de Privacidade pública.

03 Controle de Acesso e Isolamento entre Clientes

3.1. O acesso à Plataforma é controlado por papéis (administrador, editor, gestor de risco, auditor, executivo e visualizador), cada um com permissões específicas validadas a cada ação. Para versões Business e Enterprise há possibilidade de criação e customização de perfis.

3.2. Cada organização Cliente opera em um ambiente logicamente isolado das demais, com múltiplas camadas de controle de acesso e verificações automatizadas que impedem, por padrão, que dados de uma organização sejam visíveis a outra.

3.3. Sessões expiram automaticamente por inatividade, autenticação multifator está disponível para reforço de segurança da conta, e protegemos contra o uso de senhas conhecidamente vazadas em bases públicas.

04 Infraestrutura e Fornecedores

4.1. A Plataforma é hospedada em provedores de infraestrutura de porte internacional, com dados de produção armazenados no Brasil. Utilizamos um conjunto reduzido e avaliado de

fornecedores especializados (hospedagem, banco de dados, autenticação, e-mail transacional, inteligência artificial, monitoramento de erros e armazenamento de backup), listados de forma atualizada em nossa Lista de Sub-operadores pública.

4.2. Não construímos nossa própria infraestrutura física — nos apoiamos em provedores que investem, em escala muito maior do que qualquer empresa isolada conseguiria, em segurança física e resiliência de datacenter.

05 Monitoramento e Resposta a Incidentes

5.1. Monitoramos continuamente a disponibilidade e a integridade da Plataforma, com mais de um sistema independente de monitoramento por redundância.

5.2. Temos um processo definido de resposta a incidentes: detecção, investigação com metodologia de causa-raiz, correção, verificação e só então encerramento — nunca fechamos um alerta sem confirmar que a correção está de fato em produção.

5.3. Incidentes de segurança que possam afetar dados pessoais são tratados conforme a Lei Geral de Proteção de Dados (LGPD), incluindo, quando aplicável, comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

06 Segurança no Ciclo de Desenvolvimento

6.1. Nenhuma alteração chega à versão em produção sem passar por um conjunto automatizado de verificações: testes automatizados, varredura de vulnerabilidades em dependências de terceiros, verificação de segredos expostos acidentalmente e regras de segurança específicas que bloqueiam mudanças de risco antes do merge.

6.2. Realizamos varreduras periódicas e contínuas de segurança de código e de dependências, com processo formal de triagem e priorização de qualquer achado.

07 Testes de Segurança e Certificações

7.1. Estamos em processo estruturado de maturidade de segurança e conformidade, incluindo a preparação para certificação ISO/IEC 27001.

7.2. Um teste de intrusão (*pentest*) externo, conduzido por fornecedor independente especializado, está planejado como parte desse processo, com escopo já definido cobrindo aplicação web, APIs e os recursos de Inteligência Artificial da Plataforma.

7.3. Atualizaremos esta página conforme certificações e testes forem concluídos, com evidências disponíveis sob NDA mediante solicitação (Cláusula 10).

08 Continuidade de Negócio

8.1. Mantemos cópias de segurança diárias com processo de restauração documentado e testado, reduzindo o risco de perda de dados em caso de incidente grave.

8.2. Estamos formalizando um plano de continuidade de negócio mais amplo como parte do nosso *roadmap* de maturidade.

09 Privacidade e Conformidade Legal

9.1. Tratamos dados pessoais em conformidade com a LGPD (Lei nº 13.709/2018). Detalhes completos sobre papéis, finalidades, bases legais e direitos dos titulares estão na nossa Política de Privacidade.

9.2. Mantemos um Encarregado pelo Tratamento de Dados (DPO) disponível para dúvidas e solicitações.

10 Divulgação Responsável e Contato

10.1. Se você é pesquisador de segurança e identificou uma potencial vulnerabilidade em nossa Plataforma, entre em contato pelo canal indicado abaixo. Pedimos que nos dê a oportunidade de investigar e corrigir antes de qualquer divulgação pública, e nos comprometemos a responder em prazo razoável.

10.2. Contato de segurança: security@vallusgrc.com.br. Encarregado de Proteção de Dados: dpo@vallusgrc.com.br.

10.3. Para *due diligence* de segurança mais aprofundada (questionários CAIQ/SIG, evidências sob NDA), entre em contato pelo mesmo canal.