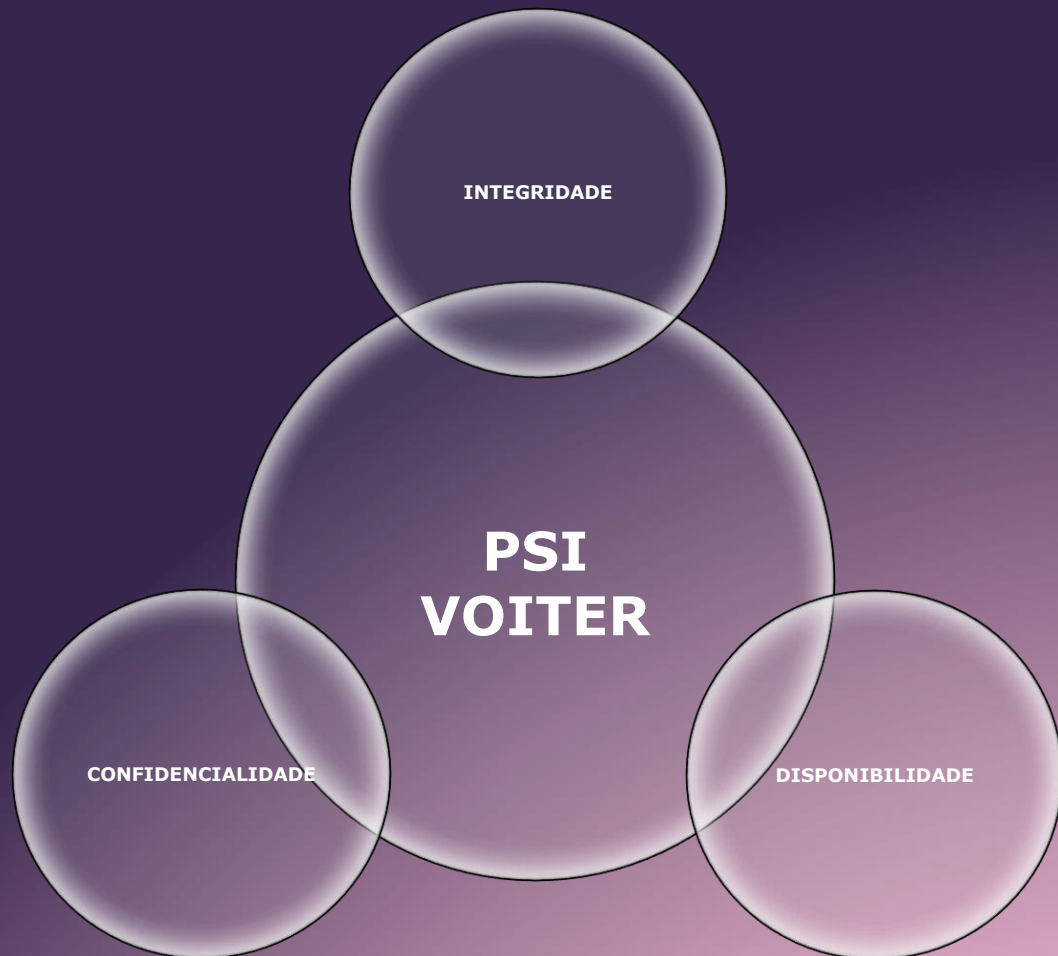


voiter



voiter

Área responsável: Segurança da Informação

Atualização: 28.03.2024



voiter

Sumário

1. Objetivo	4
2. Abrangência	4
3. Princípios	4
4. Diretrizes	4
5. Responsabilidades	5
6. Conformidade	6
7. Validade	6
8. Responsáveis	6



voiter

1. Objetivo

A Política de Segurança da Informação e Cibernética tem como propósito estabelecer diretrizes e normas de Segurança da Informação e Cibernética que permitam aos funcionários, prestadores de serviços, clientes, parceiros de negócios e fornecedores do Voiter S.A adotarem padrões de comportamento seguro, adequados às metas e necessidades da instituição.

A política é estabelecida como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e as normas nacionalmente e internacionalmente aceitas, com objetivo de garantir níveis adequados de proteção às informações da instituição ou sob sua responsabilidade.

2. Abrangência

Aplicável a todo Voiter.

3. Princípios

Os nossos princípios são:

- a) **Integridade:** garantir que as informações não serão modificadas ou comprometidas de qualquer forma.
- b) **Confidencialidade:** garantir que as informações serão acessadas somente por pessoas autorizadas.
- c) **Disponibilidade:** garantir que pessoas autorizadas tenham acesso à informação e ativos correspondentes, sempre que necessário.

4. Diretrizes

A fim de assegurar a confidencialidade, integridade e disponibilidade das informações da Instituição, mediante utilização de mecanismos de Segurança da Informação e Cibernética, balanceando fatores de risco, tecnologia e custo, alguma de nossas premissas são:



- a) Atender aos requisitos legais, aos regulamentares e às obrigações contratuais;
- b) Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas;
- c) Educar e conscientizar sobre Segurança da Informação;
- d) Tratar incidentes de Segurança da Informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
- e) Assegurar o comprometimento da Alta Administração com a melhoria contínua dos processos e recursos necessários para Segurança da Informação;
- f) Estabelecer conformidade, em caso de haver uma conduta não aderente ou descumprimento da Política, seja tomadas as medidas administrativas e/ou legais cabíveis;
- g) Seguir regulamentações no que se refere a serviços para processamento e armazenamento de dados e de computação na nuvem a fim de garantir as diretrizes mínimas de verificar a capacidade do prestador de serviço. Assim, assegurando o acesso aos ativos a serem processados ou armazenados, visando mitigar eventuais vulnerabilidades. Verificar, também, os controles físicos e lógicos oferecidos pelos prestadores de serviços;
- h) Garantir a continuidade dos negócios, com planos adequados que garantam o processo das operações e serviços providos pela Instituição.

5. Responsabilidades

Dentre as responsabilidades da nossa Área de Segurança da Informação, destaca-se:

- a) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;



- b) Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme os procedimentos estabelecidos pelo Voiter S.A;
- c) Assegurar que os controles adequados estejam disponíveis onde houver informações sensíveis;
- d) Administrar a Matriz de Segregação de Funções e realizar periodicamente a revisão de acessos, de modo a assegurar o acesso específico de determinadas informações para apenas aqueles que tenham relação com a atividade;
- e) Promover a divulgação desta política a todos os administradores, funcionários, prestadores de serviços, consultores e fornecedores, doravante denominados usuários.

6. Conformidade

Todos os ativos e sistemas de informação do Voiter S.A, assim como os seus funcionários, colaboradores e prestadores de serviço, devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecidos pela instituição. Uma 'não conformidade' advém de qualquer falha decorrente do não atendimento dos requisitos especificados nas documentações internas, regulamentações, contratos e outras obrigações dentro do Sistema de gestão da segurança da informação.

7. Validade

Um ano.

8. Responsáveis

Elaboração	Aprovação
Segurança da Informação	Conselho de Administração (28.03.2024)

