



POLÍTICA

Área responsável	SEGURANÇA DA INFORMAÇÃO
Data da Última Revisão	01/2025
Classificação da Informação	Público
Página	1/6

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ÍNDICE

1. Objetivo	2
2. Abrangência	2
3. Público Alvo	2
4. Regulamentação e Legislação	2
5. Definições	2
6. Diretrizes	3
7. Responsabilidades	5
7.1. Segurança da Informação	5
8. Disposições Gerais	6
9. Histórico	6

** Versão resumida para divulgação no website da instituição*

1. Objetivo

A Política de Segurança da Informação e Cibernética estabelece princípios para a garantia dos três pilares fundamentais em consonância com legislações e regulamentações vigentes:

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

2. Abrangência

Creditas Sociedade de Crédito Direto S.A.

3. Público Alvo

Tripulantes, terceiros, fornecedores e parceiros de negócio que façam uso e/ou tenham acesso às informações da Creditas.

4. Regulamentação e Legislação

Tipo	Emissor	Número	Ano	Assunto
Resolução	CMN	4.893	2021	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

5. Definições

5.1. Os termos desta Política terão o significado conforme abaixo:

- **Fornecedor:** Pessoa ou empresa que fornece algo ou presta algum tipo de serviço para a Creditas Sociedade de Crédito Direto;

- **Parceiro de Negócios:** Pessoa ou empresa profissional, que compartilha a propriedade da marca ou projeto da Creditas Sociedade de Crédito Direto. É um relacionamento legal, do ponto de vista das legislações, e deve ser cuidadosamente descrito para garantir que ambas as partes entendam suas obrigações financeiras e profissionais;
- **Terceiros:** Significa qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício da Creditas Sociedade de Crédito Direto, preste serviços ou forneça outros bens, assim como parceiros comerciais que prestem serviços à Creditas Sociedade de Crédito Direto, diretamente relacionados à obtenção, retenção ou facilitação de negócios, ou para a condução de assuntos da Creditas Sociedade de Crédito Direto, incluindo, sem limitação, quaisquer distribuidores, agentes, corretores, despachantes, intermediários, parceiros de cadeia de suprimento, consultores, revendedores, contratados e outros prestadores de serviços profissionais;
- **Tripulantes:** Todos os colaboradores da Creditas Sociedade de Crédito Direto, incluindo estagiários, jovens aprendizes e temporários;

6. Diretrizes

6.1. As informações são classificadas pela Creditas como “confidencial”, “interna” e/ou “pública”, e são manuseadas, tratadas e descartadas de acordo com a criticidade e sensibilidade para o negócio e clientes, de forma que a segurança adequada seja aplicada.

6.2. São mantidos 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 cibernéticos, danos ou acesso não autorizado.

6.3. As vulnerabilidades e incidentes de Segurança da Informação e Cibernética são prevenidos, detectados e tratados.

6.4. Os dados são protegidos contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas.

6.5. Periodicamente realizam-se testes e varreduras para detecção de vulnerabilidades, e mecanismo de proteção contra softwares maliciosos.

6.6. É feito a análise e o registro da causa e do impacto, bem como o controle dos efeitos de incidentes de Segurança da Informação e Cibernética para as atividades da Creditas, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

6.7. Visando garantir a continuidade das atividades da Creditas, em caso de eventuais incidentes de Segurança da Informação e Cibernética, são realizados, constantemente, testes de continuidade de negócios, considerando:

6.7.1. O monitoramento e resposta de incidentes, seguindo as etapas de detecção, mitigação emergencial e análise de causa raiz;

6.7.2. Adoção de processo de gestão de continuidade de negócios relativo à Segurança da Informação e Cibernética.

6.8. É disseminada e promovida a cultura de Segurança da Informação e Cibernética através de uma plataforma de treinamento, atendendo a requisitos de leis de proteção de dados, prevenção à lavagem de dinheiro e combate ao crime cibernético.

6.9. Todos os controles e procedimentos são implementados em conformidade com a Resolução CMN nº 4.893 de 2021 do Banco Central do Brasil.

6.10. Informamos aos clientes e usuários sobre precauções de Segurança da Informação e Cibernética na utilização de produtos e serviços financeiros.

7. Responsabilidades

7.1. Segurança da Informação

- Definir e implementar procedimentos para classificar as informações, garantindo que sejam manuseadas, tratadas e descartadas de acordo com a sua sensibilidade e criticidade;
- Proteger a infraestrutura de TI da Creditas, incluindo redes, computadores, sistemas e serviços de processamento e armazenamento de dados, contra ataques cibernéticos, danos ou acesso não autorizado;
- Prevenir, detectar e tratar vulnerabilidades e incidentes de Segurança da Informação e Cibernética;
- Proteger os dados contra acesso indevido, modificações, destruição ou divulgação não autorizada;
- Realizar testes e varreduras periódicas para detectar vulnerabilidades e garantir a eficácia dos mecanismos de proteção contra softwares maliciosos;
- Garantir a continuidade das atividades da Creditas em caso de incidentes de Segurança da Informação e Cibernética;
- Promover uma cultura de Segurança da Informação e Cibernética em toda a Creditas.

8. Disposições Gerais

8.1. Esta Política será válida por 2 (dois) anos, devendo ser atualizada sempre que forem identificados fatos que gerem impacto sobre as presentes disposições.

8.2. O descumprimento das disposições contidas nesta Política pode ocasionar a aplicação de medidas disciplinares ao infrator e aos demais que com ele colaborarem.

9. Histórico

CONTROLE DE ATUALIZAÇÕES				
Data	Versão	Elaboração	Alteração	Aprovação
12/2024	1.0	Segurança da Informação	Criação do documento	Diretoria SCD
02/2020	1.1	Segurança da Informação	Revisão do documento	Diretoria SCD
08/2020	1.2	Segurança da Informação	Revisão do documento	Diretoria SCD
04/2021	1.3	Segurança da Informação	Revisão do documento	Diretoria SCD
10/2021	1.4	Segurança da Informação	Revisão do documento	Diretoria SCD
11/2021	1.5	Segurança da Informação	Revisão do documento	Diretoria SCD
12/2022	1.6	Segurança da Informação	Revisão do documento	Diretoria SCD
04/2024	1.7	Segurança da Informação	Revisão do documento	Diretoria SCD
01/2025	1.8	Segurança da Informação	Revisão do documento Incluídos itens 6.9, alteração da marca	Diretoria SCD