1. DECLARAÇÃO DA INTENÇÃO DA ALTA ADMINISTRAÇÃO

A Dotz afirma, por meio dessa política, seu comprometimento em assegurar a disponibilidade, a integridade e a confidencialidade das informações que lhe foram confiadas pelas partes interessadas, incluindo direção, empregados, investidores e outros parceiros de negócios. A alta direção da Dotz determina que todos os seus colaboradores atuem no sentido de impedir a ocorrência de problemas de segurança com as informações sob sua posse ou responsabilidade e contribuam para resultados de qualidade nos negócios através do respeito e cumprimento da sua Política de Segurança da Informação e demais normativos internos.

2. OBJETIVOS DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética (“Política”) da CBSM CIA BRASILEIRA DE SOLUÇÕES MARKETING S.A. (“DOTZ”) visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

3.1. Consideramos que os ativos de informação são os bens mais importantes no mercado varejista, portanto, trata-los com responsabilidade é o nosso compromisso. Dessa forma, estamos fundamentados nos princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques ou comportamentos cibernéticos.

3.1.1. **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

3.1.2. **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

3.1.3. **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

4. CLASSIFICAÇÃO DAS INFORMAÇÕES

4.1. Todas as informações de propriedade ou sob a custódia da Dotz deve ter um responsável principal para realizar a classificação de acordo com os requisitos e diretrizes corporativas. No ambiente Dotz as informações serão classificadas como:

- Confidenciais;
- Restritas;
- Internas e;
- Públicas.

As diretrizes sobre a correta classificação dos ativos e informações da Dotz devem seguir o padrão definido na Política de Classificação de Informações.

5. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O gerenciamento dos controles de segurança é de responsabilidade da área de Segurança da Informação da Dotz, e tem como objetivo assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política.

5.1. GESTÃO DE ACESSOS ÀS INFORMAÇÕES

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

O acesso às informações e aos ambientes tecnológicos da DOTZ devem ser permitidos apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração as práticas disseminadas pela equipe de Segurança da Informação e o princípio do menor privilégio e segregação de funções conflitantes.

5.2. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O comportamento de possíveis ataques é identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, antivírus, antispam, entre outros e correlacionado com métricas de casos de uso para comportamentos anômalos

5.2.1. Prevenção a Vazamento de Informações

A Dotz utiliza controles tecnológicos para prevenção de perda de dados, para garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados ou exfiltrados na web por usuários não autorizados.

5.2.2. Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

5.2.3. Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

5.2.4. Controle Contra Software Malicioso

Todos os ativos (computadores, servidores, etc.) que estejam conectados à rede corporativa ou façam uso de informações da DOTZ, devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela área de Segurança da Informação.

5.2.5. Criptografia

Toda solução de criptografia utilizada na DOTZ deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

5.2.6. Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

Autenticação de usuários (tentativas válidas e inválidas);

Acesso a informações;

Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

5.2.8. Desenvolvimento Seguro

A DOTZ mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

5.2.9. Cópias de Segurança (Backup)

O processo de execução de backups é realizado, periodicamente, nos ativos de informação da DOTZ, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes ou comprometimento do seu total ou parcial conteúdo.

6.CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

7. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A DOTZ avalia a maturidade em segurança da informação os parceiros com nuvens publicas ou privadas, caracterizando quais informações estão em compliance com a LGPD – Lei Geral de Proteção de Dados Pessoais.

8. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente aos nossos canais de atendimento.

9. TRANFERÊNCIA DAS INFORMAÇÕES

Toda transferência de informações, sejam em quaisquer meios possíveis, deverá ser controlada e de maneira programada visando garantir a proteção adequada.

10.DESCARTE DE EQUIPAMENTOS E DESTRUÇÃO DE INFORMAÇÕES

As mídias utilizadas na Dotz deverão ser descartada quando se tornarem desnecessárias. Com objetivo da proteção da informação sob tutela da Dotz, mecanismos seguros deverão ser utilizados para o descarte de equipamentos e informações.

11. GERENCIAMENTO DE MUDANÇAS

Modificações e aperfeiçoamentos dos sistemas de informação deverão ser administrados através do processo controlado de gerenciamento de mudanças.

12.TREINAMENTO E CONSCIENTIZAÇÃO

A DOTZ deverá fornecer aos seus colaboradores, por meio de um programa de disseminação da cultura de segurança, o conhecimento para garantir a segurança das informações.