POLÍTICA DE SEGURANÇA CIBERNÉTICA

1 - INTRODUÇÃO

Esta Política atende à Resolução CMN – Conselho Monetário Nacional nº 4.893/2021 que dispõe sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de armazenamento de dados e de computação em nuvem a serem observados pela **COOPERATIVA DE CRÉDITO MÚTUO DOS EMPREGADOS DA TUPY MINAS GERAIS LTDA. E NEMAK ALUMÍNIO DO BRASIL LTDA – FUNCOOP**

2 - OBJETIVO

O objetivo desta política é orientar os colaboradores e definir os procedimentos e controles da FUNDCOOP 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.

Parágrafo único. O disposto nesta Resolução não se aplica às instituições de pagamento, que devem observar a regulamentação emanada do Banco Central do Brasil, no exercício de suas atribuições legais.

3 - DA IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. A FUNDCOOP deve implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. A cooperativa opera somente os produtos "capital x empréstimo" junto as seus cooperados, estando enquadrada no Segmento 5 (S5), conforme definido na regulamentação em vigor.

Para atendimento dessa demanda e atentando ao § 3º do artigo 2ª da Resolução CMN 4893/21/2021, a FUNDCOOP formaliza que não possui cibernética própria e utiliza os serviços de processamento e armazenamento de dados e de computação em nuvem por meio da empresa Fácil Tech descrita no Item 8.

§ 1º A implementação desta Política considera as seguintes compatibilidades da Cooperativa:

I - o porte, o perfil de risco e o modelo de negócio da instituição;

II - a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

III - a sensibilidade dos dados e das informações sob responsabilidade da cooperativa.

§ 2º A política de segurança cibernética deve contemplar, no mínimo as diretrizes para:

A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b) Os ambientes, sistemas, computadores e redes da Cooperativa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. Caberá todos os colaboradores conhecer e adotar as disposições desta política e deverão proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, assegurando que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades de suas atividades.

4 - TRATAMENTO DA INFORMAÇÃO

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

5 - 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 por meio de ações prover controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, deve-se seguir as principais orientações para manter seu computador seguro:

- Manter os softwares de detecção e proteção (antivírus), atualizados, capazes de proteger eficientemente o ambiente corporativo;
- Manter atualizados os softwares e aplicativos de uso na rede. Somente instalar programas legítimos, de fonte confiáveis;
- Não abrir e-mails e arquivos enviados de fontes desconhecidas. Ao compartilhar recursos do computador, estabeleça senhas para os compartilhamentos e permissões de acesso adequadas;
- Se atentar aos endereços acessados no seu navegador;
- Ao realizar compras pela internet procurar por sites reconhecidamente seguros;
- Na utilização de internet banking procurar pelos sinais de segurança;
- trocar senhas com frequência, ela é pessoal e intransferível, e, criada de acordo com as funções permitidas para o exercício das suas atividades;

- Ao detectar algum erro é importante que seja rastreado, através das tecnologias disponíveis todo o caminho do processo, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou;
- Realizar backup periodicamente de todos os arquivos e sistemas.

6 - PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

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

Gestão de Ativos da Informação: Entende-se por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir. 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.

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.

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 ações são passiveis de auditoria e que possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

Gestão de Riscos: Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos de 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.

Mitigação dos Riscos: A Cooperativa oferece aos Colaboradores estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador 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, acesso à internet, e-mail, etc.). Equipamentos e computadores disponibilizados aos Colaboradores que devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Cooperativa. A instalação de copias de arquivos de qualquer

extensão, obtido de forma gratuita ou remunerada, em computadores da Cooperativa depende de autorização do Diretor responsável pela Política de Segurança Cibernética devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes. As mensagens enviadas ou recebidas através de correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da Cooperativa poderão ser monitorados. 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 divulgados para quaisquer terceiros. O colaborador 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 forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseados em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome de empresa, nome de departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcde", "12345", entre outras. Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtivessem acesso indevido ao seu login/senha.

Tratamento de Incidentes de Segurança da Informação: Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas 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 internet;
- Sabotagem/terrorismo;
- Indisponibilidade de acesso a Cooperativa;
- Ataques DDOS.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente ao Diretor Responsável pela Política de Segurança Cibernética.

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

Controle de Prestadores de Serviços: Os prestadores de serviços que detenham informações sensíveis ou que sejam relevantes para condução das atividades operacionais da cooperativa,

deverão ser tecnicamente capacitados e extremamente envolvidos com as atividades da cooperativa, de forma íntegra e responsabilizados sobre qualquer dano ou vazamento de informações de acordo com contrato de prestação de serviço e políticas internas da cooperativa. O acesso a qualquer informação deverá ser solicitada formalmente por e-mail, ao Responsável na Cooperativa.

7 - 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.

Avaliação Inicial: Avaliar o incidente em conjunto com a Diretoria para verificar se é provável a 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: Caracteriza o incidente, devem ser tomadas as medidas imediatas, tais como: O Diretor responsável pela política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos; Conforme a relevância (sabotagem, terrorismo, etc.) poderá ser registrada um boletim de ocorrência ou queixa crime para as devidas providencias; Conforme a relevância do incidente comunicar os cooperados que por ventura foram afetados; Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções de serviços relevantes, que configurem uma situação de crise pela Cooperativa.

Recuperação: Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada e terceiros notificados. Quaisquer dados que estejam faltando ou que estejam corrompidos, ou problemas identificados por colaboradores internos devem 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 mudanças e medidas de prevenção.

Plano de Ação e de Resposta a Incidentes: A cooperativa deve estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética, o plano deve abranger, no mínimo:

- As ações a serem desenvolvidas pela cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
- A área responsável pelo registro e controle dos efeitos de incidentes relevantes está subordinada ao diretor responsável designado pela Política de Segurança Cibernética informado ao BACEN por meio do UNICAD.

Deverá ser elaborado até 31 de março do ano seguinte ao da data base e aprovado pela Diretoria Executiva em ata de reunião

8 - DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A FUNDCOOP tendo em vista a necessidade de agilizar o atendimento de seus cooperados e visando maior segurança e celeridade firmou contrato de prestação de serviços de processamento e armazenamento de dados e de computação em nuvem Nº CT-NUV-17723-2016 do SISTEMA FacCred da empresa Fácil que é a responsável pelos serviços de processamento e armazenamento de dados, sendo o processo de contingência da cooperativa detalhadas no **Anexo I** que é parte integrante do presente contrato.

I- Processo de contingência da infraestrutura;

- Armazenamento (Hospedagem) em Nuvem
- Endereços Eletrônicos
- Prestação de Serviços

II- Plano de Contingência – Continuidade de Negócios.

- Realização de backups em Nuvem
- Suporte

8.1 Para atendimento a permissão de acesso e comunicação ao Banco Central do Brasil foi firmado Termo Aditivo ao contrato (AD-CRE-26433-2022) datado de 21/09/2022.

9 - PROCEDIMENTOS E INSTRUÇÕES

Os procedimentos e as instruções encontram-se presentes na Política de Segurança Cibernética, visto que, estes representam as responsabilidades atribuídas à FÁCILTECH, por conta do objeto do contrato de Serviço de Computação em Nuvem. Assim, é necessário um detalhamento meticuloso das ações, as atividades desenvolvidas e a sua relação com as informações. Esse nível de

detalhamento pressupõe a necessidade de constante revisão e/ou manutenção dessa política, conforme a seguir:

Testes São realizados testes, sendo estes executados de forma automatizada e por robôs de monitoramento, diariamente;

Acompanhamento O acompanhamento de carga e desempenho é realizado em tempo real, através de ferramenta automatizada que, no processo de monitoramento do ambiente, pode gerar alerta em caso de pico de uso e recurso de algum servidor;

Administração do Banco de Dados Toda a parte de administração e verificação do banco de dados é de exclusiva responsabilidade da FÁCILTECH, sendo operacionalizada de forma manual ou automática pelas versões do sistema;

Administração de Contas de Usuários Os usuários que utilizaram o(s) Sistema(s) da FÁCIL TECH serão gerenciados e autorizados pela Cooperativa. Já o cadastro e criação de usuários para acessar o Cloud serão realizados pela FÁCILTECH mediante solicitação da Cooperativa;

Administração de Ferramentas de Segurança A administração das ferramentas de segurança como firewalls, IDS/IPS, WAF e BACKUP será de responsabilidade da FÁCILTECH. Há um monitoramento constante de ocorrências e aplicação de vacinas e regras que visam evitar problemas com ataques;

Plano de Contingência Como todo o ambiente FÁCILTECH cloud é virtualizado, a qualquer momento, sendo necessário, podem-se levar os snasphot dos servidores para qualquer Data Center da AMAZON no mundo, de forma a subir um novo ambiente de uso dos sistemas. Para acesso às informações, basta o colaborador na Cooperativa autorizada, conectar-se a qualquer rede de internet, em qualquer lugar do mundo "Snapshot é o registro do estado de um sistema, aplicação ou arquivos em determinado ponto no tempo";

Ocorrência de Incidente As verificações são realizadas por meio de pentests, que tem ocorrido de acordo com demanda dos clientes e com certa frequência. O tempo de restabelecimento por um eventual ataque, uma vez ocorrendo, dependerá do tipo de ataque, visto que, eventualmente, pode ser resolvido em poucos minutos ou, havendo situações mais complexas, demandará a abertura de uma janela maior para correção. No pior dos cenários, o retorno de snapshot pode ocorrer no máximo em 02 (duas) horas. "Pentest é uma forma de detectar e explorar vulnerabilidades existentes nos sistemas, ou seja, simular ataques de hackers";

Registro de Incidentes Considerando a responsabilidade da FÁCILTECH na administração do banco de dados e das ferramentas de segurança da Cooperativa, torna-se necessário a comunicação ao Diretor Responsável pela Política de qualquer incidente relevante, sendo este formalizado através de relatório e/ou declaração contendo o registro dos incidentes verificados em testes, ou os que efetivamente ocorreram;

Continuidade de negócios A estrutura de gerenciamento, em linhas gerais, visa garantir que a Política está sendo cumprida, com vistas a minimizar a ocorrência de fatores que coloquem em risco as atividades da Cooperativa, e consequentemente expondo-a a risco de descontinuidade. Nesse sentido, para evitar a descontinuidade do negócio, torna-se necessário proceder com a análise dos incidentes, de forma que estes correspondam a um nível crítico ou aceitável, e verificar se estão em consonância com as medidas corretivas a serem adotadas;

Comunicação a Diretoria: Tendo em vista a complexidade que envolve o cumprimento da Política de Segurança Cibernética, e a dificuldade da Cooperativa em validar ou não a efetivação dos procedimentos, é imperiosa manter o Diretor Responsável pela política informado sobre indícios de irregularidades verificadas quando do cumprimento das determinações dessa política. Assim, caberá à FÁCILTECH realizar a comunicação de possíveis indícios quando de sua ocorrência, de forma semestral ou anual, quando encaminhar relatório demonstrando as verificações realizadas sob a ótica da gestão de acessos, proteção de ambientes, segurança física e lógica e continuidade do negócio.

Responsabilidades e Obrigações da Contratada

Responsabilidades

- Instalação de softwares nas estações-clientes da CONTRATANTE e com a dispensa de aquisição de licenças dos softwares de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;
- realização de backup em nuvem, totalmente automatizado, em ambiente de alta disponibilidade e durabilidade, com garantia da integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações;
- acompanhamento do banco de dados, contemplando desde o dimensionamento, instalação e configuração até tuning, backup/recover, monitoramento e aplicação de patches;
- monitoramento de servidores e serviços, com notificações em caso de falhas, com características Proativas (ações para antecipação de falhas), Reativas (ações de resposta a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas);

- todas as consultas ao setor de suporte serão, necessária e obrigatoriamente, registradas no aplicativo FacCRM (Customer Relationship Management) da CONTRATADA, com livre acesso da CONTRATANTE para acompanhamento de todos os passos seguintes para a solução da ocorrência.

Obrigações

I - Garantir que o canal de comunicação seja utilizado para fins da execução dos serviços e que será seguro e livre de quaisquer intervenções de terceiros não relacionados com a presente avença. Garante, igualmente, que os seus técnicos, empregados ou não, não farão uso de quaisquer informações obtidas por qualquer meio nos referidos equipamentos, aí incluídos arquivos de qualquer tipo, senhas, nomes de usuário e afins;

II - efetuar, nos módulos do SISTEMA, em tempo hábil, todos os implementos comprovadamente necessários para a adequação à legislação exclusivamente federal em vigor, sem ônus adicional para a Cooperativa (CONTRATANTE);

III - garantir o correto funcionamento técnico dos módulos licenciados do SISTEMA mantendo todas as funções em plena operacionalidade e provendo as soluções aos eventuais problemas técnicos registrados pela CONTRATANTE na *FacCRM* e fornece suporte técnico solucionando ou oferecendo previsão para solução de problemas quanto o bom funcionamento dos serviços, salvo se tais problemas tiverem causas nas situações elencadas nos subitens 10.2 e 10.3 do presente contrato;

IV - quando executados por meio de acesso remoto (VPN), deverão preservar e garantir a segurança do ambiente de rede da CONTRATANTE garantia essa que deve ser extensiva à confidencialidade, ao sigilo, ao conteúdo e à identidade dos programas, arquivos e informações armazenados nos equipamentos da última;

V - responsabilizar-se integralmente pela segurança e pela qualidade técnica dos serviços prestados, reparando, corrigindo, quando os serviços executados se mostrarem inadequados ao uso dos equipamentos pela CONTRATANTE;

VI - prestar toda a assistência à CONTRATANTE, visando ao bom e perfeito funcionamento das instalações de seus servidores;

VII - disponibilizar para o seu pessoal todo o ferramental e todos os equipamentos que forem necessários à execução dos serviços, mantendo-se responsável, ainda, pela sua guarda e conservação;

VIII - informar aos administradores da CONTRATANTE quais tarefas administrativas relacionadas com os serviços prestados por este Contrato, mantendo, assim a transferência da tecnologia;

IX - todas as consultas ao setor de suporte serão, necessária e obrigatoriamente, registradas no aplicativo FacCRM (Customer Relationship Management) da CONTRATADA, com livre acesso da CONTRATANTE para acompanhamento de todos os passos seguintes para a solução da ocorrência;
X - todas e quaisquer comunicações entre as contraentes, que não sejam as consultas ao setor de suporte deverão ser feitas por escrito e com recebimento e aceite confirmados pelos e-mails oficiais de contato CONTRATADA: andre@facilinformatica.com.br e CONTRATANTE: adriane.fernandes@tupy.com.br
XI - a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta dias) para a interrupção do serviço, feito pelo responsável;
XII - a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante;
XIII - O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto nesta Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

Responsabilidades da Contratante
I - Realizar as etapas de sua responsabilidade para os testes do ambiente e migração para nuvem;
II - Parametrizar o SISTEMA estritamente de acordo com as normas legais pertinentes à sua atividade e manter a supervisão, administração e controle do uso do SISTEMA, designando adequadamente quem venham a ser os colaboradores responsáveis: pela sua gestão e pela segurança de uso;

III - Tomar todas as medidas de segurança possíveis, perante os seus empregados e terceiros com os quais mantenha relações comerciais, para que não sejam violados os direitos autorais do SISTEMA;

IV - Agendar com a CONTRATADA, no menor espaço de tempo possível, a data para atualização de versão do SISTEMA, de maneira a manter, necessária e obrigatoriamente, o SISTEMA na sua mais recente versão;

V - Comunicar ao Banco Central do Brasil a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem, nos termos do art. 15 da Resolução CMN nº 4.893/2021.

VI – Permitir o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos

dados e das informações, bem como aos códigos de acesso aos dados e às informações nos termos do inciso VII do art. 17. da Resolução CMN nº 4.893/2021.

Compartilhamento de informações – Fatos relevantes

I - 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 caso de incidentes relevantes ou não pois quaisquer ocorrências demonstrarão falhas nas defesas ou prevenções devendo as ocorrências nos diversos níveis operacionais da cooperativa, buscando aprimorar os mecanismos preventivos;

II - O compartilhamento de informações sobre incidentes relevantes mencionados no inciso I com outras cooperativas trata-se de uma prática que não é comum, mas que deve ser buscada em função que diversos incidentes são comuns tendo como origem fontes idênticas e o mesmo 'modus operandi". Uma das formas será por meio da empresa terceirizada de informática contratada e que serviria de elo de compartilhamento com outras cooperativas.

Tratamento de fatos relevantes no ambiente cibernético

I - os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da cooperativa;

II - os cenários de incidentes considerados nos testes de continuidade de negócios;

III - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos; e

IV - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes.

10 - DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

I - A política de segurança cibernética deve ser divulgada aos funcionários da cooperativa e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações;
II - A cooperativa deve divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

11 - DISPOSIÇÕES FINAIS

I - o documento relativo à política de segurança cibernética deve ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

II - A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente;

Foi designado e devidamente registrado no UNICAD, diretor responsável pela Política de Segurança Cibernética e pela execução do plano de ação e de resposta a incidentes.

III - A atualização da Política de Segurança Cibernética foi aprovada na Ata de Diretoria de abril/2024.

Betim 15 de maio 2024

Nelson Pinheiro Branco Junior
Diretor Administrativo
Responsável pela Política de Segurança Cibernética

FUNDCOOP

ANEXO I

Processo de contingência infraestrutura da Cooperativa de Economia e Crédito Mútuo dos Empregados da Tupy Minas Gerais LTDA. e Nemak Alumínio do Brasil LTDA. FUNDCOOP – **Servidores e tecnologias relacionadas.**

Referências

- Contrato de Armazenamento em Nuvem CT-NUV- 17723/2016
- SISTEMA: FacCred
- Armazenamento de Dados em Nuvem: Empresa Amazon- módulo FacMobile

I - Processo de contingência da infraestrutura

- **Armazenamento (Hospedagem) em Nuvem**
  Hospedagem : DataCenter utilizando estrutura da Empresa Amazon.

- **Armazenamento do Sistema e dados em Nuvem**
  - ✓ Implementar e manter controles de segurança incluindo, sem limitação, segurança de hardware e software, firewalls, filtros e outras ferramentas de segurança;
  - ✓ Armazenar e transmitir as credenciais de acesso de demais informações confidenciais de maneira criptografada;
  - ✓ Garantir a segregação de acesso entre os ambientes de seus diferentes clientes, impedindo o acesso não autorizado às informações da FUNDCOOP;
  - ✓ Garantir que os acessos sigam a diretriz do privilégio mínimo, onde os acessos aos ambientes devem ser concedidos baseando-se somente na real necessidade;
  - ✓ disponibilizar informações para auditorias (internas e externas) e investigações judiciais quando solicitadas. Caso sejam encontradas desconformidades, o SISTEMA deverá prover plano de ação para correção; e,
  - ✓ Seguir, em caso de eventuais desastres, os procedimentos preconizados pela própria AMAZON, em seu processo interno.

- **Endereços Eletrônicos**
  Hospedagem: Empresa Amazon os termos estão divulgados de forma integral nos seguintes endereços eletrônicos;

  - ✓ SLA: wttp://aws.amazon.com/pt/ec2-sla/;
  - ✓ Contrato: wttp://aws.amazon.com/pt/agreernt/;
  - ✓ Termos de Serviços: wttp://aws.amazon.com/pt/serviceterms/; e

✓ Uso Aceitável: wttp://aws.amazon.com/pt/aupt/.

- **Prestação de Serviços**
  - ✓ Disponibilização para uso de todos os módulos licenciados do SISTEMA, sem a necessidade de instalação de *softwares* nas estações-clientes da FUNDCOOP e com a dispensa de aquisição de *softwares* de banco de dados, sistema operacional e antivírus, necessários aos servidores em nuvem;
  - ✓ Na hipótese de encerramento do relacionamento mantido entre o SISTEMA e a Amazon, o SISTEMA, obriga-se a, sem quaisquer custos para a FUNDCOOP, no prazo de 5 (cinco) dias úteis, disponibilizar novo provedor de serviços com as mesmas obrigações e garantias previstas no contrato.

II - Plano de contingência – Continuidade de negócios:

- **Realização de backups em Nuvem**
  - ✓ Realização de *backup* em nuvem, totalmente automatizado em ambiente de alta disponibilidade e durabilidade, com garantia de integridade dos dados por meio de restaurações periódicas em ambiente de homologação e confidencialidade das informações;
  - ✓ Acompanhamento do banco de dados, contemplando o dimensionamento, instalação e configuração até *tuning, backup/recover*, monitoramento e aplicação de *patches*; e
  - ✓ Monitoramento de serviços e serviços, com notificações de falhas com características **Proativas** (ações para antecipações de falhas), **Reativas** (ações de resposta a eventuais falhas) e preventivas (ações para minimizar probabilidade de falhas)
  - ✓ O SISTEMA efetuará e manterá *backups* sob a política cíclica de armazenamento que garante a disponibilidade de restauração de *backup* dos 7(sete) últimos dias, com as seguintes características:
    - Backup diário de todo o banco de dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,9999999% de durabilidade e de 99,97% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais; e
    - Os backups serão testados semanalmente (restauração em ambiente de homologação) para garantir sua integridade.
    - O SISTEMA disponibilizará diariamente um arquivo contendo o backup lógico do banco de dados da FUNDCOOP. Por questões de segurança este arquivo estará disponível dentro do ambiente da AMAZON e caberá a FUNDCOOP realizar a transferência *(download)* para sua máquina local utilizando-se do recurso de copiar e colar (Ctrl+C e CtrL+V). Cabe ao SISTEMA ainda, especificar quais usuários deverá ter acesso ao arquivo. O arquivo será disponibilizado no formato EXPDP do Oracle 11g R2 e compactado através de ZIP.

- **Suporte**

  Todas as consultas ao setor de suporte serão, necessária e obrigatoriamente, registradas no aplicativo *FacCRM (Customer Relationship Management)* do SISTEMA, com acesso da FUNDCOOP para acompanhamento de todos os passos seguintes para a solução da ocorrência:

  - ✓ Fornece suporte técnico a FUNDCOOP, solucionando ou oferecendo previsão para solução de problemas quanto ao bom funcionamento dos serviços;
  - ✓ Informar a FUNDCOOP, tão logo tome conhecimento da interrupção, considerando que o prazo mínimo de aviso deverá ser de pelo menos 2 (dois) dias úteis de antecedência, da data das interrupções necessárias para ajustes técnicos ou manutenção que demandem mais de 2 (duas) horas de duração e que possam causar prejuízo à operacionalidade da plataforma, salvo em caso de urgência;
  - ✓ Nos casos de urgência, assim entendidos aqueles que coloquem em risco o regular funcionamento do servidor e aqueles determinados por motivo de segurança decorrente de vulnerabilidade detectada, as interrupções serão imediatas e sem aviso prévio a FUNDCOOP;
  - ✓ As manutenções e interrupções a serem informadas são única e exclusivamente aquelas que interfiram com a operacionalidade da plataforma, ficando dispensadas informações prévias sobre interrupções, por motivos técnicos, de serviços acessórios que não impliquem em prejuízo para a operacionalidade da plataforma;
  - ✓ A interrupção que interfira ou cause prejuízo à operacionalidade do ambiente em nuvem, onde hospedado o SISTEMA, e seja necessária para a manutenção dos serviços será realizada, sempre que possível, entre as 21 e 6 horas ou nos finais de semana; e
  - ✓ As interrupções para a manutenção na prestação de serviços acessórios, que não impliquem em prejuízo para operacionalidade do servidor, perdurarão pelo tempo necessário à supressão das irregularidades detectadas.