

3. POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO DA VITRINE DE CRAQUES

(Versão completa, técnica, jurídica e definitiva para revisão)

1. Finalidade da Política

A presente **Política de Proteção de Dados Pessoais e Segurança da Informação da Vitrine de Craques** (“Política”) estabelece princípios, diretrizes, controles, responsabilidades e padrões obrigatórios para tratamento seguro dos dados pessoais tratados pela Plataforma, garantindo conformidade integral com:

- **Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018)**
- **Marco Civil da Internet (Lei nº 12.965/2014)**
- **Estatuto da Criança e do Adolescente (Lei nº 8.069/1990)**
- **Código de Defesa do Consumidor**
- Boas práticas internacionais de segurança (ISO/IEC 27001, NIST CSF)
- Regulamentações esportivas específicas, quando aplicáveis

Esta Política vincula todos os usuários, colaboradores internos, prestadores de serviço, parceiros, agentes, clubes, empresários, olheiros, jornalistas e demais categorias cadastradas.

2. Princípios Fundamentais de Segurança e Proteção de Dados

A Vitrine de Craques adota rigorosamente os seguintes princípios:

1. **Finalidade específica:** nenhum dado é tratado para propósito incompatível.
2. **Adequação:** todos os tratamentos são compatíveis com as atividades da plataforma.
3. **Necessidade:** coleta mínima indispensável.
4. **Transparência total:** comunicação objetiva com titulares.
5. **Prevenção:** adoção prévia de medidas para evitar incidentes.
6. **Segurança:** proteção contra acessos não autorizados ou ilícitos.
7. **Responsabilização:** documentação completa das ações.
8. **Não discriminação.**
9. **Boa-fé e conformidade integral com a LGPD.**

3. Responsabilidades do Controlador e do Encarregado (DPO)

3.1 Controlador

A Vitrine de Craques é **Controladora** dos dados pessoais sob sua guarda, sendo responsável por:

- definir finalidades e bases legais
- garantir segurança e confiabilidade
- supervisionar terceiros
- responder ao titular e às autoridades

3.2 Encarregado (DPO)

O DPO é responsável por:

- receber e responder solicitações LGPD
- orientar a organização
- interagir com a ANPD
- monitorar práticas internas
- acompanhar auditorias

Dados do DPO:

Nome: [Inserir]

E-mail: [Inserir]

Canal LGPD: [Inserir]

4. Classificação das Informações

A Vitrine de Craques classifica os dados em categorias, garantindo controles apropriados:

4.1 Dados Públicos

- Dados de perfis esportivos tornados públicos voluntariamente.

4.2 Dados Internos

- Informações administrativas necessárias à operação.

4.3 Dados Confidenciais

- Dados pessoais
- Dados sensíveis
- Documentos de verificação
- Dados de contato de responsáveis legais
- Informações de segurança

4.4 Dados Ultra Sensíveis

Especial proteção, incluindo:

- Dados de crianças e adolescentes
 - Vídeos, fotos e imagens pessoais
 - Informações físicas, atléticas ou biométricas
 - Comprovantes de identidade e documentos oficiais
-

5. Controles Técnicos de Segurança

A Vitrine de Craques adota um conjunto robusto de controles, abrangendo:

5.1 Criptografia

- Dados em trânsito: criptografia TLS 1.2 ou superior
- Dados em repouso: criptografia AES-256
- Senhas: hashing seguro com salting e algoritmos adequados (ex.: bcrypt)

5.2 Gestão de Acessos

- Acesso restrito por função
- Mínimo privilégio (least privilege)
- Autenticação em dois fatores (2FA) para administradores
- Revisões periódicas de permissões
- Perfis privilegiados monitorados

5.3 Segurança de Aplicações

- Proteção contra ataques conhecidos (OWASP Top 10)
- Prevenção contra injeção de código
- Firewalls de aplicação (WAF)
- Proteção contra scraping e automação indevida
- Sanitização de entrada de dados

5.4 Segurança de Infraestrutura

- Data centers certificados (ISO 27001, SOC 2 ou equivalente)
- Segmentação de redes
- Monitoramento contínuo 24/7
- Logs detalhados de eventos críticos

- Backups criptografados e redundantes

5.5 Monitoramento e Detecção

- Sistemas de detecção de intrusão (IDS/IPS)
 - Análise comportamental
 - Alertas automáticos de violação
 - Auditoria constante de requisições críticas
-

6. Controles Administrativos e Processuais

6.1 Políticas Internas Obrigatórias

A plataforma mantém:

- Política de acesso interno
- Política de retenção e descarte
- Procedimento de verificação de identidade
- Política de moderação de conteúdo
- Procedimento de resposta a incidentes
- Treinamento obrigatório de colaboradores

6.2 Treinamento e Conscientização

Todos os colaboradores e terceiros com acesso a dados passam por treinamento:

- LGPD
- Segurança da informação
- Tratamento de dados de menores
- Ética e confidencialidade

6.3 Contratos com Terceiros (DPA)

Todo fornecedor que trate dados deve:

- cumprir a LGPD
 - adotar medidas equivalentes de segurança
 - ser auditável
 - tratar apenas o necessário
 - excluir dados ao final da prestação
-

7. Registro das Atividades de Tratamento (ROPA)

A Vitrine de Craques mantém documentação integral das operações:

- categoria de dados
- finalidade
- base legal
- prazo de retenção
- responsáveis
- compartilhamentos
- mecanismos de segurança

Disponível à ANPD quando requisitado.

8. Tratamento de Dados Sensíveis e de Menores

8.1 Dados Sensíveis

Qualquer dado sensível é tratado com:

- consentimento específico
- controle reforçado
- acesso restrito
- criptografia
- auditoria permanente

8.2 Dados de Crianças e Adolescentes

A plataforma adota proteção reforçada:

- consentimento verificável do responsável legal
 - acesso supervisionado
 - comunicação intermediada pelo responsável
 - bloqueio automático de adultos não autorizados
 - proibição de contato direto não supervisionado
 - tratamento mínimo necessário
-

9. Prevenção, Detecção e Resposta a Incidentes

A Vitrine de Craques possui **Plano de Resposta a Incidentes**, incluindo:

1. Identificação imediata
2. Contenção
3. Análise de impacto
4. Mitigação de danos
5. Registros completos
6. Comunicação ao titular quando necessário
7. Comunicação à ANPD nos casos exigidos
8. Adoção de medidas preventivas pós-incidente

Qualquer incidente será tratado com máxima prioridade.

10. Armazenamento, Retenção e Descarte

10.1 Retenção

- Logs mínimos exigidos: 6 meses (Marco Civil)
- Conteúdos do usuário: enquanto a conta estiver ativa
- Dados sensíveis: apenas pelo tempo indispensável
- Documentos de verificação: conforme necessidade operacional

10.2 Descarte Seguro

Ao final da necessidade:

- dados são deletados com técnicas seguras
 - backups são eliminados após prazos legais
 - terceiros são obrigados a comprovar descarte
-

11. Auditorias e Monitoramento de Conformidade

A plataforma realiza auditorias internas e externas periódicas para:

- validar segurança
- revisar controles
- testar vulnerabilidades
- comprovar aderência à LGPD

Todos os resultados são documentados.

12. Transferências Internacionais

Permitidas somente quando houver:

- país com nível adequado de proteção
 - cláusulas contratuais específicas
 - comprovação de segurança equivalente
 - consentimento informado quando exigido
-

13. Comunicação com Autoridades

A Vitrine de Craques coopera com:

- ANPD
- Ministério Público
- Autoridades judiciais

Sempre respeitando:

- limites legais
 - necessidade comprovada
 - proteção de menores
-

14. Atualizações da Política

A Política pode ser atualizada por:

- exigência legal
- inserção de novas tecnologias
- mudança de procedimentos internos

Quaisquer atualizações relevantes serão comunicadas ao usuário.

15. Foro e Legislação Aplicável

Esta Política é regida integralmente pela legislação brasileira.

Fica eleito o foro da comarca de [inserir cidade/estado], com renúncia de qualquer outro.