## 1. INTRODUÇÃO

Esta Política estabelece as diretrizes de governança relacionadas à Segurança da Informação e de Cyber Segurança adotadas pela **MINASKRAFT,** visando a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), conforme orientações da norma ABNT NBR ISO/IEC 27001 e regulamentações aplicáveis. Tem como objetivo orientar os funcionários, os contratados e os prestadores de serviço da **MINASKRAFT** sobre suas responsabilidades, atribuições e ações necessárias na condução do SGSI e para reduzir ou mitigar riscos e assegurar a confidencialidade, a integridade e a disponibilidade das informações existentes ou geradas durante o desempenho de suas atribuições.

## 2. PÚBLICO ALVO

As disposições desta política aplicam-se:

- A todos os funcionários, estagiários e aprendizes, doravante denominados “colaboradores”;
- Às entidades e aos órgãos que possuam acesso às informações da **MINASKRAFT**;
- Aos prestadores de serviços, pessoas físicas ou jurídicas, que possuam acesso aos dados ou informações sensíveis necessários para a condução das atividades operacionais da organização.

.

## 3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

O processo de Segurança da Informação e de Cyber Segurança da **MINASKRAFT**, cujo objetivo é proteger as informações do negócio e clientes, é pautado pelos princípios fundamentais de:

- **Confidencialidade**: quando o acesso à informação deve ser disponibilizado apenas para as entidades ou pessoas devidamente autorizadas pelo proprietário ou dono da informação;
- **Integridade**: fato de manter a informação armazenada e trafegada com todas as suas características originais ao longo do seu ciclo de vida estabelecidas pelo proprietário ou dono da informação;
- **Disponibilidade:** garantir que a informação esteja disponível para uso sempre que entidades ou pessoas autorizadas necessitarem.

## 4. DIRETRIZES

As diretrizes estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados aos incidentes de segurança da informação e de Cyber Segurança.

### 4.1. INFORMAÇÃO

Importância e proteção Classificação da informação e Governança.

A informação é um importante ativo da **MINASKRAFT** e deve ser preservada e salvaguardada em conformidade com suas políticas, normas, procedimentos e controles, bem como, com as leis e regulamentos sobre o tema.

**Proteção de dados e privacidade**

A **MINASKRAFT** tem o compromisso de promover a aderência às leis de privacidade de dados e de proteção financeira de seus clientes, sendo este compromisso transmitido aos seus colaboradores, contratados e prestadores de serviço.

### 4.2. GESTÃO DE IDENTIDADES E DE ACESSOS

A gestão e revisão das identidades e dos acessos aos recursos computacionais da MINASKRAFT são realizados em conformidade com os requisitos descritos em Norma específica, garantindo a definição de:

- Recursos;
- Mínimos privilégios;
- Operações que podem ser executadas;
- Componentes autorizados; e
- Devida rastreabilidade de acessos realizados.

### 4.3. CONTROLE DOS DISPOSITIVOS DE TECNOLOGIA

Os recursos de tecnologia disponibilizados pela **MINASKRAFT** para uso dos funcionários são protegidos por controles contra-ataques cibernéticos, infecções e prevenção ao vazamento de dados.

### 4.4 DESENVOLVIMENTO DE SISTEMAS E GARANTIA DE QUALIDADE

A avaliação dos aspectos de segurança deve ser parte integrante no desenvolvimento de sistemas relevantes. Controles de segurança devem ser estabelecidos ao longo de toda a vida útil desses sistemas para assegurar que as informações processadas estejam protegidas, de acordo com sua classificação e exposição a risco.

### 4.5 SEGURANÇA E MONITORAMENTO DA INFRAESTRUTURA, REDES E SISTEMAS

As redes e sistemas corporativos relevantes devem ser administrados, monitorados e protegidos em consonância com as exigências e requisitos de Segurança da Informação da **MINASKRAFT.** Devem também ser protegidos contra acessos não autorizados por meio de tecnologias de rede devidamente atualizadas, revisadas e testadas periodicamente, de forma independente.

## 4.6. REGISTRO E RESPOSTAS DE INCIDENTES DE SEGURANÇA

Os incidentes de segurança da informação relevantes são registrados e destes decorrem a devida análise das referidas causas e impactos. No caso da ocorrência de incidentes relevantes, devem ser realizadas as avaliações de adequabilidade dos controles existentes e de necessidade de criação de novos controles, bem como, a contenção dos efeitos do incidente para as atividades da **MINASKRAFT**.

## 4.7. CONTINUIDADE DO NEGÓCIO E RECUPERAÇÃO DE INCIDENTES

O planejamento de continuidade do negócio é administrado de acordo com os requisitos estabelecidos na Política de Continuidade de Negócios e do Plano de Continuidade de Negócio de TI, que contempla cenários de incidentes relevantes a serem considerados nos testes de continuidade de negócios.

## 4.8. GESTÃO DOS PRESTADORES DE SERVIÇOS RELEVANTES

Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética destinados a assegurar que as informações tratadas pelos seus fornecedores estejam devidamente protegidas.

## 4.9. AVALIAÇÃO DE RISCOS DE PRODUTOS OU SERVIÇOS

Os riscos de segurança da informação devem ser avaliados e administrados de acordo com os requisitos definidos em Norma específica e nos controles de proteção. Após o registro e a análise devem ser executadas as respostas proporcionais aos riscos identificados.

## 4.10. BACKUP DE DADOS

A **MINASKRAFT** deve zelar pelo processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender aos requisitos operacionais e legais, assegurar a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação.

## 4.11. CONSCIENTIZAÇÃO DE COLABORADORES, CLIENTES E FORNECEDORES

A **MINASKRAFT** mantém um plano anual de conscientização direcionado ao desenvolvimento e à manutenção das habilidades dos funcionários em relação à segurança da informação.

# 5. VIOLAÇÃO DE SEGURANÇA

As violações das regras definidas nesta Política poderão ensejar a aplicação de medidas disciplinares, conforme determinam as normas internas e o Código de Conduta da **MINASKRAFT.**

A **MINASKRAFT** não tolera violações a esta política. Qualquer denúncia será tratada como assunto de extrema gravidade, e, em caso de apuração de qualquer violação à esta política, a **MINASKRAFT** adotará todas as medidas necessárias para sanar o problema.

## 6. CANAL DE TRANSPARÊNCIA

No caso de alertas de segurança, incidentes ou suspeitas sobre desvio de políticas, procedimentos e/ou regulamentações, as notificações devem ser enviadas para os canais de comunicação a seguir: compliance@minaskraft.com.br.

A suspeita de qualquer atividade realizada em desacordo com esta Política, ao Código de Ética, Conduta e Compliance ou ainda em desacordo com a legislação aplicável e vigente à época da atividade, deverá ser imediatamente informada no Canal de Transparência, em caráter totalmente sigiloso:

| TIPO | DESCRIÇÃO |
|---|---|
| **Site** | **https://www.minaskraft.com.br/Programa-de-Compliance/**<br>**compliance@minaskraft.com.br** |

A **MINASKRAFT** não tolera qualquer retaliação ao funcionário ou terceiro que, de boa-fé, utilizou o Canal de Transparência, procurou o Comitê de Ética, Conduta e Compliance, reportou ou se recusou a contribuir em qualquer atividade que violasse o presente procedimento.

## 7. NÃO RETALIAÇÃO

A **MINASKRAFT** não tolera qualquer retaliação ao funcionário ou terceiro que, de boa-fé, procurou conselho, reportou ou se recusou a contribuir em qualquer atividade que violasse o presente documento.

## 8. ALTERAÇÕES/REVISÕES

| Revisão | Vigência | Descrição da Alteração |
|---|---|---|
| 00 | 10/04/2023 | Publicação. |