COCBAN
COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS BANCÁRIOS DE JF LTDA

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Resolução	4.893 de 26 de fevereiro de 2021
Diretor responsável indicado no Unicad	Katya Maria Chaves
Aprovada em reunião da Diretoria	28/03/2025

COCBAN
COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS BANCÁRIOS DE JF LTDA

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

ÍNDICE

1		Conceito	3
2		Estrutura Física	3
3		Regras de uso dos recursos de tecnologia	3
	3.1	Regras do uso do computador	4
	3.2	Internet	5
	3.3	Correio eletrônico	5
	3.4	Estação de trabalho	6
	3.5	Regras de uso do telefone	6
	3.6	Linhas gerais do comportamento seguro	6
4		Controles de Acessos	7
5		Segurança no Tratamento das Informações	7
6		Política de Backup	8
	6.1	Tipos de Backup	8
7		Propósito da Política de Segurança Cibernética	9
	7.1	Área gestora da Segurança Cibernética	9
	7.2	Razões, Ameaças e Riscos Cibernéticos	10
	7.3	Princípios	11
	7.4	Diretrizes para Segurança da Informação	11
8		Implementação	12
	8.1	Tratamento da Informação	12
	8.2	Objetivos da Política Cibernética	12
9		Procedimentos e Controles	13
10		Processos de Segurança da Informação	14
11		Aspectos da Segurança Cibernética que devem ser observados	17
12		Gerenciamento de Incidentes	19
13		Continuidade dos Negócios	21
14		Plano de Ação e de Respostas a Incidentes	22
15		Contratação de Clouds Services e Processamento/Armazenamento de Dados	22
16		Site Cocban	24
17		Gestão da Segurança Cibernética – Mapeamento	24
18		LGPD – Lei Geral Proteção de Dados	24
19		Considerações Finais/Recomendações na política	30

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

1 – CONCEITO

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 da empresa no mercado. Em muitos segmentos a informação possibilita novas oportunidades de negócio e agiliza o atendimento aos clientes de uma organização.

Pelo grau de importância que representa, a informação precisa ser adequadamente protegida. Para tanto, é preciso primeiramente levar em consideração as inúmeras formas nas quais a informação pode ser apresentada, como por exemplo, em papel, mídia eletrônica, e até mesmo falada. Além disso, a informação pode ser transmitida pelos mais variados meios, como armazenamento em nuvem, e-mails, documentos, arquivos, apresentações e até mesmo em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, deve-se protegê-la adequadamente.

A segurança da informação é baseada em três pilares: confidencialidade (garantia de que a informação é acessível somente por pessoas autorizadas), integridade (salvaguarda da exatidão e completude da informação) e disponibilidade (garantia de acesso à informação sempre que preciso).

A gestão da segurança da informação necessita do apoio e participação de todos os diretores que prestam serviço na Cocban, envolvendo também prestadores de serviço, fornecedores, parceiros e demais envolvidos.

Esta política tem como propósito promover uma base comum para as práticas efetivas de gestão de segurança e viabilizar a confiança nos relacionamentos entre a COCBAN e seus colaboradores.

Esta política tem por objetivo atender a resolução CMN 4.893/2021 que dispõe sobre a segurança cibernética e sobre os requisitos para contratação de serviços de processamentos e armazenamentos de dados e de computação em nuvem.

2 - ESTRUTURA FÍSICA

Atualmente a COCBAN possui 4 computadores e 1 notebook.

3- REGRAS DE USO DOS RECURSOS DE TECNOLOGIA

Os recursos tecnológicos que são de propriedade da cooperativa, são autorizados e disponibilizados exclusivamente para os usuários desempenharem suas funções a serviço da cooperativa.

A comunicação através dos recursos tecnológicos deve ser formal e profissional dentro da ética, de modo a preservar a imagem institucional da cooperativa.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Os conteúdos acessados e transmitidos através dos recursos de tecnologia devem ser legais, bem como a utilização de equipamentos e programas, de modo a contribuir para atividades profissionais dentro da ética.

O uso dos recursos de tecnologia, deverá ser submetido a testes periódicos pela Auditoria Interna, com pleno conhecimento e autorização da diretoria da cooperativa e em Conformidade com a Resolução Bacen 4.893/2021.

Cada usuário é responsável pelo uso dos recursos tecnológicos que lhe for confiado e autorizado, que estarão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas instalados, sendo vedado o uso de programas ilegais nos equipamentos.

Os recursos de tecnologia da cooperativa disponibilizados para os usuários, não podem ser repassados para terceiros, estranhos à cooperativa, salvo em caso de autorização expressa.

Qualquer anormalidade ou irregularidade nos recursos de tecnologia, devem ser comunicados de imediato aos superiores hierárquicos.

3.1 – Regras do uso do computador

Os computadores disponibilizados para os usuários são de propriedade da cooperativa, e devem ser utilizados com zelo e os cuidados necessários para assegurar seu pleno funcionamento dentro da vida útil estimada do equipamento.

A utilização dos equipamentos poderá implicar/exigir a utilização de senha específica e login de acesso, bem como limites de acesso, de modo a que se possa identificar a qualquer tempo, o usuário na realização de tarefas, pois a senha e o login serão assinatura digital do usuário.

É vedada a cessão de senha pelo usuário, sendo de sua inteira responsabilidade tal ocorrência, pois a mesma é pessoal e intransferível.

Os programas básicos, operacionais e aplicativos instalados nos computadores são de responsabilidade da cooperativa, cabendo ao usuário a sua correta utilização, desde que esteja capacitado para tal e em caso de necessidades, deverá encaminhar solicitação a superior hierárquico de novas configurações.

Bloqueios de acesso podem ser implantados como formas preventivas de incidentes, devendo o usuário estar sempre atento a atualizações de programas de proteção antivírus; tentativas de ataques; programas maliciosos e outras situações que possam redundar em incidentes.

O usuário deverá estar sempre atento a realizar cópias de segurança dos programas e arquivos, armazenando-as em local seguro e ao menos uma cópia fora das dependências da cooperativa.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

O usuário está ciente de que a instalação ou utilização de programas não autorizados, constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/1998, sujeitando os infratores a pena de detenção e multa.

A cooperativa não se responsabiliza por qualquer ação individual que esteja em desacordo com a lei mencionada, sendo considerada sua prática, uma ameaça à segurança da informação e será tratada com aplicação de ações disciplinares.

3.2 Internet

As regras visam basicamente o desenvolvimento de um comportamento ético e profissional na instituição.

O uso da internet para fins pessoais será permitido desde que não prejudique o andamento dos trabalhos nas unidades. Sites pornográficos, jogos, apostas e similares são proibidos.

É proibida a divulgação e/ou compartilhamento indevido de informações da área administrativa em WhatsApp, Instagram, Telegram, listas de discussões, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet.

Os colaboradores estão proibidos de realizar download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O uso de serviços tais como: mensagens instantâneas; uso de serviço de rádio, vídeos, músicas e correio eletrônico particular, poderão ser tolerados desde que não se confunda e nem prejudiquem os trabalhos da Cooperativa, situação que poderá não ser permitida e até proibida.

3.3 Correio eletrônico

O uso do correio eletrônico é para fins corporativos e relacionados a atividade do colaborador dentro da instituição. A utilização deste serviço para fins pessoais é permitida desde que seja feita com bom senso, que não prejudique a Cooperativa e também não atrapalhe o tráfego da rede.

No caso de endereço eletrônico individual para usuário, este é intransferível e pertence à cooperativa, sendo o mesmo enquanto permanecer o vínculo com a cooperativa.

O usuário que utiliza o endereço individual do correio eletrônico da cooperativa, é responsável por todo o acesso, conteúdo de mensagens e uso relativo ao seu e-mail, podendo enviar mensagens necessárias ao seu desempenho profissional e a sua atuação na cooperativa.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

O usuário deve estar ciente que o correio eletrônico da cooperativa deve ser utilizado para os serviços da instituição em todos os seus aspectos formais e profissionais, devendo abster-se de uso particular ou em benefício de terceiros não autorizados, salvo se previamente autorizado.

3.4 Estação de trabalho

Cada usuário possui sua própria estação de trabalho. Tudo o que venha a ser executado de sua estação, acarretará em responsabilidades do próprio.

Nenhum software/hardware poderá ser instalado sem autorização.

É proibido manter filmes, músicas, fotos pessoais na estação de trabalho.

É obrigatório que o usuário quando não estiver utilizando a estação efetue o Logoff na mesma.

3.5 Regras de uso do telefone

A cooperativa disponibiliza telefone fixo e celular para utilização dos diretores liberados para prestarem serviço na instituição, para atendimento ao quadro social e ao público em geral.

Os atendimentos devem ser formais e objetivos aos usuários e clientes, fornecedores e ao público em geral.

Os telefones poderão ser usados para recebimento ou chamadas particulares, mas sempre com objetividade de brevidade de modo que as linhas estejam prontamente liberadas.

O uso racional das linhas telefônicas pressupõe economia no custo mensal com telefone, devendo ser buscado e implementado por todos.

3.6 Linhas gerais do comportamento seguro

O acesso à cooperativa é vedado para aqueles que não são membros estatutários e/ou prestadores de serviço.

Os dados confidenciais não podem ser acessados de maneira alguma por quem não é permitido. O atendimento ao quadro social e ao público em geral, deve ser de forma separada, e de preferência, sem acesso ao local de trabalho da equipe.

Todo o lixo de informações confidenciais deve ser descartado utilizando a fragmentadora de papéis.

Os diretores liberados para prestarem serviço na cooperativa devem adotar um comportamento seguro quanto a não compartilhar e nem divulgar sua senha a terceiros; não transportar informações confidenciais sem o conhecimento e/ou devida autorização; não discutir assuntos confidenciais em ambiente público; abrir e-mails com mensagens de origem desconhecida ou suspeita; armazenar e proteger

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

adequadamente documentos impressos e arquivos eletrônicos com informações confidenciais, e por fim, seguir corretamente a política de segurança cibernética para uso da internet e correio eletrônico ou outras formas de comunicação.

4 - CONTROLE DE ACESSOS

O acesso ao computador possui senha, a qual está disponível para os diretores que prestam serviço na Cocban e ao Suporte TI.

O acesso ao sistema Sycoop32, possui senha exclusiva de acordo com cada perfil.

5 - SEGURANÇA NO TRATAMENTO DAS INFORMAÇÕES

Os arquivos referentes aos dados do Syscoop-32, estão armazenados em nuvem pelo Clouad.

Além do Backup (do software Syscoop-32) realizado semanalmente em máquina, também realizamos o backup mensal em mídia externa.

Os arquivos armazenados na estação, tais como: arquivos criados no Office, ou em formatos PDF, JPG, PNG e outros, são salvos mensalmente em mídia externa.

Existe cópia dos arquivos, fora das dependências da Cooperativa, em posse de um Diretor da Instituição que assinou o termo de responsabilidade de mídias externas.

TERMO DE RESPONSABILIDADE

Eu, xxxxxxxxxxxxxxxx, CPF XXXXXXXXXXXXXX. mediante este instrumento declaro responsabilizar-me pela conservação dos backups em PenDrive e HD de propriedade da COCBAN – Cooperativa de Economia e Crédito Mútuo dos Bancários de Juiz de Fora, inscrita no CNPJ 04.158.581/0001-45, para fins de armazenamento externo fora das dependências da Cooperativa, comprometendo-se a devolvê-los em perfeito estado e mantê-los atualizados.

Em caso de extravio e danos que acarretem a perda total ou parcial do bem, a cooperativa deverá ser informada imediatamente após o fato ocorrido.

Juiz de Fora, xx de xx de xx

xxxxxxxxxxxxxxxxxxxxxxxx

Diretor

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

6 – POLÍTICA DE BACKUPS COCBAN

Esta política de backup é um conjunto de diretrizes que define como, quando e onde os dados da Cocban serão copiados e armazenados.

O objetivo é garantir que os dados estejam disponíveis e inalterados em caso de falhas técnicas, ataques ou desastres naturais.

A política de backup é parte integrante da governança de TI e é um dos documentos-chave para minimizar os riscos e aumentar a produtividade dos usuários.

6.1 – Tipos de Backups:

I - Backup em Nuvem:

Frequência: Diariamente

Localização: Nuvem – Sistema Clouad Prodaf

Tipo de arquivos armazenados: Dados do Syscoop 32

Responsabilidade: Prodaf

Retenção: 07 dias

Segurança: Testes de verificação e recuperação realizados pela Prodaf

II – Backups realizados em mídias externas:

Frequência: Semanalmente

Localização: HD Externo

Tipo de arquivos armazenados: Pasta Modelos Cocban; Arquivos do Outlook; Windows Live Mail

Responsabilidade: GironSoft

Retenção: Cópia anual, 3 últimos meses, 8 últimas semanas.

Segurança: Testes de verificação e recuperação de dados são realizados trimestralmente pela Gironsoft. É emitido termo de recuperação de dados.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

TERMO DE RECUPERAÇÃO DE DADOS

Declaro para os devidos fins, que foram realizados testes de recuperação de dados nos arquivos descritos abaixo:

DATA ARQUIVO	LOCAL ARMAZENAMENTO	NOME ARQUIVO	RESULTADO

Juiz de Fora, _____/ _____/ _____

Daniel Giron Bernardo
GironSoft

7 - PRÓPOSITO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

O propósito desta Política é orientar a Cooperativa no que diz respeito a gestão de riscos e ao tratamento de incidentes de Segurança da Informação Cibernética, em conformidade com as disposições constitucionais, legais e regimentais vigentes, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da Cooperativa, dos cooperados e envolvidos, além disso, assegurar a proteção dos ativos de informação da cooperativa contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios.

7.1 - Área Gestora da Segurança Cibernética

A responsabilidade pela gestão desta política na Cocban é da Diretoria.

Cabe então:

a) Revisar e aprovar anualmente as políticas e estratégias de gerenciamento de Segurança Cibernética;

b) Assegurar a aderência de todos os envolvidos na Cooperativa, às políticas e as estratégias de gestão de Segurança Cibernética;

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

c) Assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de Segurança Cibernética;

d) Promover a disseminação da cultura de Gerenciamento de Segurança Cibernética.

Conforme art.7º resolução 4893 de 26/02/2021, foi designado no Unicad, Diretor Responsável pela Política de Segurança Cibernética e pela execução do plano de ação e respostas à incidentes.

Cabe ao Diretor Responsável pela Segurança Cibernética na Instituição:

a) Supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de Segurança Cibernética, incluindo seu aperfeiçoamento;

b) Subsidiar e participar do processo de tomadas de decisões estratégicas relacionadas ao gerenciamento de Segurança Cibernética, auxiliando a Diretoria;

c) Responsabilizar-se pela capacitação de todos os que compõem a estrutura de gerenciamento de Segurança Cibernética, acerca das políticas, dos planos e dos controles.

7.2 – Razões, Ameaças e Riscos Cibernéticos

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições,

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, competidores, etc) como por exemplo:

- Ganhos financeiros através de roubos, manipulação ou adulteração de informações;

- Obter vantagens competitivas e informações confidenciais de Clientes ou Instituições concorrentes;

- Fraudar, sabotar ou expor a Instituição invadida por motivos se vingança, ideias políticas ou sociais;

- Praticar o terror e disseminar o pânico e caos,

- Enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além disso riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Tanto instituições grandes como menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados, sendo também essa necessidade um dos motivos de implementação desta política.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;

- Conectividades como acesso à Internet, Banco Central, Receita Federal, etc..

- Informações sigilosas de cooperados;

- Componentes físicos como servidores, estações de trabalho, notebooks, etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central do Brasil, através da Res.4.893/21 já mencionada, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

7 .3 – Princípios

A segurança da informação é baseada em três pilares:

I – Confidencialidade: busca garantir que a informação é acessível somente por pessoas autorizadas;

II – Integridade: Salvaguarda da exatidão e completude da informação;

III- Disponibilidade: Garantia de acesso à informação sempre que preciso.

7.4 – Diretrizes para segurança da informação:

A Segurança da Informação da Cooperativa estabelece os principais controles, denominados diretrizes:

a) As informações da Cooperativa, dos cooperados e de todos os envolvidos devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) A informação deve ser utilizada de forma transparente e apenas para finalidade para a qual foi coletada.

c) Todo processo, durante o seu ciclo de vida deve garantir a segregação de funções, por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada por uma única pessoa.

d) O acesso às informações e recursos só deve ser feito se devidamente autorizado.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

e) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-a como responsável pelas ações realizadas.

f) A concessão de acessos deve obedecer a critérios de menor privilégio, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades.

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

h) Os riscos às informações da Cooperativa devem ser reportados à Diretoria que é responsável pela área de Segurança da Informação.

i) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes.

8- IMPLEMENTAÇÃO

A implementação desta política considera as seguintes compatibilidades da Cooperativa:

a) O porte, perfil de riscos e o modelo dos negócios;
b) A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais.
c) A sensibilidade dos dados e das informações sob responsabilidade da Instituição.

Os ambientes, sistemas, computadores e redes da Cooperativa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá todos os envolvidos com a Instituição conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não autorizadas, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

8.1 – Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Cooperativa em todos os seus ciclos de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

8.2 – Objetivos da Política de Cibernética

I – Assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) da Cooperativa;

II – Capacitar e gerir talentos humanos necessários à conduta ética e segura das atividades no âmbito tecnológico da Cooperativa;

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

III – Prover uma base comum para as práticas efetivas de gestão de segurança cibernética;

IV – Viabilizar a confiança nos relacionamentos entre a Cooperativa e seus cooperados.

9 - PROCEDIMENTOS E CONTROLES

No intuito de registrar procedimentos e controles para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos demais objetivos de Segurança Cibernética, e através disso prover controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, apresentamos a seguir as principais orientações para manter seu computador seguro:

I – Manter os softwares de detecção e proteção (anti-virus), atualizados, capazes de proteger eficientemente o ambiente corporativo;

II – Manter atualizados os softwares e aplicativos de uso na rede;

III-Somente instale programas legítimos de fontes confiáveis;

IV –Não abra e-mails de arquivos enviados de fontes desconhecidas;

V – Ao compartilhar recursos de seu computador, estabeleça senhas para os compartilhamentos e permissões de acesso adequadas;

VI- Fique atento aos endereços acessados no seu navegador;

VII – Ao realizar compras pela internet procure por sites reconhecidamente seguros;

VIII – Na utilização de internet banking procure pelos sinais de segurança;

IX – Troque suas senhas com frequência, ela é pessoal e intransferível, e, criada de acordo com as funções permitidas para o exercício das suas atividades;

X – A maioria das redes sem fio usa algum tipo de configurações de segurança. Essas configurações de segurança definem a autenticação (como o dispositivo se identifica para a rede) e a criptografia (como os dados são criptografados à medida que são enviados através da rede). Procure sempre acessar redes seguras;

XI – Ao detectar algum erro é importante que seja rastreado, através de tecnologias disponíveis todo o caminho do processo, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou;

XII – Realize backup diariamente de todos os seus sistemas.

Ressaltamos que a simples aplicação destas recomendações auxilia, porém não garante a segurança da informação, orientamos que no caso de dúvidas, não seja executado nenhum procedimento sem o conhecimento e orientação de pessoas regularmente habilitadas para sanar quaisquer dúvidas e executar procedimentos de segurança.

Os procedimentos acima descritos buscam abranger no mínimo a autenticação, criptografia, prevenção, detecção e possíveis vazamentos de informação, a realização periódica de testes e varreduras para detecção de vulnerabilidade, bem como a proteção contra software maliciosos, e o estabelecimento

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

de mecanismos de rastreabilidade. Busca prover ainda, o controle de acesso e segmentação da rede, a manutenção de cópias de segurança dos dados e das informações e o desenvolvimento de sistemas seguros

Além das informações acima, a Diretoria aprovou a elaboração do Plano de Ação de Segurança Cibernética e o Monitoramento de Riscos para acompanhamento periódico.

10 - PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Cocban adota os seguintes processos:

a) Gestão de ativos da informação.

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

c) Gestão de acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Cooperativa.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o usuário do computador, para que seja devidamente responsabilizado por suas ações.

d) Gestão de riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos da informação da Cooperativa, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

e) Mitigação dos Riscos:

A Cooperativa oferece uma completa estrutura tecnológica para o exercício de suas atividades, sendo responsabilidade de cada Diretor liberado para prestar serviço na cooperativa manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, Notebook, Smartfone, Acesso à Internet, e-mail etc.)

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Equipamentos e computadores disponibilizados pela Cocban devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Cooperativa.

A instalação de cópias de arquivos de qualquer extensão, obtida de forma gratuita ou remunerada, em computadores da Cooperativa depende da autorização do Diretor Responsável pela Política de Segurança Cibernética devendo o mesmo observar os direitos de propriedade intelectual pertinentes, tais como: copyright, licenças e patentes.

As mensagens enviadas ou recebidas através de correio eletrônico (e-mails corporativos), seus respectivos anexos, e a navegação através da Internet em equipamentos da Cooperativa poderão ser monitoradas.

As senhas de acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. O usuário do computador/equipamento poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe foram designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos, como em Word ou Excel, compreensíveis por linguagem humana (Não criptografados).

Não devem ser baseadas em informações pessoais (data de nascimento, nome próprio e de familiares, placa carro, etc.), também não devem ter combinações obvias de teclado como (abcde, 12345.)

As senhas para maior segurança devem conter: Letras maiúsculas e minúsculas, números e caracteres.

Os usuários podem alterar a própria senha e devem ser orientados à fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

f) Tratamentos de incidentes de Segurança da Informação e Cyber Security

Incidentes são interrupções de sistema não planejadas que ocorrem de várias maneiras e que afetam os negócios da Cooperativa, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão;
- Servidor fora do ar;
- Ausência de conexão com a Internet;
- Sabotagem/Terrorismo;
- Indisponibilidade de acesso à Cooperativa.

Os incidentes de Segurança da Informação e cibernéticos da Cooperativa devem ser reportados ao Diretor Responsável pela Política Cibernética da Instituição imediatamente após sua detecção.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

g) Conscientização em Segurança da Informação e Cyber Security

A Cooperativa promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

h) Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

i) Programa Cyber Security

O programa de Cyber Security da Cooperativa é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores Práticas;
- Cenário Mundial.

j) Controle de prestadores de serviço que manuseiam dados ou informações sensíveis

Os prestadores de serviços que detenham informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Cooperativa, deverão ser tecnicamente treinados e extremamente envolvidos com as atividades da cooperativa de forma íntegra e profissional.

Os mesmos estão cientes que poderão ser responsabilizados por qualquer dano ou vazamento de informações de acordo com o contrato de prestação de serviços e políticas internas da Cooperativa.

O acesso a qualquer informação deverá ser solicitado formalmente.

k) Melhoria Contínua de Procedimentos:

A Diretoria é responsável pela melhoria contínua dos procedimentos relacionados com a Segurança Cibernética, e além do controle em ata de reunião da Diretoria, o assunto deverá ser pauta dos relatórios anuais da Instituição.

Conforme criticidade, o programa divide-se hein:

AÇÕES CRÍTICAS: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;

AÇÕES DE SUSTENTAÇÃO: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o nível de risco da Cooperativa e permitindo que ações estruturantes de longo prazo possam ser realizadas;

AÇÕES ESTRUTURANTES: Iniciativas de médio/longo prazo que tratam a raiz dos riscos e que preparam a Cooperativa para o futuro.

AÇÕES DE PREVENÇÃO: Consideramos principais ações de proteção para manter o bom funcionamento e a efetividade da Segurança Cibernética da Cooperativa:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Exemplo: Softwares não licenciados ou piratas.

- Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

- Monitorar rotinas de backup, executando testes regulares de restauração dos dados;

- Realizar periodicamente testes de invasão externa e phising;

- Realizar análises de vulnerabilidades na estrutura tecnológica periodicamente ou sempre que houverem mudanças significativas em tal estrutura.

11 – ASPECTOS DA SEGURANÇA CIBERNÉTICA QUE DEVEM SER OBSERVADOS

Conforme está previsto na resolução 4.893/2021, devem ser previstos diversos aspectos da segurança cibernética que irão nortear esta política:

I - Objetivos da Segurança Cibernética: Assegurar a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados.

Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, res. 4.893, deve ser contemplada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

II - Procedimentos e os controles adotados para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos objetivos da segurança cibernética: Esses procedimentos requerem controles, como os níveis de acesso às informações, a contínua vigilância e principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamento de dados.

III – Controles específicos que busquem garantir a segurança das informações sensíveis, incluindo os voltados para a rastreabilidade da informação: Esses procedimentos requerem a utilização de equipamentos e programas confiáveis, com a utilização de programas antivírus adequados e capazes de assegurar a confiabilidade da proteção, aliado a uma manutenção preventiva e constante dessas ferramentas. O armazenamento em nuvem deverá ser adotado como princípio de segurança confiável.

IV – O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição: Deve-se estar atento às tentativas de ataques cibernéticos, bem como as apurações em casos de incidentes relevantes ou não, pois qualquer ocorrência demonstrará falhas nas defesas ou prevenções, devendo ser debatidas as ocorrências nos diversos níveis operacionais da cooperativa, buscando aprimorar os mecanismos preventivos.

V- As diretrizes para:

a) A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios: Deve-se levar em consideração cenários que possam abalar os negócios causando interrupções danosas às operações; acesso e roubos de informações confidenciais; acesso e roubos nas contas de depósitos da

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Cooperativa; destruição de arquivos e bancos de dados; bloqueio de acessos com a liberação mediante resgates criminosos, entre outros.

b) A definição de procedimentos e de controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços, a terceiros que manuseiam dados ou informações sensíveis ou que seja relevantes para a condução das atividades operacionais da Cooperativa: Trata-se de uma parte extremamente relevante na política de segurança cibernética, pois a relação da cooperativa e as empresas prestadoras desses serviços deve estar estruturada além da sua capacitação técnica, na confiabilidade recíproca conquistada em anos de relacionamento. Juridicamente deve estar ancorada em contrato, que seja considerado um ato jurídico perfeito, com cláusulas pétreas e preventivas de segurança, além dos aspectos técnicos sobre os serviços contratados e outros, devendo ser revisto periodicamente para atualizações, aperfeiçoando essa relação com uma segurança jurídica garantidora da prestação dos serviços.

c) A classificação dos dados e das informações quanto a relevância: A Cooperativa como instituição financeira, opera com informações protegidas por sigilo de acordo com a Legislação em Vigor (Lei Complementar 105/2001), que relaciona essas operações cuja violação é passível de penalizações. Essas operações elencadas terão tratamento prioritário na classificação de dados na política de segurança cibernética tanto pela relevância, quanto pela penalização imposta por sua violação. O seu manuseio e acesso pelas pessoas, que por dever de ofício tem autorização para fazê-lo, deverão ser cientificadas quanto a violações. Outros tipos de dados e informações poderão ter classificação mais abrandada nas atividades da cooperativa.

d) A definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes: Como está evidenciado no item "c" anterior, os parâmetros levarão em consideração em primeiro lugar, as informações previstas na Lei Complementar 105/2001 e que a cooperativa por sua classificação está autorizada a operar. Atendida essa relevância, as demais informações serão avaliadas por outros critérios, dentro das relevâncias julgadas pertinentes.

VI – Os mecanismos de disseminação da cultura de segurança cibernética na cooperativa incluindo:

a) A implementação de programas de capacitação e de avaliação periódica de pessoal: Dentro dos programas de treinamento e capacitação de membros estatutários e colaboradores, a cooperativa incluirá a segurança cibernética como programa de capacitação, bem como avaliação do pessoal.

b) A prestação de informações a clientes e usuários sobre precaução na utilização de produtos e serviços financeiros: Essa é uma parte sensível no relacionamento cooperativa e seus associados, pois a cooperativa não pode negligenciar nas orientações e precauções na utilização desses serviços. Os colaboradores serão orientados sempre na prestação dos atendimentos e as informações e orientações no trato desses serviços, que são protegidos pelo sigilo previstos na Lei complementar 105/2001.

c) O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética: A diretoria da cooperativa deverá ter comprometimento prioritário com a segurança cibernética, pois além de ter um diretor indicado responsável pela segurança,

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

deverá estar atualizada no que ocorre na área de segurança cibernética, atuando preventivamente, cobrando informações e providências diuturnas.

VII – As iniciativas para compartilhamento de informações sobre incidentes relevantes mencionados no inciso IV, com outras cooperativas de crédito: Trata-se de uma prática que não é comum, mas que deve ser buscada em função de que diversos incidentes são comuns tendo como origem fontes idênticas e o mesmo "modus operandi". Uma das formas seria através das empresas de informática contratadas que prestam serviços a diversas cooperativas e serviriam de elo de compartilhamento de incidentes, que para tanto, deveriam ser autorizadas a divulgarem incidentes ocorridos para ações preventivas.

CONSIDERAÇÕES COMPLEMENTARES SOBRE OS INCISOS CITADOS ANTERIORMENTE:

Inciso I – Deverá ser contemplada a capacidade da cooperativa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, situação esta, que está ligada aos operadores do sistema de informática (equipamentos e programas), com sistemas adequados de detecção.

Inciso II – Os procedimentos e controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção da vulnerabilidade, a proteção contra programas maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, devendo também ser aplicado no desenvolvimento ou contratação de sistemas de informação seguros e na adoção de novas tecnologias empregadas na atividade cooperativa.

Inciso III – O registro, a análise da causa, o impacto, bem como o controle dos efeitos de incidentes devem abranger inclusive informações recebidas das empresas de prestação de serviços de informática contratadas.

Inciso IV – As diretrizes devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão, compatíveis com os utilizados pela cooperativa.

12- GERENCIAMENTO DE INCIDENTES

O Gerenciamento de Incidentes, tem o objetivo de assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de Informação da Cooperativa.

O procedimento padronizado para o tratamento de incidentes de segurança compreende as seguintes etapas:

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

I – Recepção da denúncia ou notificação interna de atividade suspeita: serão aceitas denúncias e a Cooperativa colaborará plenamente com a polícia e entidades legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede da Cocban, e serão investigados os alertas provenientes dos sistemas de monitoramento da rede, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com os procedimentos éticos de padrões estabelecidos.

II - Medidas de contenção imediatas ao incidente: a contenção imediata ocorrerá por meio de bloqueio de acesso ao host envolvido à rede até o término da investigação.

III – Coleta de Informações e evidências: Serão coletadas informações e evidências sobre as atividades denunciadas através dos logs dos diversos sistemas e serviços disponíveis na rede da Cooperativa.

IV – Análise de informações e evidências: Todas as informações e evidências serão analisadas para investigar o host que gerou o incidente denunciado. A identificação do host compreenderá a determinação do seu endereço de IP e endereço MAC da interface de rede, nome, switch, porta de acesso, usuário e todas as outras informações possíveis.

O tipo de atividade será determinado pelas informações evidenciadas em logs de serviço. As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

V – Notificação dos envolvidos: Será encaminhada notificação por escrito da atividade denunciada ou sob investigação à direção da Cooperativa. Cabe ao responsável pelos usuários da máquina alvo de investigação a determinação da origem da atividade, com sua adequada comprovação.

Como origem das atividades pode considerar:

a) Atividade realizada pelo usuário;
b) Atividade realizada por terceiro com autorização do usuário;
c) Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Como evidência da origem da atividade pode-se considerar:

a) Logs de acesso local ou remoto na máquina;
b) Logs de detecção de vírus, spyware, malware, etc.
c) Outras informações que possam identificar claramente a origem da atividade.

VI – Análise crítica e medidas corretivas: A Diretoria notificada com auxílio do responsável pela tecnologia da Cocban avaliará a resposta e determinará as medidas corretivas no host identificado. Nos casos comprovados de invasão e de atividades maliciosas por parte do usuário, o host permanecerá bloqueado até a implantação das medidas corretivas apresentadas.

Qualquer reclamação em relação à utilização ilícita ou questões de segurança do sistema ou da rede, uso indevido de correio eletrônico, violação de direitos autorais ou qualquer atividade em desacordo com a política devem ser enviadas para o e-mail oficial da Cocban, com a devida comprovação da atividade.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

A Diretoria será responsável pela avaliação da melhor forma de compartilhamento das informações sobre incidentes relevantes ora identificados. Tal decisão deverá ser analisada em reunião do Conselho e descrita em ata do mesmo.

Avaliação Inicial: Avaliar o incidente para verificar se é provável sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.

Analisar motivos e consequências imediatas, bem como a gravidade da situação.

Incidente Caracterizado: Deverão ser tomadas medidas imediatas como:

- O Diretor Responsável pela Segurança Cibernética avaliará o impacto do incidente nos diversos riscos envolvidos;

- Conforme relevância (sabotagem, terrorismo, etc..) poderá ser registrado um boletim de ocorrência ou queixa crime para que sejam tomadas as devidas providências;

- Conforme a relevância do incidente comunicar aos cooperados que por ventura tenham sido afetados;

- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções relevantes, que configurem uma situação de crise pela cooperativa.

Recuperação: Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chaves notificados.

Quaisquer dados que estejam faltando ou corrompidos, ou problemas detectados internamente deverão ser comunicados a Diretoria.

Retomada: Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais medidas de prevenção.

13 – CONTINUIDADE DOS NEGÓCIOS

A Cooperativa COCBAN procurará investigar os eventos e incidentes de forma a não influenciar a continuidade dos negócios, principalmente no caso de ocorrer interrupção de serviços relevantes, primando assim pela execução normal das atividades da instituição o mais breve possível, de forma que a interrupção não ultrapasse 24 (vinte e quatro) horas.

Alguns cenários de incidentes que podem influenciar a continuidade dos negócios são: vazamento de dados/informações, indisponibilidade de recursos computacionais, quebra da integridade dos dados, via

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados, fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição.

A Cooperativa COCBAN deverá fazer comunicação ao Banco Central dos procedimentos adotados para continuidade dos negócios em caso de ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que venha a afetar o funcionamento normal de suas atividades que configurem uma situação de crise pela instituição financeira.

14 – PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A Cooperativa estabelecerá Plano de Ação e de Resposta a Incidentes que é parte integrante da Política de Segurança Cibernética:

Este plano abrangerá:

1) – Ações a serem desenvolvidas pela cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes de segurança cibernética previstas.

2) – As rotinas, os procedimentos, os controles e as tecnologias que serão utilizadas na prevenção e na resposta de incidentes, em conformidade com as diretrizes da política de segurança prevista.

3) – A área responsável pelo registro e controle dos efeitos de incidentes relevantes, estará sob a responsabilidade do diretor responsável designado pela Política de Segurança Cibernética, a ser informado ao Bacen através do Unicad.

O plano de ação e respostas a incidentes deverá ser aprovado pela Diretoria e revisado anualmente.

15 - CONTRATAÇÃO DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

As instituições referidas no art. 1º, da Res. 4.893/2021, devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior.

Conforme, art. 12 as instituições mencionadas no art. 1º, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

II - a verificação da capacidade do potencial prestador de serviço de assegurar:

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Conforme Art. 15 da Res.4893/2021, a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições referidas no art. 1º ao Banco Central do Brasil.

§ 1º A comunicação mencionada no caput deve conter as seguintes informações:

I - a denominação da empresa contratada;

II - os serviços relevantes contratados;

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

§ 2º A comunicação de que trata o caput deve ser realizada até dez dias após a contratação dos serviços.

§ 3º As alterações contratuais que impliquem modificação das informações de que trata o § 1º devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Em agosto/2024 a Cocban realizou a contratação dos serviços em nuvem pela Prodaf, aderindo ao Clouad.

Junto ao Clouad, foram adquiridas também licenças para o Syscoop Web e Syscoop APP. Ambos de propriedade da Fischer Informática Ltda (Prodaf).

Foi feita a comunicação ao Bacen, conforme ofício 17.128/2024.

16 – SITE COCBAN

A Cocban possui site www.cocban.com.br que está de acordo com todas as normas da LGPD e possui Política de Privacidade, Termo de Uso e Política de Confiabilidade e Segurança dos Dados.

17 – GESTÃO DA SEGURANÇA CIBERNÉTICA - MAPEAMENTO

A Cocban possui mapeamento mensal de todas as avaliações e acompanhamentos que são realizados pela equipe para fins de manter o gerenciamento do ambiente cibernético, com base no porte e complexidade da Cooperativa.

GESTÃO DE SEGURANÇA CIBERNÉTICA											
RES.4893/21											
	Controle de Acesso			Segurança e Tratamento da Informação						Melhoria Contínua	
Identificação	Syscoop	Rede Interna	Senha de Arquivos relevantes	Backup Syscoop (Mídia Externa)	Backup Arquivos Office e PDF/JPG/ Outros	Software de Proteção (atualização por máquina)	Software de aplicativos e uso na rede (atualização por máquina)	Firewall de proteção e tráfico de dados (por máquina)	Controle de acesso remoto / Prestadores de Serviços	Tratamento de Incidentes	Necessidade de Investimentos
Verificação	Troca de senha a cada 120 dias			Quinzenal	Quinzenal	Mensal / Sempre que necessário			Quando necessário	Mensal	Mensal
Responsável	Diretor Resp. Res.4893			Diretor Resp. Res.4893		Gironsoft			Diretor Resp.Res.4893	Diretoria	
Verificação Mensal											

18 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Base regulatória:

É a lei nº 13.709 de 14/08/2018 que regulamenta o tratamento de dados pessoais realizado por pessoas físicas ou jurídicas no Brasil, tanto por meios físicos quanto digitais.

Qual a abrangência e para que ela serve?

Tem aplicação em todo território nacional e determina as regras para coleta, armazenamento, processamento e compartilhamento de dados pessoais. Serve portanto, para proteger o usuário do uso abusivo e indiscriminado dos seus dados por parte de instituições – públicas ou privadas.

Quando começou a vigorar?

Entrou em vigor na data de 18 de setembro de 2020.

Qual a sua importância?

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Hoje vivemos em meio a uma sociedade hiperconectada, que gera e movimenta uma quantidade enorme de dados pessoais, que são armazenados em diversas plataformas online no mundo todo.

A lei confere ao titular dos dados o poder de controla-los. É dele a decisão de quais dados ele quer divulgar.

A lei coíbe possíveis abusos com frequentes casos de vazamentos de dados e penaliza o uso impróprio dos mesmos, além disso, também resguarda a privacidade da população, estabelecendo parâmetros, direitos e obrigações, conferindo mais transparência e responsabilidade no uso e tratamento de dados.

Em quais situações a Lei é aplicada?

Em quaisquer cidadãos, instituições ou empresas, de direito público ou privado, que realizem o tratamento de dados de pessoas com as quais tem alguma relação.

Em quais situações a Lei não é aplicada?

Em casos de uma pessoa usar os dados pessoais de terceiros para fins exclusivamente particulares e não econômicos. Ex: Compartilhamento de número de telefone celular entre amigos.

Para fins exclusivamente jornalísticos, artísticos ou acadêmicos. Ex: divulgação de notícias com dados de um criminoso.

Para fins exclusivos de segurança pública, defesa nacional, segurança de Estado ou atividades de investigação e repressão de atividades penais. Ex: investigação policial

Quais são os tipos de dados que a Lei trabalha?

Dados Pessoais: Qualquer informação relacionada a pessoa natural identificada ou identificável. Ex: nome, endereço, dados cadastrais, profissão, nacionalidade, etc...

Dados Pessoais Sensíveis: Dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.

Dados Pessoais de Crianças ou Adolescentes: Os dados que envolvam menores de idade precisarão do consentimento dos pais e/ou responsáveis.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

Por que informações como CPF e endereço são dados pessoais?[1]

Conforme a LGPD, art. 5º, I, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Este conceito é composto por quatro elementos:		
Elementos do dado pessoal	**Informação**	Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).
	Relacionada a	Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios: (i) se relaciona a um conteúdo sobre o indivíduo; (ii) tem a finalidade de avaliar um indivíduo ou seu comportamento; ou (iii) tem um impacto sobre interesses ou direitos do indivíduo.
	Pessoa Natural	Para ser pessoal, a informação deve estar relacionada a um indivíduo humano.
	Identificada ou identificável	"Identificada" significa que a ligação ao indivíduo é feita de forma direta, como pelo tratamento de seu nome completo ou sua foto. Como "identificável", a ligação é indireta, e um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. É o caso de identificadores como o RG, CPF, o endereço e o telefone de uma pessoa natural.

1 Article 29 Working Party, Opinion 4/2007 on the concept of personal data Brussels, 2007. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. Acesso em: 23 abr. 2020.

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

https://blog.trinks.com/lei-geral-de-protecao-de-dados-lgpd-o-que-muda-em-seu-salao/

Quem são os sujeitos envolvidos na Lei?

Titular: é o "dono" dos dados pessoais – Pessoa física que os dados se referem

Controlador: (Agente de tratamento): é a empresa responsável por definir o que será feito com os dados pessoais. Ex: A Cooperativa que possui o cadastro do associado para fins de controle e transações comerciais.

Operador: (Agente de tratamento): é a empresa ou a pessoa que, a pedido do controlador, realiza o trabalho com os dados pessoais. Ex: A Cooperativa contrata uma empresa terceira para determinado trabalho, que exige a exposição dos dados do associado.

Encarregado de Dados Pessoais: é a pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ex: Setor ou alguém responsável pela Ouvidoria na Cooperativa.

ANPD: Agência Nacional de Proteção de Dados, que é o órgão federal responsável por regulamentar e fiscalizar o cumprimento da Lei.

Fonte: https://www.senior.com.br/blog/lgpd-o-que-e-como-vai-funcionar-e-o-que-muda-para-sua-empresa

Quais são dos direitos do titular dos dados pessoais?

Ele tem direito de solicitar ao Controlador, a qualquer momento e mediante requisição:

- Confirmação da existência de tratamento;
- Acesso aos seus dados;

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na LGPD;
- Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento;
- Revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem o seu interesse.

Quais são os benefícios que a cooperativa tem com a observância da Lei?

- Aumento da segurança jurídica;
- Maior valor agregado à empresa pelo estabelecimento de uma relação de maior transparência e confiança com os titulares dos dados;
- Ganho de credibilidade em função da privacidade garantida dos dados de associados e clientes;
- Garantia da existência de controles de segurança adequados a um ambiente operacional seguro.

Quais são as sanções que a cooperativa pode ter pela não observância da Lei, que entram em vigor a partir de 01/08/2021?

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, até 2 % do faturamento da Cooperativa, excluídos os tributos, limitadas, no total a R$ 50 milhões de reais por infração;
- Multa diária, observado o limite total;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração por até 6 meses;
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 meses;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Adoção de boas práticas para o alinhamento com a LGPD

- Não envie para e-mails pessoais os dados pessoais dos clientes, associados, fornecedores e colaboradores;

- Em e-mails destinados a fornecedores e parceiros comerciais, encaminhe apenas o dado necessário para a execução daquele serviço;
- Tenha cuidado com e-mails suspeitos que solicitem o preenchimento de formulários;
- Use uma fragmentadora de papel para descartar documentos que contenham dados pessoais;
- Não utilize o e-mail da cooperativa em cadastros de uso pessoal;
- Evite expor dados pessoais, bem como deixá-los em locais de fácil acesso a outras pessoas além de você;
- Mantenha o computador e o software antivírus sempre atualizados.

Um passo a passo para estar no caminho certo da LGPD

- Mapeie os pontos de entrada e saída de dados;
- Sempre peça consentimento;
- Colete apenas dados essenciais;
- Opte pelo armazenamento curto de dados (apenas o que precisa);
- Torne os dados anônimos sempre que possível;
- Lembre-se que a criptografia é obrigatória;
- Faça da documentação uma amiga importante;
- Auditoria SEMPRE;
- Você está no caminho do COMPLIANCE.

https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-giro

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

POLÍTICA DE PRIVACIDADE COCBAN

Ao acessar o site da Cocban, o usuário, expressa sua livre aceitação quanto aos termos e diretrizes de privacidade, autorizando a obtenção dos dados e informações mencionados, bem como sua utilização pela cooperativa.

Caso não esteja de acordo com esta política o usuário poderá descontinuar o seu acesso ao site e/ou aplicativo.

A política de privacidade segue anexa à este documento e está disponível na íntegra em nosso site.

19 - CONSIDERAÇÕES FINAIS/ RECOMENDAÇÕES NA POLÍTICA

I - Indicação Diretor Unicad/Plano de Ação e de Respostas a Incidentes/Relatório anual/ Revisão Política:

- Deverá ser emitido plano de ação e respostas à incidentes (Art. 6 – Resolução 4.893)

- Deverá ser indicado Diretor Responsável pela Segurança Cibernética no Unicad (Art.7– Resolução 4.893);

- Deverá ser emitido relatório anual sobre a implementação do plano de ação e respostas à incidentes com data base de 31 de dezembro (Art. 8 –Resolução 4.893)

- Esta política e o plano de ação e de respostas a incidentes deverão ser aprovados pela Diretoria (Artº 9 – Resolução 4.893)

- Esta política e o plano de ação e de respostas a incidentes deve ser revisada, no mínimo, anualmente (Artº 10 – Resolução 4.893)

II - Devem ser mantidos à disposição do Banco Central do Brasil por 5 anos:

1 – Política de Segurança Cibernética, anexa Política de Privacidade;

2 – A ata de reunião da Diretoria;

3 – O Plano de Ação e de Respostas Incidentes;

CNPJ: 04.158.581/0001-45 - NIRE: 31400041451
RUA HALFELD, Nº 525 SALA 605
CENTRO – JUIZ DE FORA – MG – CEP: 36.010-001
TELEFONE: (32) 3235-6317
E-MAIL: COCBAN@COCBAN.COM.BR
SITE: WWW.COCBAN.COM.BR
OUVIDORIA – 0800 – 283-6317 / OUVIDORIA_COCBAN@IG.COM.BR

4 – O relatório anual de implementação do plano de ação e de respostas a incidentes;

III – Aprovação Diretoria

Esta política foi aprovada em reunião da Diretoria de 28/03/2025.

IV- Assinaturas Diretoria:

Katya Maria Chaves Diretora Segurança Cibernética	gov.br Documento assinado digitalmente KATYA MARIA CHAVES Data: 26/03/2025 15:13:07-0300 Verifique em https://validar.iti.gov.br
Carlos Álvaro de Souza Paulo Diretor – Presidente	CARLOS ALVARO DE SOUZA PAULO:35983990730 Assinado de forma digital por CARLOS ALVARO DE SOUZA PAULO:35983990730 Dados: 2025.03.26 09:30:36 -03'00'
Claudio Márcio Santos Chaves Diretor - Financeiro	CLAUDIO MARCIO SANTOS CHAVES:89908600672 Assinado de forma digital por CLAUDIO MARCIO SANTOS CHAVES:89908600672 Dados: 2025.03.26 09:29:58 -03'00'
Graziela Polato Nicolau Diretora - Administrativa	GRAZIELA POLATO NICOLAU:02849014664 Assinado de forma digital por GRAZIELA POLATO NICOLAU:02849014664 Dados: 2025.03.26 09:29:11 -03'00'