POLÍTICA DE SEGURANÇA CIBERNÉTICA

RESOLUÇÃO CMN Nº 4.893/21

ILHÉUS/BA
2024

ÓRGÃOS ESTATUTÁRIOS

Conselho de Administração (CONAD)
José Montival de Alencar Júnior
Laudelino Quinto de Souza Júnior
Lino Arnulfo Vieira Cintra
Luis Frank Costa Ferreira
Luiz Henrique Farias dos Santos
Renata Vieira de Abreu
Vitoria Solange Coelho Ferreira
Cristiano Caetano da Silva
Edenilton Santana

Diretoria Executiva (DIREX)
Luiz Henrique Farias dos Santos
Edenilton Santana
Cristiano Caetano da Silva

Conselho Fiscal (CONFIS)
Manoelita Maria dos Santos
Carina de Farias Gonçalves
Priscila Silveira Sousa
Herval Passos dos Santos
Vinicius Nascimento Santos

Ouvidoria
Luiz Henrique Farias dos Santos

Setor Administrativo
Viviane Almeida Morais

Estágio
Gabriele Santos Batista
Eric Araújo Duarte
Marina Lavigne da Costa Santos
Artur Henrique Pereira Santos

SUMÁRIO

1. INTRODUÇÃO

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

A Resolução CMN n° 4.893/2021 dispõe sobre **a Política de Segurança Cibernética** e sobre os requisitos necessários para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, os quais deverão ser observados pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**.

2. OBJETIVO

O objetivo desta política é orientar os dirigentes e colaboradores e definir os procedimentos e controles da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, em relação à segurança cibernética. Os requisitos mínimos se alinham 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 de Segurança Cibernética**.

ATENÇÃO: Paralelo ao armazenamento de dados em nuvens, **a Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deve manter um eficiente e moderno Arquivo Físico de Documentos.

3. CONCEITO

Para melhor compreensão da necessidade de se cumprir o descrito na **Política de Segurança Cibernética,** é necessário conhecer os conceitos que fazem parte desse segmento, onde a informação é extremamente valiosa e passível de riscos que colocam em xeque a continuidade da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.** A seguir ficam listados os seguintes conceitos que norteiam entendimentos, facilitando aplicações pelos dirigentes e colaboradores:

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

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

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

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

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

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

MALWARE**:** é um termo amplo que é usado para classificar todo tipo de software malicioso usado para causar prejuízo, que pode ser até financeiro, danificar sistemas, interceptar dados ou simplesmente irritar o usuário, afetando tanto computadores como celulares e até redes inteiras.

VÍRUS: software que causa danos à máquina, rede, softwares e banco de dados. Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador.

SPYWAR*E***:** software malicioso para coletar e monitorar o uso de informações.

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

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

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

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

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

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

ACESSO PESSOAL**:** pessoas localizadas em lugares públicos como: bares, cafés e restaurantes, que captam qualquer tipo de informação que possa ser utilizada, posteriormente, para um ataque.

FRAUDES EXTERNAS E INVASÕES: realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

ATAQUE DDOS E BOTNETS**:** ataques que visam negar ou atrasar o acesso aos serviços, ou sistemas da instituição; no caso dos *Botnets*, o ataque vem de inúmeros computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens, resultando na negação do serviço.

4. SEGURANÇA CIBERNÉTICA

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, através do Conselho de Administração ou da Diretoria Executiva, estabelece **a Política de Segurança Cibernética**, bem como os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando total observância e adequação ao exigido na Resolução 4.893/21.

O propósito desta **Política de Segurança Cibernética** é orientar os dirigentes e colaboradores da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação Cibernética, em conformidade com as disposições constitucionais, legais e regimentais vigentes.

O objetivo fundamental desta **Política de Segurança Cibernética** é garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual **da Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** dos seus cooperados e envolvidos.

A Política de Segurança Cibernética deve assegurar a proteção dos ativos de informação da referida **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** contra as ameaças, internas ou externas, deve reduzir a exposição ou danos decorrentes de falhas de cyber segurança e deve garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo dos negócios.

5. DIRETRIZES CORPORATIVAS

A segurança da informação da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** estabelece os principais controles, denominados diretrizes, a seguir:

a) As informações da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** 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) As informações devem ser utilizadas de forma transparente e apenas para a 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 recurso só deve ser feito se devidamente autorizado;
e) A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizada;
f) A concessão de acessos deve seguir 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 de Crédito de Servidores da UESC Ltda. – UESCOOP** devem ser reportados ao Diretor que é responsável pela área de Segurança da Informação "BCB"; e
i) As responsabilidades quanto à Segurança da Informação devem ser, amplamente, divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes.

Conforme a Resolução n° 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

a) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos adquiridos;
b) Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** utilizando recursos computacionais de seus prestadores de serviços;
c) Execução por meio de Internet de aplicativos, implantados ou desenvolvidos por prestadores de serviços, com utilização de recursos computacionais do próprio prestador contratado pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

A Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP é responsável pela Gestão dos serviços contratados incluindo as seguintes atividades:

- Análise de informações e de recursos adequados ao monitoramento dos serviços;
- Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a prestadores de serviços;
- Cumprimento da legislação e da regulamentação vigente.

6. IMPLEMENTAÇÃO

A implementação desta **Política de Segurança Cibernética** da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** considera as seguintes compatibilidades:

- O porte, perfil de risco e o modelo de nossos negócios;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais;
- A sensibilidade dos dados e das informações sob responsabilidade da instituição;
- Os ambientes, sistemas, computadores e redes da **Cooperativa de Crédito de Servidores da UESC Ltd**a. **– UESCOOP** poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras; e
- Caberá a todos os dirigentes e colaboradores conhecer e adotar as disposições desta **Política de Segurança Cibernética**. Deverão proteger as informações, contra acesso, modificação, destruição ou divulgação não autorizada, assegurando que os recursos tecnológicos à sua disposição e que sejam utilizados apenas para as finalidades de suas atividades.

7. TRATAMENTO DA INFORMAÇÃO

A informação deve receber proteção adequada em observância aos princípios e diretrizes da política de segurança da informação cibernética da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** em todo seu ciclo de vida, que compreende a geração, manuseio, armazenamento, transporte e descarte.

8. PROCEDIMENTOS E CONTROLES

No intuito de registrar procedimentos e controles para reduzir a vulnerabilidade da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** a incidentes atendendo aos demais objetivos, traçados pela **Política de Segurança Cibernética**. Através disso, prover controles específicos, incluindo os voltados para a rastreabilidade da informação, buscando garantir a segurança das informações sensíveis, alinhando-se, conforme pontuado a seguir, as principais orientações, visando manter seguro seu computador:

a) Manter os softwares de detecção e proteção (antivírus), atualizados, capazes de proteger eficientemente o ambiente corporativo;
b) Manter atualizados os softwares e aplicativos de uso na rede;
c) Instalar, somente, programas legítimos, de fonte confiáveis;
d) Evitar abrir e-mails e arquivos enviados de fontes desconhecidas;
e) Compartilhar recursos do seu computador, estabelecendo senhas para os compartilhamentos e permissões de acesso adequadas;
f) Ficar atento aos endereços acessados no seu navegador;
g) Realizar compras pela internet, procurando por sites reconhecidamente seguros;
h) Fazer utilização de internet banking, procurando pelos sinais de segurança;
i) Trocar, sempre, suas senhas com frequência. Elas são pessoais e intransferíveis, e, são criadas de acordo com as funções permitidas para o exercício das suas atividades;
j) Procurar detectar, sempre, a ocorrência de erros. Tal proceder é importante que seja rastreado, através das tecnologias disponíveis em todo o caminho do processo, facultando, rapidamente, corrigir os pontos onde os erros acontecem ou iniciam; e
k) Realizar backups, periodicamente, de todos os arquivos e sistemas.

9. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam, adequadamente, protegidas, a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** adota os seguintes processos:

GESTÃO DE ATIVOS DA INFORMAÇÃO

a) Entender por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir, podendo ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas); e
b) Identificar os Ativos da Informação de forma individual, inventariados e protegidos de acessos indevidos, fisicamente e logicamente, e ter documentos e planos de manutenção.

CLASSIFICAÇÃO DA INFORMAÇÃO

Classificar as informações 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 acessos e os impactos no caso de utilização indevida das informações.

GESTÃO DE ACESSOS

a) Utilizar as concessões, revisões e exclusões de acesso como ferramentas, atendendo aos processos desenvolvidos e utilizados pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**; e
b) Rastrear ao máximo os acessos utilizados pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**. A fim de garantir que ações sejam passiveis de auditoria e possam identificar, individualmente, o dirigente e colaborador, para que seja responsabilizado por suas ações.

GESTÃO DE RISCOS

a) Identificar os riscos por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os Ativos de Informação da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, para que sejam recomendadas as proteções adequadas; e
b) Escalonar os cenários de riscos de trabalhados pela Política de Segurança Cibernética, evidenciados pelos Ativos de Informação nos setores apropriados, para decisão.

MITIGAÇÃO DOS RISCOS

a) **Oferecer à Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** aos seus dirigentes e colaboradores estrutura tecnológica para o exercício das atividades, sendo responsabilidade de todos e por extensão de cada um manter e zelar pela integridade dessas ferramentas de trabalho, mantendo o controle sobre segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, notebook, acesso à internet, e-mail, etc.);
b) Disponibilizar equipamentos e computadores aos dirigentes e colaboradores para bem utilizarem, com a finalidade precípua de atender aos interesses comerciais legítimos da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**;
c) Arquivar as instalações de copias, promovidas em qualquer extensão, obtendo de forma gratuita, ou remunerada, e utilizadas pelos computadores da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** dependendo de autorização do Diretor responsável pela **Política de Segurança Cibernética,** devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes;
d) Receber as mensagens enviadas, através de correio eletrônico corporativo (e-mails similares), seus respectivos anexos, nas navegações da rede mundial de computadores (internet), alcançados pelos equipamentos da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**; podendo ser monitoradas;
e) Conter e acompanhar a utilização das senhas pessoais e intransferíveis de acesso aos dados disponibilizados em todos os computadores, bem como nos e-

mails, devendo ser conhecidas pelo respectivo usuário de computador e em hipótese nenhuma, dever ser divulgados para quaisquer terceiros;

f) Responsabilizar o dirigente e o colaborador, 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;

g) Proibir as anotações e armazenamentos das senhas em arquivos eletrônicos (Word, Excel, etc.). Não devem ser baseadas em informações pessoais, como, nome próprio, data de nascimento, endereço, placa de veículo, nome de empresa, nome de departamento. Não devem ser constituídas de combinações óbvias de teclado, como “abcde”, “12345”, entre outras; e

h) Alterar a própria senha é uma faculdade dada aos usuários, devendo cada responsável ser orientado a fazê-lo, caso suspeite que terceiros obtiveram acessos indevidos ao seu login/senha.

TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os Incidentes de Segurança da Informação são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam aos negócios desenvolvidos pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** como por exemplo:

a) Queda de energia elétrica;
b) Falha de um elemento de conexão;
c) Servidor fora do ar;
d) Ausência de conexão com internet;
e) Sabotagem/terrorismo;
f) Indisponibilidade de acesso a cooperativa;
g) Ataques DDOS.

SEGURANÇA FÍSICA DO AMBIENTE

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

Controle de Prestadores de Serviços que manuseiam dados ou informações sensíveis:

Procurar não deter informações sensíveis dos prestadores de serviços que sejam relevantes e essenciais na condução das atividades operacionais da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, devendo os prestadores de serviços serem tecnicamente capacitados e extremamente envolvidos com as atividades realizadas;

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** de forma plena responsabilizará o servidor ou prestador de serviço, envolvido sobre qualquer dano ou vazamento de informações de acordo com contrato de prestação de trabalho, referendado pela **Política de Segurança Cibernética** e outras normas internas. O acesso a qualquer informação deverá ser solicitada formalmente por e-mail, ao Responsável na **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**.

10. 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 de Crédito de Servidores da UESC Ltda. UESCOOP.**

AVALIAÇÃO INICIAL

a) Avaliar o incidente em conjunto com o Conselho de Administração ou Diretoria Executiva para verificar se é provável a sua reincidência ou se é um sintoma de problema crónico, para a tomada providências e medidas corretivas; e
b) Analisar motivos e consequências imediatas, bem como a gravidade da situação.

INCIDENTE CARACTERIZADO

Sendo caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

a) O Diretor responsável pela Política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos;
b) Conforme a relevância (sabotagem, terrorismo, etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providencias:
c) Conforme a relevância do incidente comunicar os cooperados que porventura foram afetados; e
d) 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 de Crédito de Servidores da UESC Ltda. – UESCOOP**.

RECUPERAÇÃO

a) Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada e terceiros notificados; e
b) Quaisquer dados que estejam faltando ou que estejam corrompidos, ou problemas identificados por dirigentes e colaboradores devem ser comunicados ao Conselho de Administração ou 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.

RELATÓRIO SOBRE IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

a) Será parte integrante do relatório de controles internos e do relatório integrado de gestão de risco da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, tendo em vista a complexidade e ao porte da mesma, e deve contemplar, no mínimo, as seguintes informações;
b) A efetividade da implementação das ações relativas à implementação da **Política de Segurança Cibernética;**

c) O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
d) Os incidentes relevantes relacionados com o ambiente cibenético ocorridos no período;
e) Os resultados de testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes; e
f) Deverá ser elaborado até 31 de março do ano seguinte ao da data base e aprovado pelo Conselho de Administração em ata de reunião.

11. EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** ao realizar contratações de serviços relevantes e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo;
b) Se mantém Política de Segurança da Informação;
c) Se possui Plano de Continuidade Operacional; e
d) Se as mudanças ou alterações de Serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças), fica mantido Gestão de Incidentes.

VERIFICAÇÃO DA CAPACIDADE DO POTENCIAL PRESTADOR DE SERVIÇOS DE FORMA A ASSEGURAR OS SEGUINTES REQUISITOS:

a) Cumprimento da legislação e da regulamentação em vigor;
b) Permissão de acesso da **Cooperativa de Crédito de Servidores da UESC Ltda. UESCOOP** aos dados e as informações a serem processadas ou armazenadas pelo Prestador de Serviços;
c) Confidencialidade, Integridade, disponibilidade e recuperação dos dados e das Informações processadas ou armazenadas pelo Prestador de Serviços;
d) Aderência a certificações que a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** possa exigir para a prestação do serviço a ser contratado;
e) Acesso da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de Serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
f) Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
g) Identificação e segregação dos dados dos clientes **da Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** por meio de controles físicos e lógicos; e

h) Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados.

12. AVALIAÇÀO DOS SERVIÇOS A SEREM CONTRATADOS

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deve proceder a uma avaliação da relevância dos serviços prestados por empresa com possibilidade de serem contratadas, considerando o seguinte:

a) Criticidade dos serviços a serem prestados;
b) Sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
c) Verificação, quanto à adoção, por parte do prestador de serviços, naquilo que se reporta aos controles, que mitiguem efeitos eventuais, vulnerabilidade na liberação de novas versões de aplicativos, no caso de serem executados através de internet.

13. COMUNICAÇÃO AO BANCO CENTRAL

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deverá informar previamente ao Banco Central do Brasil a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada 10 (dez) dias após a contratação dos serviços e deve conter as seguintes informações:

a) Denominação da empresa a ser contratada;
b) Os serviços relevantes a serem contratados; e
c) 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, com destaque para os casos de contratação no exterior.

As alterações contratuais, que impliquem modificações nas informações contratadas, devem ser comunicadas ao Banco Central do Brasil, no mínimo 10 (dez) dias após a alteração contratual verificada.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada **pela Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** quando houver, deve observar o alinhamento dos seguintes requisitos:

a) Elaborar um convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
b) Assegurar que a prestação dos serviços não cause prejuízo ao seu regular funcionamento, nem embaraço a atuação do Banco Central do Brasil;
c) Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
d) Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio, citado nos itens anteriores, a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deve assegurar que a legislação preceituada nos países e regiões onde ficar em atuação será obedecida em todas sua regulamentação. Em cada país onde os serviços poderão ser prestados não restringem, nem podem impedir o acesso das instituições contratantes e do Banco Central do Brasil, referente às suas informações.

14. DOS CONTRATOS

Os contratos firmados entre **a Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) 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, quando houver;
b) A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
c) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
d) A obrigatoriedade, em caso de extinção do contrato, deve conter:
- Transferência dos dados ao novo prestador de serviços ou à **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP;** e
- Exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos; e

e) O acesso da **Cooperativa de Crédito de Servidores da UESC Ltda. UESCOOP** deve acolher às:
- Informações fornecidas pela empresa contratada, visando o cumprimento dos itens previstos, escalonados acima;
- Informações relativas às Certificações, exigidas pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** e aos relatórios de auditoria especializada, contratada pelo prestador de serviços;
- Informações e recursos de Gestão, adequados ao monitoramento dos serviços prestados; e

f) A obrigação da empresa contratada de notificar a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** sobre a subcontratação de serviços relevantes para a Instituição;
g) A permissão de acesso do Banco Central do Brasil às seguintes informações:
- Contratos e acordos firmados para a prestação de serviços;
- Documentação e informações referentes aos serviços prestados;
- Os dados armazenados;
- As informações sobre processamentos;

- As cópias de segurança dos dados e das informações;
- Códigos de acesso aos dados e as informações; e

h) A adoção de medidas pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** obedecendo determinações do Banco Central do Brasil. A obrigatoriedade da empresa contratada de manter a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**; permanentemente, informada sobre eventuais limitações que possam afetar prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor;

i) O contrato deve, também, prever, para o caso de decretação de regime de resolução da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** pelo Banco Central do Brasil:

- A obrigação da empresa contratada para a prestação de serviços concede pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações, referentes aos serviços prestados, também, aos dados armazenados e às informações, sobre seus processos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada;
- A notificação prévia, deve obedecer pelo menos 30 (trinta) dias da data prevista para interrupção e se faz em caráter obrigatório pelo responsável do regime de resolução, sobre a intenção da empresa contratada de interromper a prestação de serviços, observando que:
    1) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, realizado pelo responsável pelo regime da resolução;
    2) A notificação prévia deve ocorrer, também, na situação em que a interrupção for motivada por inadimplência **da Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP;** e
    3) Os regimes de resolução são pautados pelo interesse público, pela preservação da estabilidade financeira e pela não interrupção do funcionamento de funções críticas para a economia real.

15. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**, tendo em vista a necessidade de agilizar o atendimento de seus cooperados e visando maior segurança e celeridade, fez a contratação do Serviço de Computação em Nuvem.

O contrato foi firmado com a empresa PRODAF INFORMÁTICA que, é a responsável pelos serviços de processamento e armazenamento de dados. Esta, por sua vez, possui contrato regular de Serviços junto a DEDALUS que, é detentora do espaço utilizado pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP**; para armazenar seus dados.

Por sua vez, o espaço objeto do contrato entre a DEDALUS x PRODAF INFORMÁTICA pertence à AMAZON WEB SERVICES.

16. PROCEDIMENTOS E INSTRUÇOES

Os procedimentos e as instruções encontram-se presentes na **Política de Segurança Cibernética,** visto que, estes representam as responsabilidades atribuídas à PRODAF INFORMÁTICA, 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 manutenção desta **Política de Segurança Cibernética**, 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 PRODAF INFORMÁTICA, 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 PRODAF INFORMÁTICA serão gerenciados e autorizados pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

Já o cadastro e criação de usuários para acessar o Cloud pelo GO-Global, serão realizados pela PRODAF INFORMÁTICA mediante solicitação da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

ADMINISTRAÇÃO DE FERRAMENTAS DE SEGURANÇA

A administração das ferramentas de segurança como firewalls, IDS/IPS, WAF e BACKUP será de responsabilidade da PRODAF INFORMATICA e da DEDALUS.

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 PRODAF INFORMÁTICA Cloud é virtualizado, a qualquer momento, sendo necessário, podem-se levar os snapshots dos servidores para qualquer datacenter da AMAZON no mundo, de forma a subir um novo ambiente de uso dos sistemas.

Para acesso às informações, basta o dirigente ou colaborador da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** autorizado, 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 PRODAF INFORMÁTICA, na administração do banco de dados e das ferramentas de segurança, a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** exige ser necessário à comunicação ao Diretor Responsável pela Política de Segurança Cibernética de qualquer ocorrência relevante, sendo este formalizado através de relatório elou declaração, contendo o registro dos incidentes verificados em testes ou os que efetivamente ocorreram.

17. ESTRUTURA DE GERENCIAMENTO

Embora a responsabilidade pela administração do banco de dados, bem como das ferramentas utilizadas para garantir a segurança desses dados, seja de responsabilidade da PRODAF INFORMÁTICA, a **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** deve garantir, como parte interessada, e se respaldar do atendimento da **Política de Segurança Cibernética** por parte da PRODAF INFORMÁTICA, através de relatórios e ou declarações emitidas por conta da verificação dos controles de Segurança Cibernética, cuja periodicidade poderá ser semestral ou anual.

Esse gerenciamento dos procedimentos e controles tem o objetivo de assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e modificados de acordo com objetivas e diretrizes estabelecidas na **Política de Segurança Cibernética** da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

Nesse sentido, a estrutura de gerenciamento deve prever o atendimento de padrão mínimo para conhecimento do Conselho de Administração ou Diretoria da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

18. GESTÃO DE ACESSO ÀS INFORMAÇOES

O acesso e cadastro de usuários, para acessar o Cloud pela GO-Global, será realizado pela PRODAF INFORMÁTICA mediante solicitação da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

Nesse sentido, caberá a esta a verificação do controle de acessos, por conta do monitoramento efetivado, que devem ser revistos, periodicamente, como forma de manter

as restrições e ou permissões, autorizadas pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP.**

PROTEÇÃO DO AMBIENTE

Considerando os serviços contratados de processamento e armazenamento em nuvem, torna-se prudente a apresentação de relatórios que demonstrem o efetivo monitoramento, aplicação de testes, tratamentos e resposta aos incidentes, quando de suas ocorrências, com vistas a minimizar o risco de falhas, favorecendo uma administração segura e transparente para ambas as partes. Esse relatório deve ser apresentado ao Conselho de Administração ou Diretoria da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** semestral ou anual.

SEGURANÇA FÍSICA E LÓGICA

Caberá à PRODAF INFORMÁTICA orientar se as condições e configurações das máquinas utilizadas pela **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** atendem aos propósitos estabelecidos para o bom desempenho e gerenciamento do serviço em nuvem.

No que tange ao seu quadro de colaboradores, a PRODAF INFORMÁTICA deve mantê-los atualizados e em constante treinamento, com vista a acompanhar as novidades acerca da Política de Segurança Cibernética e suas informações.

CONTINUIDADE DE NEGÓCIO

A estrutura de gerenciamento, em linhas gerais, visa garantir que a **Política de Segurança Cibernética** está sendo cumprida, com vistas a minimizar a ocorrência de fatores que coloquem em risco as atividades da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** e, consequentemente, a expondo em risco de descontinuidade.

Nesse sentido, para evitar a descontinuidade do negócio, torna-se necessário proceder com a análise dos incidentes, de forma que estes podem corresponder a um nível crítico e aceitável, visando verificar se estão em consonância com as medidas corretivas a serem adotadas.

19. COMUNICAÇÃO AO CONSELHO DE ADMINISTRAÇÃO OU DIRETORIA

Tendo em vista a complexidade que envolve o cumprimento da Política de Segurança Cibernética e a dificuldade da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** em validar ou não a efetivação dos procedimentos, é imperioso manter o Diretor Responsável pela **Política de Segurança Cibernética** informado sobre indícios de irregularidades verificadas, quando do cumprimento das suas determinações.

Assim, caberá à PRODAF INFORMÁTICA 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.

20. DOCUMENTOS DISPONÍVEIS AO BANCO CENTRAL

Os documentos, listados a seguir, devem ficar à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos, conforme Resolução **BACEN** nº 4.893 de 26/02/2021. São eles:

- Política de Segurança Cibernética;
- Ata de Reunião do Conselho de Administração ou Diretoria, implementando e aprovando a Política de Segurança Cibernética e suas revisões;
- Documento relativo ao Plano de Ação e de Resposta a Incidentes, com relatórios, visando a implementação da Política de Segurança Cibernética;
- Relatório Anual de Controles Internos e Gerenciamento de Risco no qual devem contemplar o item sobre a implementação do Plano de Ação e de Resposta a Incidentes;
- Documentação sobre os procedimentos relativos à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, prestados no exterior, “caso isso ocorra”;
- Contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controles, com vistas a assegurar a implementação e a efetividade da Política de Segurança Cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

21. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO, E REVISÃO DA POLÍTICA

O conteúdo desta **Política de Segurança Cibernética** aplica-se a todos os dirigentes, colaboradores e prestadores de serviços relevantes da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** no âmbito de suas atividades, atribuições e responsabilidades.

O Conselho de Administração ou Diretoria aprova a **Política de Segurança Cibernética** e se compromete com a melhoria contínua do disposto nesse documento normativo.

O conteúdo da **Política de Segurança Cibernética** é publicado, no site da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP,** e divulgado a todos os dirigentes, colaboradores, empresas contratadas de serviços cibernéticos, clientes e partes externas relevantes, para o necessário cumprimento.

É obrigação de todos os dirigentes e colaboradores conhecer e praticar às disposições desta **Política de Segurança Cibernética** e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

22. CONSIDERAÇÕES FINAIS

Esta **Política de Segurança Cibernética** será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia, sempre aprovada pelo Conselho de Administração ou Diretoria em Ata de Reunião Mensal.

Esta **Política de Segurança Cibernética** da **Cooperativa de Crédito de Servidores da UESC Ltda. – UESCOOP** foi aprovada na reunião do Conselho de Administração (CONAD) realizada em 07/11/2024 e o que dela decorre entrarão em vigor a partir desta data.

Registre-se, divulgue-se e cumpra-se.

Campus da UESC, 07 de novembro de 2024.

Conselho de Administração (CONAD)

José Montival de Alencar Júnior
Laudelino Quinto de Souza Júnior
Lino Arnulfo Vieira Cintra
Luis Frank Costa Ferreira
Luiz Henrique Farias dos Santos
Renata Vieira de Abreu
Vitoria Solange Coelho Ferreira
Cristiano Caetano da Silva
Edenilton Santana