

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

1. Objetivos e Escopo

A presente Política de Segurança da Informação (PSI) estabelece os princípios, diretrizes e normas de segurança cibernética e proteção de dados aplicáveis à **Marco Zero Conteúdo Ltda.** O objetivo principal é proteger os ativos de informação da empresa contra acessos não autorizados, vazamentos, perdas, adulterações e ameaças cibernéticas.

Esta PSI aplica-se a todos os sócios, colaboradores, jornalistas, produtores de eventos, estagiários, prestadores de serviços e parceiros comerciais que utilizem a infraestrutura tecnológica ou manuseiem dados corporativos, editoriais, de clientes ou de congressistas/participantes de eventos.

2. Princípios Fundamentais da Segurança da Informação

- **Confidencialidade:** Garantia de que as informações sejam acessíveis apenas por pessoas devidamente autorizadas.
- **Integridade:** Salvaguarda da exatidão e completude das informações e dos métodos de processamento.
- **Disponibilidade:** Garantia de que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Privacidade por Padrão (Privacy by Default):** Proteção rigorosa dos dados pessoais de fontes, clientes e participantes de eventos, em consonância com a LGPD (Lei nº 13.709/2018).

3. Classificação das Informações e Dados

Todas as informações produzidas, custodiadas ou manuseadas no âmbito da Marco Zero Conteúdo Ltda. devem ser classificadas em quatro níveis:

Nível de Classificação	Descrição e Exemplos	Diretriz de Acesso e Custódia
Pública	Notícias publicadas, edições finais de revistas/livros, programação aberta de feiras e congressos.	Acesso livre ao público em geral. Sem restrições.
Interna	Comunicados internos, organogramas, minutas operacionais de eventos e diretrizes não sigilosas.	Acesso permitido a todos os colaboradores e contratados da empresa.
Confidencial	Identidade protegida de fontes jornalísticas, dados cadastrais de congressistas (LGPD), contratos com patrocinadores e relatórios financeiros.	Acesso restrito estritamente a pessoas designadas que necessitam da informação para suas funções.
Restrita / Ultrassecreta	Investigações jornalísticas em andamento, estratégias de negócios da diretoria, credenciais mestre de sistemas e segredos de empresa.	Acesso exclusivo aos sócios e profissionais diretamente envolvidos sob Termo de Confidencialidade (NDA).

4. Diretrizes de Uso de Ativos e Infraestrutura Tecnológica

4.1. Controle de Acesso e Senhas

- É obrigatória a utilização de autenticação de dois fatores (2FA/MFA) em todas as contas corporativas (e-mail, armazenamento em nuvem, gerenciadores de conteúdo de sites e sistemas de credenciamento).
- As senhas devem possuir no mínimo 12 caracteres, combinando letras maiúsculas, minúsculas, números e símbolos, devendo ser alteradas periodicamente. É proibido o compartilhamento de senhas pessoais entre colaboradores.

4.2. Segurança em Dispositivos Móveis e Trabalho Remoto/Em Campo

- Computadores, smartphones e câmeras utilizados em coberturas jornalísticas ou na

operação de feiras e eventos devem estar protegidos por senha/biometria e criptografia de disco ativada.

- É proibida a conexão de dispositivos corporativos a redes Wi-Fi públicas sem o uso de VPN (Rede Privada Virtual) homologada.
- Em caso de perda, roubo ou furto de equipamento contendo dados corporativos ou editoriais, a equipe de TI/Direção deve ser informada em até 2 horas para bloqueio e limpeza remota (*wipe*).

4.3. Segurança do Sigilo Jornalístico e Proteção de Fontes

- Documentos e comunicações com fontes que exijam sigilo reservado devem ser transacionados exclusivamente por canais com criptografia de ponta a ponta ou armazenados em cofres digitais com acesso restrito.
- É vedado o upload não criptografado de gravações de áudio e notas de apuração sensíveis em pastas compartilhadas abertas.

5. Segurança da Informação na Operação de Eventos (Feiras, Congressos e Festas)

- **Sistemas de Credenciamento e Cadastro:** As plataformas digitais utilizadas para inscrição e venda de ingressos devem estar em ambiente seguro (HTTPS/TLS) e integradas a gateways de pagamento em conformidade com o padrão PCI-DSS.
- **Manipulação de Listas de Presença e Mailing:** Listas de participantes e congressistas contendo dados pessoais (nome, CPF, e-mail, cargo) devem ter acesso restrito à equipe de credenciamento e ser eliminadas ou anonimizadas após a prestação de contas do evento, salvo consentimento (*opt-in*) para mailing contínuo.
- **Segurança Física de Equipamentos em Campo:** Servidores locais, switches de rede, mesas de corte de transmissão e computadores de credenciamento em feiras e congressos devem permanecer em áreas restritas com controle de acesso físico.

6. Resposta a Incidentes de Segurança e Notificação de Vazamentos

- **Plano de Resposta a Incidentes:** Ocorrendo suspeita ou confirmação de ataque cibernético (ex.: *ransomware*, *phishing*, invasão de site) ou vazamento de dados, a equipe deve acionar imediatamente a Gestão de Incidentes.
- **Notificação sob a LGPD:** Caso o incidente envolva dados pessoais que possam acarretar risco ou dano relevante aos titulares (congressistas, leitores ou clientes), a empresa realizará a notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos afetados nos prazos legais.

7. Conscientização, Treinamento e Sanções

- **Capacitação Contínua:** Todos os colaboradores passarão por orientações periódicas sobre engenharia social, prevenção a *phishing* e boas práticas de proteção de dados.
- **Consequências Disciplinares:** A violação intencional ou por negligência grave destas diretrizes resultará em sanções disciplinares (advertência, suspensão ou rescisão por justa causa), além das responsabilizações cíveis e criminais aplicáveis.

8. Disposições Finais

Esta Política de Segurança da Informação entra em vigor na data de sua publicação e será revisada anualmente para adequação a novas ameaças tecnológicas e alterações legislativas.

Marco Zero Conteúdo Ltda.

CNPJ: 36.234.429/0001-90

Sede: Rua Alexandre Martins, nº 3, cj. 7101 – Santos/SP

falecom.marcozero.blog.br