

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E PROTEÇÃO DA  
PRIVACIDADE VENTURA  
(SGSI - SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO)**

---

**VENTURA PETRÓLEO S.A.**

---

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

## Sumário

I.	Introdução .....	3
II.	Glossário .....	4
III.	Princípios da Segurança Cibernética .....	5
IV.	Objetivos da política de SGSI (Sistema de Gestão da Segurança da Informação).....	6
V.	Atualizações da Política .....	7

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY

## I. Introdução

A informação é um recurso fundamental para o desenvolvimento das atividades da Ventura Petróleo S.A. e, como tal, necessita ser protegida. Esta Política de segurança da informação, segurança cibernética e proteção da privacidade (“Política”) tem como objetivo estabelecer as regras, conceitos e orientações para a gestão do ambiente tecnológico seguro, compreendendo infraestrutura, sistemas, aplicativos, ativos de informação e segurança dos dados em meio digital ou físico, pelos integrantes ou parceiros da Ventura Petróleo S.A. no desenvolvimento de suas atividades de perfuração, avaliação, completação e workover de poços de petróleo e gás, utilizando redes de TO (Tecnologia Operacional) e de TI (Tecnologia da Informação), visando assegurar a segurança cibernética, bem como a confidencialidade, integridade, privacidade e disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política é uma declaração formal da Ventura Petróleo S.A. acerca de seu compromisso com a privacidade e a proteção das informações de sua propriedade e/ou sob sua guarda. Destina-se a todos os colaboradores da Ventura Petróleo S.A. e às empresas prestadoras de serviços, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. Esta Política deverá ser comunicada a todos os colaboradores da Ventura Petróleo S.A., visando assegurar que todas as pessoas tenham ciência da mesma e a pratiquem na empresa.

A Política está de acordo com as normas, leis, regulamentação e autorregulação aplicáveis, incluindo a Lei nº 13.709/18 – Lei Geral de Proteção de Dados (“LGPD”), as Normas INCITS/ISO 27.001:2022, INCITS/ISO 27.002:2022 e família IEC/TS 62443, bem como as boas práticas de mercado. Esta Política é o documento que estabelece as diretrizes corporativas para a proteção dos ativos de informação da Ventura. É aprovada pela Diretoria e divulgada pelo Comitê de Segurança da Informação (ou de Compliance) da Ventura. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

## II. Glossário

Ataque: tentativa não autorizada, bem-sucedida ou malsucedida, de destruir, alterar, desabilitar, obter acesso a um ativo de informação ou qualquer tentativa de expor, roubar ou fazer uso não autorizado de um ativo de informação.

Controles: definido como uma medida que modifica ou mantém o risco.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Evento de segurança da informação: ocorrência indicando uma possível violação de segurança da informação ou falha de controles.

Incidente cibernético: ocorrência que realmente ou potencialmente compromete a confidencialidade, integridade ou disponibilidade de um sistema de informação ou as informações que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitável.

Política: diretrizes, intenções e direção de uma organização, expressa formalmente pela Alta Direção.

Sistema de informação: conjunto de aplicações, serviços, ativos de tecnologia da informação ou outros componentes de manuseio de informações.

Violação de segurança da informação: comprometimento de segurança da informação que leva à destruição indesejada, perda, alteração, divulgação de, ou acesso a, informações protegidas transmitidas, armazenadas ou tratadas de diversas formas.

### III. Princípios da Segurança Cibernética

A utilização de informações para a realização das nossas atividades é imprescindível que seja seguido durante o ciclo de vida da informação, considerando os seguintes princípios fundamentais:

- **Confidencialidade:** garantir que a informação seja acessada somente por pessoas autorizadas.
- **Integridade:** garantir que a informação não seja alterada indevidamente durante seu ciclo de vida de forma a assegurar a integridade da informação, garantindo que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional.
- **Disponibilidade:** garantir que a informação esteja acessível sempre que necessário; diz respeito à garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades no momento que for requerida. Logo, a disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações.
- **Rastreabilidade:** garantir que os registros de transações relevantes sejam armazenados para que sejam consultados quando necessário.

CÓPIA NÃO CONTROLADA / NOT CONTROLLED COPY

#### IV. Objetivos da política de SGSI (Sistema de Gestão da Segurança da Informação)

A Ventura Petróleo S.A. adota para as suas atividades de perfuração, avaliação, completação e workover de poços de petróleo e gás, uma política segurança da informação, segurança cibernética e proteção da privacidade, alinhado com o nosso código de conduta ética e baseada em comprometimento e responsabilidade com a confidencialidade, integridade, privacidade e disponibilidade dos dados e dos ativos de informação utilizados na Ventura Petróleo S.A., estabelecendo os seguintes objetivos:

Elaborar, implantar e seguir a política, as normas e os procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes internas e externas.

Prover um ambiente digital seguro, protegendo as informações contra o mal-uso, modificações indevidas, destruição ou divulgação não autorizada, perda ou roubo através de práticas robustas de segurança cibernética, por meio do gerenciamento dos riscos cibernéticos de forma a prevenir, detectar e reduzir a probabilidade de incidentes.

Identificar, registrar e tratar integralmente incidentes de segurança cibernética e da informação, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às partes interessadas.

Implementar ações e medidas de controle necessárias para a melhoria contínua do sistema de gestão e segurança da informação.

Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos no seu sistema de gestão de segurança da informação.

## V. Atualizações da Política

Eventual revisão desta Política, desde que implique modificações substanciais, deverá ser comunicada as partes interessadas. De todo modo, recomendamos a consulta periódica aos termos desta Política que se manterão atualizados em conformidade com a legislação vigente e disponíveis no site da Empresa.

Macaé, 21 de dezembro de 2023.

Mardonildo Filho  
Diretor de Estratégia CSO

Mardonildo Filho  
Diretor de Estratégia

CÓPIA NÃO CONTROLADA / NON CONTROLLED COPY