BASF
We create chemistry

Política de Segurança Cibernética CrediBASF

Sumário

1. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO 3

2. PROCEDIMENTOS PARA PROTEÇÃO DA INFORMAÇÃO 3

3. PROCESSOS DE GERENCIAMENTO DOS RISCOS 5

Internal

Política de Segurança Cibernética

1. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança Cibernética foi elaborada em atendimento à Resolução nº 4.893 de 26 de fevereiro de 2021, publicada pelo Conselho Monetário Nacional, e estabelece os princípios e diretrizes que devem ser adotados pelos administradores, colaboradores e prestadores de serviços relevantes da Cooperativa de Economia e Crédito Mútuo do Grupo BASF - CrediBASF, com o objetivo de assegurar a proteção dos ativos de informação contra ameaças internas ou externas, visando reduzir a exposição a perdas ou danos decorrentes de falhas de segurança cibernética.

São princípios básicos da segurança da informação:

- **Confidencialidade**: Proteção da informação compartilhada contra acessos não autorizados.
- **Integridade**: Garantia da veracidade da informação.
- **Disponibilidade**: Prevenção contra as interrupções das operações da empresa como um todo.

2. PROCEDIMENTOS PARA PROTEÇÃO DA INFORMAÇÃO

Os procedimentos de segurança devem atender os seguintes componentes:

Internal

I. INFRAESTRUTURA

A CrediBASF é uma cooperativa financeira fechada aos colaboradores do Grupo BASF no Brasil e, por questões de eficiência e segurança, utiliza a infraestrutura do Grupo BASF, que possui governança de ponta, gerenciada pelo Framework Global de TI da BASF.

Para assegurar a continuidade dos negócios, a cooperativa também realiza periodicamente as seguintes ações:

- Restauração de cópia de segurança em QA;
- Due Diligence Infra da empresa mantenedora; e
- Controle de Incidentes.

a. Localização Atual dos Servidores e Banco de Dados

Os servidores e o banco de dados do sistema ERP utilizado pela CrediBASF estão atualmente alocados na Alemanha, em um datacenter de alta disponibilidade e segurança, contando com o monitoramento de performance e vulnerabilidades, com proteção antivírus e firewall quando abertos para ambiente externo.

b. Segurança Data Center

- Sistema de detecção e combate a incêndio
- Controle de acesso físico restrito
- Sala climatizada para garantir a estabilidade dos equipamentos
- Monitoramento 24x7, tanto lógico quanto físico
- Câmeras de segurança em pontos estratégicos

c. Backup

- Os backups dos servidores e do banco de dados são realizados diariamente
- Os dados são replicados em nuvem, garantindo alta disponibilidade, segurança e recuperação em caso de falhas
- O processo de backup é automatizado e segue políticas rígidas de retenção e recuperação

II. SISTEMAS

O fornecedor do sistema ERP e autoatendimento aos cooperados deve garantir o serviço de suporte à CrediBASF com regras de confidencialidade, conforme previsto no contrato de prestação de serviços, e uma vez aberto o chamado, o fornecedor diagnosticará o problema e elucidará as dúvidas conforme as especificações definidas pela CrediBASF, sempre considerando a prioridade de cada suporte.

III. OPERACIONAL

Todo componente da estrutura organizacional da cooperativa, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações desta política, normas e padrões de segurança cibernética. A disseminação da cultura de riscos e controles para os colaboradores tem sido importante pilar para subsidiar o melhor entendimento do assunto e o relevante papel desempenhado por cada integrante da equipe, já que fortalece a responsabilidade individual e coletiva em relação ao gerenciamento de riscos, em respeito à ética e à gestão dos negócios. Adicionalmente, a Matriz de Acessos aos sistemas foi implementada e é atualizada periodicamente ou conforme necessidade, pelo usuário master da instituição.

IV. USUÁRIOS

A CrediBASF sempre atuará em conjunto com os usuários, colaboradores da cooperativa, administradores de sistemas e infraestrutura, promovendo uma cultura de conscientização em que todos compreendam os riscos e adotem práticas seguras em suas ações. Para isso, a cooperativa disponibiliza em seu site dicas de como utilizar a ferramenta de autoatendimento de forma segura. Além disso, oferece aos usuários um login seguro com autenticação, utilizando o Enter ID da Microsoft, garantindo maior proteção e confiabilidade no acesso às informações.

3. PROCESSOS DE GERENCIAMENTO DOS RISCOS

Ambiente de Controle

O ambiente de controle influencia a consciência de controles e reflete o comprometimento de todos e, portanto, deve ser uma situação permanente e contínua.

CrediBASF

Contato

credibasf@basf.com

whatsApp (11) 99614 7663