POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Portal Executivo mTinoco.eti.br | Marco Maurício Tinoco

Versão 1.0 – Vigência a partir de Abril de 2026

1. Escopo e Propósito

A presente Política estabelece as diretrizes de segurança aplicadas aos ativos de informação do portal **mTinoco.eti.br**. Como especialista em Soberania Digital e Governança, Marco Maurício Tinoco assegura que a proteção dos dados pessoais e a integridade das operações acadêmicas e consultivas seguem os mais rigorosos padrões de mercado, alinhados à ISO/IEC 27001 e à LGPD.

2. Segurança da Infraestrutura e Hospedagem

O portal é hospedado em ambiente de alta disponibilidade (WebServer), contando com:

- **Criptografia em Trânsito:** Todo o tráfego de dados entre o navegador do usuário e o servidor é protegido pelo protocolo **TLS 1.3 (HTTPS)**, impedindo ataques de interceptação (*Man-in-the-Middle*).
- **Roteamento Seguro:** A utilização de regras customizadas via .htaccess garante o redirecionamento forçado para conexões seguras e impede a navegação não autorizada em diretórios sensíveis do servidor.

3. Blindagem de Aplicação e Backend

A arquitetura do portal foi desenhada sob o conceito de "Defesa em Profundidade":

- **Segurança de Formulários (Anti-Bot):** Implementação de técnica *Honeypot* (bot_field), capaz de identificar e descartar submissões automatizadas de robôs sem coletar dados biométricos desnecessários dos usuários.
- **Backend Seguro (PHP/PHPMailer):** O processamento de e-mails é isolado no servidor. As credenciais de acesso SMTP são *hardcoded* no lado do servidor, tornando-as invisíveis para qualquer análise de código-fonte no navegador (*Frontend*).

- **Prevenção contra Abusos (*Open Relay*):** O script de *backend* possui destinatário fixo (contato@mtinoco.eti.br), impossibilitando que terceiros utilizem a infraestrutura do portal para o disparo de SPAM ou ataques de *phishing*.

4. Governança e Rastreabilidade (*Compliance*)

Cada interação crítica no portal gera uma cadeia de evidências digitais:

- **Protocolo de Consentimento Forense:** Ao submeter dados, o sistema registra o endereço IP, *User-Agent* e carimbo de tempo (*Timestamp*). Este registro assegura o princípio do não-repúdio e serve como lastro jurídico em auditorias de conformidade.
- **CORS (*Cross-Origin Resource Sharing*):** Cabeçalhos de segurança restringem as requisições ao *backend*, garantindo que apenas o domínio oficial possa interagir com as funções de disparo de dados.

5. Área Acadêmica e Gestão de Acessos

O acesso a conteúdos exclusivos para alunos segue protocolos de autorização controlada:

- **Segurança por Token:** O acesso à rota /academia é protegido por validação de *tokens* de turma, impedindo a indexação pública de materiais restritos.
- **Repositórios Isolados:** A integração com o Microsoft OneDrive utiliza *tokens* de compartilhamento específicos, mantendo a integridade dos arquivos originais fora da raiz de hospedagem do site.

6. Monitoramento e Analytics

A utilização do **Google Analytics 4 (GA4)** é realizada de forma ética e minimizada. O portal prioriza a coleta de dados comportamentais anonimizados, focando na performance técnica e na relevância do conteúdo para o usuário, sem rastreio de identidade individual fora dos contextos de consentimento explícito.

7. Continuidade de Negócio

Para garantir a soberania das informações, são realizados backups periódicos da estrutura do portal e das bases de conhecimento acadêmico, assegurando a rápida recuperação em caso de incidentes técnicos no provedor de hospedagem.

8. Canais de Denúncia e Contato

Qualquer vulnerabilidade identificada ou dúvida sobre o tratamento seguro de dados deve ser reportada imediatamente ao Encarregado de Proteção de Dados (DPO):

- **E-mail:** contato@mtinoco.eti.br

Marco Maurício Tinoco – Especialista em Governança de TI, DPO e Perito Computacional. Última atualização: 19 de Abril de 2026.