

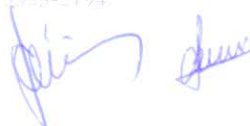
**POLÍTICA
SEGURANÇA
CIBERNÉTICA
2022**

**RESOLUÇÃO DO CMN
Nº 4.893/21**



SUMÁRIO

1.	INTRODUÇÃO.....	03
2.	OBJETIVO.....	03
3.	CONCEITO.....	03
4.	SEGURANÇA CIBERNÉTICA.....	06
5.	DIRETRIZES CORPORATIVAS.....	07
6.	IMPLEMENTAÇÃO.....	09
7.	TRATAMENTO DA INFORMAÇÃO.....	10
8.	PROCEDIMENTOS E CONTROLES.....	10
9.	PROCESSOS DE SEGURANÇA DA INFORMAÇÃO.....	11
10.	GERENCIAMENTO DE INCIDENTES.....	15
11.	EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM.....	18
12.	AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS.....	19
13.	COMUNICAÇÃO AO BANCO CENTRAL.....	20
14.	DOS CONTRATOS.....	21
15.	CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM.....	24
16.	PROCEDIMENTOS E INSTRUÇÕES.....	25
17.	ESTRUTURA DE GERENCIAMENTO.....	28
18.	GESTÃO DE ACESSO ÀS INFORMAÇÕES.....	28
19.	COMUNICAÇÃO AO CONSELHO DE ADMINISTRAÇÃO OU DIRETORIA.....	30
20.	DOCUMENTOS DISPONÍVEIS AO BANCO CENTRAL..	30
21.	ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO, E REVISÃO DA POLÍTICA.....	31
22.	CONSIDERAÇÕES FINAIS.....	32



1. INTRODUÇÃO

A informação representa um dos bens mais valiosos de uma organização, garantindo a continuidade dos negócios, minimizando os riscos de perdas financeiras e a imagem no mercado. Em muitos segmentos a informação possibilita novas oportunidades de negócio e agilidade no atendimento aos clientes.

A Resolução CMN nº 4.893/2021 dispõe sobre a Política de Segurança Cibernética e sobre os requisitos necessários para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, os quais deverão ser observados pela Cooperativa.

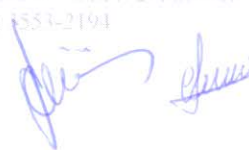
3

2. OBJETIVO

O objetivo desta política é orientar os colaboradores e definir os procedimentos e controles da COOPERATIVA em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação vigente. Destaca-se que além dos fornecedores de nuvem, os fornecedores de tecnologia da informação relevantes devem estar em conformidade com esta Política.

3. CONCEITO

Para melhor compreensão da necessidade de se cumprir o descrito na Política de Segurança Cibernética, é necessário conhecer os conceitos que fazem parte desse segmento, onde a informação é extremamente valiosa e passível de riscos que colocam em xeque a continuidade da



cooperativa. Dessa forma, temos os seguintes conceitos para facilitar o entendimento dos colaboradores:

Segurança Cibernética: refere-se a um conjunto de práticas adotadas pelas instituições, que protege a informação armazenada nos computadores, cujo fluxo se dá através de redes de comunicação em nuvem. Essa proteção visa garantir a propriedade da informação quanto a sua confidencialidade, integridade e disponibilidade.

Informação: é a reunião ou conjunto de dados e conhecimentos organizados, que possam constituir referências sobre determinado acontecimento ou processos comunicativos.

Confidencialidade: considera-se que, toda informação deve ser protegida, principalmente se considerado suas características e o grau de sigilo, de forma que exista limitação de acesso e uso apenas às pessoas autorizadas ou a quem é destinada.

Integridade: toda informação deve ser mantida na condição em que foi disponibilizada pelo seu titular, visando protegê-la contra alterações indevidas, intencionais e acidentais.

Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição, deve estar disponível aos seus usuários quando os mesmos necessitarem delas para qualquer finalidade.

Riscos Cibernéticos: são considerados ataques que as informações podem sofrer, oriundos de malware, invasões, fraudes externas, desprotegendo, inclusive, redes e sistemas das organizações, podendo causar danos financeiros, à reputação, e até mesmo colocar em risco a continuidade da instituição.

“MALWARE é um termo amplo que é usado para classificar todo tipo de



software malicioso usado para causar prejuízo, que pode ser até financeiro, danificar sistemas, interceptar dados ou simplesmente irritar o usuário, afetando tanto computadores como celulares e até redes inteiras”.

Vírus: software que causa danos à máquina, rede, softwares e banco de dados.

Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador.

Spyware: software malicioso para coletar e monitorar o uso de informações.

Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja restabelecido.

5

“**ENGENHARIA SOCIAL** é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados”.

Pharming: direciona o usuário para um site fraudulento, sem seu conhecimento.

Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável, que envia comunicação eletrônica oficial para obter informações confidenciais.

Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.

Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais.

