PLANO DE AÇÃO DE MITIGAÇÃO DE RISCOS DA BOWE LTDA.

A **BOWE LTDA.** ("**BOWE**") é uma empresa comprometida com a proteção dos dados pessoais e preza pela conformidade com a Lei Geral de Proteção de Dados (LGPD) e normas editadas pela Autoridade Nacional de Proteção de Dados (ANPD).

O presente Plano de Ação de Mitigação de Riscos visa demonstrar à equipe do Ifood a existência de medidas efetivas para evitar riscos e a implementação de ações para as seguintes Recomendações:

> *Recomendações*
> *1. Enviar evidência de conscientização em segurança para informação para as pessoas que prestarão serviços para o iFood.*
> *2. Enviar evidência de gestão de criptografia para os devices que prestarão serviço para o iFood.*
> *3. Enviar evidência de gestão de ferramenta de antivírus/anti-malware utilizado nos computadores que prestarão serviços para o iFood.*
> *4. Enviar evidência do processo de gestão de vulnerabilidades para os computadores que prestarão serviços para o iFood.*

1. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

A **BOWE** se preocupa em conscientizar os seus colaboradores e prestadores de serviços por meio de treinamentos sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

Essa conscientização tem como objetivo trazer conhecimento para os colaboradores do impacto das suas tarefas diárias e o dever de proteger as informações que tiverem acesso por meio das suas atividades.

Por isso, foi realizado no dia 24 de abril de 2023 um treinamento sobre os conceitos básicos da Lei Geral de Proteção de Dados com uma especialista em privacidade com certificação em CIPP-E, conforme certificado anexo.

Ressaltamos que a Bowe tem em seu cronograma deste trimestre a realização de um treinamento em segurança da informação, com uma especialista em proteção de dados com certificação internacional PDPELGPD EXIN e CPPD que abordará os seguintes tópicos, tratando-se de orientações da Autoridade Nacional de Proteção de Dados:

- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;

• manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
• não compartilhar logins e senhas de acesso das estações de trabalho;
• bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
• seguir as orientações da política de segurança da informação.

Os colaboradores possuem uma Política Interna de Privacidade publicada que, em seu tópico 3 demonstra que, embora não sejam agentes de tratamento, possuem responsabilidade pelos dados e devem tratá-los de acordo com a lei e as políticas internas da empresa.

A **BOWE** também possui Política de Segurança da Informação publicada internamente e difundida pela sua equipe, na qual consta de forma expressa as medidas de segurança que devem ser aplicadas por todos, com o objetivo de manter os dados pessoais seguros.

A **BOWE** possui, ainda, um canal de comunicação aberto com a sua equipe para tirar dúvidas e dar orientações a qualquer tempo e está acompanhada de uma assessoria jurídica especializada em privacidade e proteção, o escritório NDM Advogados, desde 07/03/2018, auxiliando cotidianamente a empresa na aplicação das melhores práticas.

2. GESTÃO DE CRIPTOGRAFIA PARA DISPOSITIVOS

A **BOWE** aplica técnicas de criptografia nos dispositivos que prestam serviço para o iFood e realiza o gerenciamento desses dispositivos, garantindo que a criptografia esteja sempre ativa e seja periodicamente verificada. Para isso, todos os dispositivos devem ter a criptografia nativa do Windows ativada (BitLocker), o que protege os dados contra acessos não autorizados.

Todos os dispositivos que contêm dados dos clientes são manipulados dentro do Google Workspace, utilizando o Google Sheets, Google Docs e Google Apresentações, por se tratarem de serviços baseados em nuvem. Para armazenamento de dados, utilizamos o BigQuery do Google Cloud Platform. Em nosso relatório, são oferecidos os seguintes recursos de segurança:

Proteção por Criptografia

- **Criptografia em trânsito**: Todos os dados que trafegam entre os usuários e os servidores do Google são protegidos com HTTPS e TLS;
- **Criptografia em repouso**: Os dados armazenados nos servidores do Google são criptografados usando protocolos avançados, como AES-256. Dentro do BigQuery ainda contamos com Suporte a **chaves gerenciadas pelo cliente (Customer-Managed Encryption Keys - CMEK) B** e a tecnologia **Confidential Computing**, que protege os dados enquanto estão sendo processados no BigQuery.

3. GESTÃO DE FERRAMENTA DE ANTIVÍRUS/ANTI-MALWARE

Com o objetivo de prevenir acessos indevidos e incidentes de informação, em todos os dispositivos aplicáveis da **BOWE** são utilizados sistemas Antivírus, corretamente instalados e programados para serem executados em intervalos regulares.

Nesse sentido, o Windows Defender realiza varreduras automáticas diárias e manuais sempre que necessário. Os logs de varredura e relatórios de status são revisados trimestralmente pela equipe de Backoffice.

4. GESTÃO DE VULNERABILIDADES

A Gestão de Ameaças e Vulnerabilidades da **BOWE** emprega uma variedade de ferramentas e soluções para prevenir e lidar com ameaças cibernéticas.

Assim, a gerência de vulnerabilidade ocorre da seguinte forma:

a) Google Workspace

- **Análises automáticas de segurança**: O Google realiza varreduras regulares para detectar e corrigir vulnerabilidades em seus serviços.
- **Central de segurança**: O Google Workspace inclui ferramentas de monitoramento, como a Central de Segurança (Security Center), para detectar ameaças e vulnerabilidades em tempo real.
- **Admin Console**: Permite gerenciar dispositivos e controlar acessos, além de configurar políticas de segurança para minimizar riscos

b) BigQuery:

- **Detecção e Mitigação de Vulnerabilidades:** O GCP realiza análises regulares para detectar vulnerabilidades em sua infraestrutura e aplicar correções de segurança automaticamente;
- **Security Command Center:** Oferece uma visão unificada das configurações de segurança, permitindo identificar e corrigir vulnerabilidades ou configurações incorretas em serviços como o BigQuery;
- **IAM (Identity and Access Management):** Permite controlar quem tem acesso ao BigQuery e definir permissões granulares para proteger os dados de acessos não autorizados;
- **Proteção contra ameaças:** Inclui detecção de anomalias, proteção contra ataques DDoS, e ferramentas como Cloud Armor para proteger serviços baseados no BigQuery.

5. **CONCLUSÃO**

O presente Plano de Ação de Mitigação de Riscos visa demonstrar a conformidade da **BOWE** com as melhores práticas de segurança da informação. Em caso de dúvidas e novos esclarecimentos, permanecemos à disposição.

Uberlândia – MG, 28 de janeiro de 2025.

Bowe Ltda.