AVENIDA LUIS VIANA FILHO
WALL STREET EMPRESARIAL
SALA 606, TORRE A

(71) 2200-0665

TERMOS DE SEGURANÇA

Política de Segurança da Informação

Nossa Política de Segurança da Informação descreve as diretrizes aplicadas aos processos da empresa, sendo o principal guia para apoiar nossos colaboradores.

Para garantir que nossas diretrizes permaneçam alinhadas às demandas do mercado, atualizamos nossa Política de Proteção de Dados anualmente. Dentre os vários tópicos abordados na política, enfatizamos a Classificação de Dados, Avaliação de Riscos e Trabalho Remoto.

- **Prática de Segurança**

Buscamos referências nas melhores diretrizes internacionais de segurança da informação para fornecer produtos seguros aos nossos clientes. Essa proteção abrange desde a fase de concepção até o suporte diário de nossos produtos.

Os controles de segurança são aplicados com base nos 3 pilares da Segurança da Informação:

Confidencialidade: Garantir que apenas indivíduos autorizados tenham acesso às informações.

Integridade: Certificar-se de que as informações permaneçam completas e não sejam modificadas de maneira inadequada.

Disponibilidade: Assegurar que as informações estejam acessíveis sempre que requeridas.

Abaixo, listamos as principais práticas que aderimos internamente:

Nossa infraestrutura e aplicações passam por análises de vulnerabilidades recorrentes, contando também com atividades voltadas às correções necessárias conforme o nível de criticidade da vulnerabilidade identificada;

Anualmente, nossos produtos passam por um teste de penetração executada por consultorias independentes; realizamos análises nos códigos e bibliotecas a fim de identificar e corrigir possíveis vulnerabilidade durante o ciclo de desenvolvimento de software;

Negócios e segurança andam juntos, assim, aplicamos Security & Privacy by Design;

Nossa infraestrutura está atrás de tecnologias que fornecem proteção para o perímetro, tais como firewall, WAF, anti-DDoS e IPS.

- **Respostas a Incidentes**

Nós supervisionamos constantemente nosso ambiente e respondemos prontamente a possíveis incidentes.

Além disso, contamos com um procedimento formal que permite a qualquer funcionário relatar ao time responsável assim que identificar um incidente.

O processo de gestão de incidentes abrange desde a detecção e contenção inicial até a elaboração de relatórios e análise das lições aprendidas, implementando correções necessárias para evitar recorrências.

- **Continuidade de Negócio**

Contamos com estratégias para garantir a disponibilidade contínua e a rápida recuperação de nossos produtos em situações de desastre. Além disso, nossos ambientes são configurados com redundância para eliminar pontos únicos de falha (SPoF).

Nossa dedicação à disponibilidade dos produtos é detalhada em nosso Termo de Uso. Clique aqui para acessá-lo.

- **Gestão de Identidade e Acesso**

Na Hotmobile, adotamos metodologias como “least privilege” e “need to know” em todo o ciclo de vida dos acessos. Para conceder um acesso, é fundamental garantir que o solicitante tenha uma necessidade de negócio legítima, considerando a confidencialidade e integridade dos dados envolvidos.

Uma vez concedido o acesso, implementamos controles para verificar a identidade do usuário e a continuidade da necessidade de acesso. Utilizamos:

Multi fator de autenticação (MFA) para acessos internos, indo além do simples "algo que você sabe";

Revisões periódicas de acesso para revogar qualquer acesso desnecessário;

Gestão de acesso centralizada, garantindo que o acesso seja revogado imediatamente em casos de término de relacionamento com o usuário.

- **Uso Aceitável de Ativos**

Consideramos que disponibilizar um equipamento funcional e com os devidos controles de segurança implementados aos nossos colaboradores, auxilia na proteção das informações que podem ser acessadas. Desta forma, apenas equipamentos corporativos e em compliance devem ser utilizados para realizar as rotinas de negócio.

Abaixo, estão alguns dos controles implementados nos dispositivos:

Antivírus para monitorar e proteger os dispositivos contra ameaças;

Criptografia do disco para proteger as informações que possam ser armazenadas nos dispositivos;

Através do **DLP (Data Loss Prevention)** conseguimos monitorar e evitar possíveis compartilhamentos inadequados de informação;

Mesmo para colaboradores remotos, monitoramos a navegação na web e restringimos o acesso a sites inadequados por meio do controle de navegação **(CASB)**;

Além de tudo, todos os colaboradores da Hotmobile são orientados sobre as melhores práticas para o trabalho remoto, seguindo nossas políticas.

- **Qualificação de Segurança em Fornecedores**

Para minimizarmos os riscos que possam ser gerados por um fornecedor, conduzimos avaliações rigorosas durante o processo de contratação e realizamos revisões periódicas dos fornecedores que tenham acesso ao nosso ambiente. Nosso objetivo é selecionar parceiros que compartilhem nossos padrões de segurança.

- **Programa de Conscientização**

A segurança da informação e a proteção de dados são responsabilidades de todos os colaboradores, por isso, promovemos treinamentos e iniciativas contínuas sobre o tema. Além disso, oferecemos treinamentos especializados em desenvolvimento seguro para as equipes responsáveis por essa área.

Essa abordagem colaborativa garante que todas as áreas trabalhem juntas na proteção das informações de nossos clientes.

- **Privacidade de Dados**

Valorizamos a privacidade de nossos clientes e garantimos que o processamento de seus dados pessoais seja realizado em conformidade com as regulamentações pertinentes. Para mais informações, consulte nossa Política de Privacidade.