

POLITICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Esta Política estabelece os princípios, diretrizes e controles mínimos de Segurança da Informação adotados pela Empresa, visando assegurar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações utilizadas em suas atividades.

A política busca proteger ativos físicos, digitais e intelectuais, reduzir riscos cibernéticos, fortalecer a governança corporativa e garantir a continuidade dos negócios.

2. Abrangência

Esta Política aplica-se a:

- ✓ sócios;
- ✓ administradores;
- ✓ colaboradores;
- ✓ desenvolvedores;
- ✓ terceiros;
- ✓ prestadores de serviços;
- ✓ fornecedores;
- ✓ consultores;
- ✓ parceiros comerciais que possuam acesso às informações ou aos ambientes tecnológicos da Empresa.

3. Natureza da Atividade

A Empresa atua no desenvolvimento de soluções tecnológicas destinadas ao mercado regulado de apostas esportivas, oferecendo software, integrações, APIs, arquitetura tecnológica e suporte especializado.

Por essa razão, reconhece que a proteção das informações representa um dos pilares fundamentais para a continuidade de seus negócios e para a confiança de seus clientes.

4. Princípios

Toda atividade relacionada à segurança da informação observará os seguintes princípios:

- ✓ Confidencialidade;
- ✓ Integridade;
- ✓ Disponibilidade;
- ✓ Autenticidade;
- ✓ Rastreabilidade;

- ✓ Menor Privilégio;
- ✓ Necessidade de Conhecimento;
- ✓ Segurança desde a Concepção (Security by Design);
- ✓ Privacidade desde a Concepção (Privacy by Design);
- ✓ Melhoria Contínua.

5. Governança

A Diretoria é responsável pela implementação desta Política.

Compete à Administração:

- ✓ aprovar esta Política;
 - ✓ disponibilizar recursos necessários;
 - ✓ incentivar a cultura de segurança;
 - ✓ apoiar auditorias;
 - ✓ promover treinamentos periódicos.
-
- ✓ O responsável técnico deverá:
 - ✓ acompanhar a aplicação desta Política;
 - ✓ recomendar melhorias;
 - ✓ coordenar ações de resposta a incidentes;
 - ✓ apoiar auditorias;
 - ✓ elaborar relatórios periódicos destinados à Diretoria.

6. Ativos de Informação

- ✓ Constituem ativos de informação da Empresa, entre outros:
 - ✓ código-fonte;
 - ✓ APIs;
 - ✓ bancos de dados;
 - ✓ credenciais de acesso;
 - ✓ documentação técnica;
 - ✓ contratos;
 - ✓ registros de clientes;
 - ✓ infraestrutura em nuvem;
 - ✓ servidores;
 - ✓ equipamentos corporativos;
 - ✓ repositórios de desenvolvimento;
 - ✓ documentação interna;
 - ✓ propriedade intelectual.

Todos os ativos deverão receber proteção compatível com seu nível de criticidade.

7. Classificação das Informações

As informações deverão ser classificadas, no mínimo, nas seguintes categorias:

Pública – informações destinadas ao conhecimento público.

Uso Interno – informações restritas ao ambiente corporativo.

Confidencial – informações cujo acesso é limitado a pessoas autorizadas.

Restrita – informações críticas cujo acesso dependerá de autorização específica da Diretoria ou do responsável técnico.

8. Controle de Acessos

O acesso aos sistemas corporativos observará os princípios do menor privilégio e da necessidade de conhecimento.

Serão adotadas, sempre que possível:

- ✓ autenticação multifator (MFA);
- ✓ senhas fortes;
- ✓ revisão periódica de acessos;
- ✓ bloqueio automático de contas inativas;
- ✓ revogação imediata de acessos após desligamento;
- ✓ segregação de perfis administrativos.
- ✓ Credenciais são individuais, intransferíveis e de responsabilidade exclusiva do usuário.

9. Desenvolvimento Seguro de Software (SSDLC)

A Empresa adotará práticas de Secure Software Development Lifecycle (SSDLC) em todas as fases do desenvolvimento de software.

Os projetos deverão considerar requisitos de segurança desde a concepção da solução, incluindo: análise de riscos; revisão de arquitetura; validação de requisitos de segurança; revisão de código; testes de segurança; correção de vulnerabilidades antes da implantação em produção.

Sempre que aplicável, serão observadas as boas práticas da OWASP e de frameworks reconhecidos internacionalmente.

É vedada a inclusão intencional de funcionalidades ocultas, credenciais embutidas em código-fonte ou mecanismos que comprometam a integridade da aplicação.

10. Gestão de Código-Fonte

O código-fonte deverá ser armazenado em repositórios corporativos com controle de acesso e registro de alterações.

Serão adotadas, sempre que possível:

- ✓ autenticação multifator para acesso aos repositórios;
- ✓ segregação entre ambientes de desenvolvimento e produção;
- ✓ revisão de pull requests;

- ✓ rastreabilidade de alterações;
- ✓ backups dos repositórios;
- ✓ controle de versões.

O compartilhamento de código-fonte fora dos ambientes autorizados depende de aprovação formal da Empresa.

11. Gestão de Vulnerabilidades

A Empresa realizará atividades periódicas de identificação, avaliação e tratamento de vulnerabilidades.

Os controles poderão incluir:

- ✓ varreduras automatizadas;
- ✓ análise de dependências;
- ✓ atualização de bibliotecas;
- ✓ aplicação de patches de segurança;
- ✓ testes de intrusão (penetration tests);
- ✓ monitoramento de vulnerabilidades críticas divulgadas publicamente.

Vulnerabilidades classificadas como críticas deverão receber tratamento prioritário.

12. Criptografia

Informações sensíveis deverão ser protegidas por mecanismos de criptografia compatíveis com as boas práticas de mercado.

A criptografia será aplicada, sempre que apropriado:

- ✓ em dados em trânsito;
- ✓ em dados armazenados;
- ✓ em backups;
- ✓ em comunicações administrativas;
- ✓ em integrações com terceiros.

As chaves criptográficas deverão ser gerenciadas de forma segura, com acesso restrito e controle de ciclo de vida.

13. Segurança em Nuvem

A infraestrutura em nuvem deverá ser configurada segundo princípios de segurança por padrão.

Serão observados, entre outros:

- ✓ segmentação de ambientes;
- ✓ controle de acessos privilegiados;
- ✓ registro de eventos;
- ✓ monitoramento de atividades;
- ✓ proteção contra exposição indevida de serviços;

- ✓ revisão periódica de configurações.

Ambientes de desenvolvimento, homologação e produção deverão permanecer segregados.

14. Backups e Recuperação

A Empresa manterá rotinas de backup compatíveis com a criticidade de seus sistemas.

Os backups deverão, sempre que possível:

- ✓ ser automatizados;
- ✓ ser criptografados;
- ✓ possuir cópia em local distinto do ambiente principal;
- ✓ ser testados periodicamente quanto à capacidade de restauração.

Os procedimentos de recuperação deverão permitir a retomada das operações em prazo compatível com a continuidade do negócio.

15. Registro e Monitoramento

Os sistemas corporativos deverão manter registros (logs) suficientes para permitir rastreabilidade de eventos relevantes.

Poderão ser registrados:

- ✓ autenticações;
- ✓ tentativas de acesso;
- ✓ alterações administrativas;
- ✓ implantações em produção;
- ✓ eventos de segurança;
- ✓ atividades privilegiadas.

Os registros serão protegidos contra alteração indevida e mantidos pelo período definido nas normas internas ou na legislação aplicável.

16. Resposta a Incidentes

Todo evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade das informações será tratado como incidente de segurança.

O processo de resposta poderá incluir:

- ✓ identificação;
- ✓ contenção;
- ✓ erradicação;
- ✓ recuperação;
- ✓ análise de causa raiz;
- ✓ registro das evidências;
- ✓ comunicação interna;
- ✓ comunicação externa quando legalmente exigida.

Incidentes relevantes deverão ser reportados à Diretoria com a maior brevidade possível.

17. Continuidade de Negócios

A Empresa manterá medidas destinadas a reduzir impactos decorrentes de indisponibilidade de sistemas, falhas de infraestrutura, ataques cibernéticos ou outros eventos críticos.

Os planos de continuidade deverão considerar:

- ✓ sistemas essenciais;
- ✓ prioridades de recuperação;
- ✓ responsabilidades das equipes;
- ✓ comunicação em situações de crise;
- ✓ testes periódicos.

18. Segurança de Terceiros

A Empresa poderá compartilhar informações e permitir acesso a sistemas somente quando necessário à execução de contratos ou atividades legítimas, observando critérios de segurança compatíveis com o nível de risco envolvido.

Sempre que aplicável, fornecedores, consultores e parceiros deverão assumir compromissos de confidencialidade e proteção das informações, além de cumprir os requisitos de segurança estabelecidos pela Empresa.

O acesso concedido a terceiros deverá observar o princípio do menor privilégio e ser revisto periodicamente, sendo imediatamente revogado quando deixar de existir a necessidade operacional.

19. Trabalho Remoto

O acesso remoto aos recursos tecnológicos da Empresa deverá ocorrer por meios autorizados e seguros.

Os colaboradores deverão observar, entre outras diretrizes:

- ✓ utilização de equipamentos confiáveis;
- ✓ proteção física dos dispositivos utilizados;
- ✓ bloqueio automático de tela durante ausências;
- ✓ atualização periódica dos sistemas operacionais e aplicativos;
- ✓ vedação ao compartilhamento de credenciais;
- ✓ utilização de redes seguras para acesso aos ambientes corporativos.

Sempre que possível, conexões remotas deverão utilizar mecanismos de autenticação multifator e comunicação criptografada.

20. Conscientização e Capacitação

A Empresa promoverá ações periódicas de conscientização em Segurança da Informação, visando fortalecer a cultura organizacional e reduzir riscos decorrentes de falhas humanas.

Os treinamentos poderão abordar, entre outros temas:

- ✓ boas práticas de segurança digital;
- ✓ proteção de credenciais;
- ✓ prevenção a ataques de engenharia social;
- ✓ identificação de tentativas de phishing;
- ✓ classificação das informações;
- ✓ uso seguro dos recursos tecnológicos;
- ✓ tratamento de incidentes.

A participação dos colaboradores poderá ser registrada para fins de controle interno.

21. Auditoria e Monitoramento

A Empresa poderá realizar auditorias internas, avaliações técnicas ou revisões periódicas com o objetivo de verificar a efetividade desta Política.

As auditorias poderão abranger:

- ✓ controles de acesso;
- ✓ registros de eventos;
- ✓ gestão de vulnerabilidades;
- ✓ processos de desenvolvimento seguro;
- ✓ proteção de ativos;
- ✓ conformidade com normas internas.

Sempre que identificadas oportunidades de melhoria, serão adotadas medidas corretivas proporcionais aos riscos identificados.

22. Descumprimento da Política

O descumprimento desta Política poderá caracterizar violação das normas internas da Empresa. Conforme a gravidade da ocorrência, poderão ser adotadas medidas administrativas e contratuais, incluindo:

- ✓ orientação formal;
- ✓ advertência;
- ✓ suspensão de acessos;
- ✓ revisão de permissões;
- ✓ rescisão contratual, quando aplicável;
- ✓ comunicação às autoridades competentes, caso haja obrigação legal.

A aplicação das medidas observará os princípios da proporcionalidade, razoabilidade e ampla apuração dos fatos.

23. Revisão e Melhoria Contínua

Esta Política será revisada, no mínimo, uma vez por ano ou sempre que ocorrerem:

- ✓ alterações legislativas;
- ✓ mudanças regulatórias;
- ✓ modificações relevantes na infraestrutura tecnológica;
- ✓ incidentes relevantes de segurança;
- ✓ alterações significativas nas atividades da Empresa.

As atualizações deverão ser aprovadas pela Diretoria e registradas no controle de versões.

24. Vigência

Esta Política entra em vigor na data de sua aprovação e permanecerá válida até que seja formalmente substituída por nova versão.

Aprovação

Elaboração e Revisão Jurídica

Everson Alessandro Pereira

Advogado – OAB/SC 12.470

Especialista em Direito Digital



Documento assinado digitalmente

EVERSON ALESSANDRO PEREIRA

Data: 04/08/2026 16:59:32-0300

Verifique em <https://validar.iti.gov.br>