



Política de Segurança Cibernética

Nós, da Creditas, buscando a excelência de nossos serviços nos preocupamos com a proteção de dados e informações relativas aos nossos Clientes, operações e sistemas internos. Neste sentido, tomamos precauções dentro dos mais altos padrões comerciais, a fim de garantir a segurança de tais dados e informações, respeitando, ainda as leis e normas aplicáveis às nossas atividades e adotando todos os padrões de segurança necessários.

A nossa Política de Segurança Cibernética apresenta como objetivo, de segurança da informação, a garantia de três pilares fundamentais:

- **Confidencialidade:** Garantia de que a informação somente estará acessível para pessoas autorizadas;
- **Integridade:** Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
- **Disponibilidade:** Garantia de que a informação deve ser disponível para usuários autorizados quando solicitado.

Com relação às medidas de segurança ainda temos os controles de: autenticação, criptografia, prevenção e a detecção de intrusão, e prevenção de vazamento de informações.

1. Nossa Política de Segurança Cibernética

- 1.1. A nossa Política foi especificamente estruturada em concordância com o nosso porte, perfil de risco e a complexidade dos nossos produtos e atividades. Esta é aplicável a nossos tripulantes e parceiros de negócios que façam uso e tenham acesso às informações Creditas.

2. Diretrizes Gerais de Segurança Cibernética

- 2.1. As informações são classificadas, manuseadas, tratadas e descartadas de acordo com sua criticidade e sensibilidade para o negócio e clientes, de forma que a segurança adequada seja aplicada, conforme os níveis abaixo:

- Confidencial
- Restrita;
- Interna;
- Pública.

Classificação do documento:

Confidencial

Restrito

Interno

Público

- 2.2. Mantemos um conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e serviços de processamento e armazenamento de dados e de computação em nuvem de ataques, danos ou acesso não autorizado.
- 2.3. Prevenimos, detectamos e reduzimos as vulnerabilidades e incidentes relacionados com o ambiente cibernético, utilizando registros de rastreabilidade da manipulação de dados da companhia e de nossos clientes.
- 2.4. A proteção dos dados é resguardada contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;
- 2.5. São realizados testes e varreduras periódicas para detecção de vulnerabilidades, e mecanismo de proteção contra softwares maliciosos.
- 2.6. Realizamos o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Creditas, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.
- 2.7. Visando garantir a continuidade de nossas atividades em caso de eventuais incidentes de segurança cibernética, realizamos, constantemente, testes de continuidade de negócios, nos seguintes cenários:
 - Condução de monitoramento e resposta de incidentes, seguindo as etapas de detecção, mitigação emergencial e análise de causa raiz;
 - Adoção de processo de gestão de continuidade de negócios relativo à segurança da informação e cibernética.
- 2.8. Disseminamos e promovemos a cultura de Cibersegurança corporativa através de uma plataforma de gamificação, que atende requisitos da LGPD, Prevenção à lavagem de dinheiro e combate ao crime cibernético.
- 2.9. Demonstramos também o nosso compromisso com os aspectos regulatórios, e as principais resoluções vigentes.
- 2.10. Nossa Política de Segurança Cibernética é revisada, no mínimo, anualmente.

Classificação do documento:

Confidencial

Restrito

Interno

Público