Moção 45

Pela segurança digital dos órgãos internos do LIVRE.

Fundamentação

Na era digital, cada vez mais marcada pela dependência de organizações em plataformas digitais para comunicar, gerir documentos, coordenar atividades e gerir o seu dia a dia, conseguimos observar um aumento da exposição a ameaças como ataques informáticos, phishing, ransomware, fugas de informação e utilização indevida de credenciais. Só em 2025, segundo o Centro Nacional de Cibersegurança, o número de ciberataques aumentou em 36% face a 2024[1].

A facilidade de acesso a ferramentas de IA aumentou exponencialmente o número de potenciais atacantes. Onde antes era preciso alguém que soubesse o que estava a fazer, hoje basta alguém mal-intencionado; se a segurança for frágil, as ferramentas ensinam a quebrá-la.

Uma simples falha de segurança pode pôr em risco dados pessoais e informações confidenciais em meros instantes e criar um ambiente onde o atacante tem acesso a plataformas essenciais para a comunicação do partido, arriscando severamente danos reputacionais que põem em causa a confiança do eleitorado.

Muitas destas vulnerabilidades decorrem do desconhecimento tecnológico e falta de formação de dirigentes, eleitos, funcionários e voluntários e da inexistência de políticas de prevenção e resposta a incidentes. O elo mais fraco de uma cadeia de segurança é, normalmente, a pessoa que inadvertidamente deixa os atacantes aceder aos dados, e muitas vezes sem se aperceber disso. Considerando o aumento dos nossos eleitos locais e da criação de cada vez mais Núcleos Territoriais, e consequentemente, mais Grupos de Coordenação Local, é urgente garantir que os novos eleitos e dirigentes tenham formação de boas práticas digitais para evitar futuros incidentes.

A adoção de medidas como gestores de passwords, autenticação multifator, atualizações regulares, cópias de segurança, controle de acessos, formação contínua e monitorização dos riscos constitui uma abordagem proporcional e eficaz para reduzir a probabilidade e o impacto de incidentes de cibersegurança. Investir em segurança digital é fortalecer simultaneamente a componente tecnológica, os processos internos e a cultura organizacional do partido.

Neste contexto, torna-se importante que o LIVRE assuma um compromisso estratégico com a segurança digital dos seus órgãos internos, de forma evitar incidentes e fugas de informação. A presente moção procura precisamente incentivar este compromisso, estabelecendo uma orientação clara para a implementação de boas práticas e de uma política de cibersegurança sustentável e alinhada com os desafios atuais.

Deliberações

Considerando tudo o exposto, a presente moção propõe ao XVII Congresso do LIVRE mandatar os órgãos competentes do partido a:

1. Realizar, no prazo de 12 meses, uma avaliação à atual forma em que os atuais dirigentes, eleitos, funcionários e voluntários lidam com informações privilegiadas do partido e quais as atuais medidas de segurança implementadas, apresentando relatório ao próximo Congresso.

2. Realizar uma avaliação periódica dos riscos de cibersegurança e dos sistemas utilizados pelos vários órgãos do partido, requisitando auditorias aos Grupos de Coordenação Locais quando se justifique;
3. Implementar uma política de gestão de palavras-passes para gerir acessos às principais plataformas usadas pelos dirigentes, funcionários e eleitos do partido, como o email, o Action Network, o Canva, e as redes sociais, através do uso de uma plataforma centralizada com acesso restrito e baseado no princípio do menor privilégio;
4. Definir procedimentos claros para as transições de pasta em órgãos eleitos, locais e nacionais, para garantir que os acessos são atribuídos e removidos de forma organizada, atempada e segura;
5. Realizar ações de formação e sensibilização dirigidas a funcionários, dirigentes, eleitos e voluntários sobre cibersegurança, por exemplo: phishing, gestão segura de credenciais, autenticação multifator, proteção de dados, utilização segura do correio eletrónico e de ferramentas digitais, resposta a incidentes, prevenção de malware e ransomware e uso responsável de tecnologias emergentes, designadamente sistemas de inteligência artificial;
6. Definir um plano de resposta a incidentes de cibersegurança, com procedimentos claros para a comunicação, contenção, recuperação e análise pós-incidente, estabelecendo responsabilidades específicas, canais de reporte e mecanismos de coordenação que assegurem uma atuação célere e eficaz.

Proponentes

- Márcio Sousa
- Henrique Falcão

Subscritores

- Duarte Reis
- Matias Feijoo
- Sérgio Alves
- Sílvia Pais
- Lúcia Maria
- Tiago Domingues