2.8. POLÍTICA DE RISCO CIBERNÉTICO

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SERVIDORES PÚBLICOS DO PODER EXECUTIVO FEDERAL NO ESTADO DO ESPÍRITO SANTO - CREDES

SUMÁRIO

2. GERENCIAMENTO DE RISCOS 3
2.8. Política de Risco Cibernético 3
2.8.1. Princípios da Segurança da Informação 3
2.8.2. Objetivos 4
2.8.3. Controles da Segurança da Informação 5
2.8.4. Registros de Incidentes Relevantes 6
2.8.5. Divulgação da Política de Segurança Cibernética 6
2.8.6. Plano de Ação e de Resposta a Incidentes 7
2.8.7. Aplicação 8
2.8.8. Serviços de Rede 8
2.8.9. Armazenamento de Dados 9
2.8.10. Prodaf Informática LTDA 10
2.8.11. Relatório de Testes de Segurança das Informações 12
2.8.12. Continuidade dos Negócios 13
2.8.13. Responsabilidades CREDES 13
2.8.14. Considerações Finais 14

2. GERENCIAMENTO DE RISCOS

2.8. Política de Risco Cibernético

A política de segurança cibernética tem como objetivo atender a Resolução CMN – Conselho Monetário Nacional nº 4.893/21 e estabelecer os princípios, conceitos, valores e práticas, sobre os requisitos da contratação de serviços de processamentos e armazenamento de dados e de computação em nuvem que devem ser adotados pelos administradores, colaboradores da **Cooperativa de Economia e Crédito Mútuo dos Servidores Públicos do Poder Executivo Federal no Estado do Espírito Santo - CREDES**.

A Diretoria Executiva é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados, conforme as exigências do Banco Central do Brasil, considerando o porte e complexidade das operações da **CREDES,** bem como o fato da **CREDES** ter sua sede instalada em sala alugada em conjunto comercial.

2.8.1. Princípios da Segurança da Informação

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: controle de acesso e riscos cibernéticos. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

a) **Confidencialidade**: proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas, voluntária ou involuntariamente, dados restritos que deveriam ser acessíveis apenas por um determinado grupo de usuários.

b) **Integridade**: garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

c) **Disponibilidade**: prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

d) **Acesso controlado**: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

e) **Riscos Cibernéticos:** Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

2.8.2. Objetivos

A **CREDES** estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

a) Proteger o valor e a reputação da empresa;

b) Garantir a confidencialidade, integridade e disponibilidade das informações da **CREDES** contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

c) Identificar violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

d) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

f) Conscientizar, educar e treinar os colaboradores por meio dessa política, normas e procedimentos internos aplicáveis as suas atividades diárias;

g) Estabelecer e melhorar continuamente um processo de gestão de riscos de segurança cibernética.

2.8.3. Controles da Segurança da Informação

São exigidos alguns controles básicos de segurança da informação:

a) Política de segurança cibernética e plano de ação que precisam ser aprovados pela Diretoria Executiva;

b) Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;

c) Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;

d) Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis. e. classificação de dados ou de informações;

e) Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;

f) Implementação de programas de capacitação em segurança;

g) Comunicação para clientes e usuários;

h) Comprometimento da alta administração.

2.8.4. Registros de Incidentes Relevantes

O registro de incidentes toma uma importância muito grande nas normatizações relativas a esse assunto. É exigido a existência e formalização dos seguintes controles relacionados ao registro de incidentes:

- **a)** Identificação da causa e impactos dos incidentes;
- **b)** Planos de ação e planos de resposta para incidentes (*);
- **c)** Área específica para os registros de incidentes;
- **d)** Plano de continuidade de negócio e relatório anual – Andamento do plano de ação e resposta para incidentes;
- **e)** Revisão anual pela Diretoria Executiva;
- **f)** Tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

(*) Plano de resposta a incidentes de Segurança – Prodaf – V 1.4 de dez/2020 – documento que fará parte dessa política.

2.8.5. Divulgação da Política de Segurança Cibernética

A política de segurança cibernética será divulgada aos funcionários da instituição 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, podendo a seu critério, considerar tais informações no contrato de prestação de serviço, quando necessário.

A **CREDES** divulgará ao público resumo contendo as linhas gerais da política de segurança cibernética.

Os mecanismos para disseminação da cultura de segurança cibernética na **CREDES** são descritos a seguir:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações aos associados e usuários sobre precauções na utilização de produtos e serviços financeiros; e

c) o comprometimento da Diretoria Executiva com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

2.8.6. Plano de Ação e de Resposta a Incidentes

Fica estabelecido plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética que abrange:

I. as ações a serem desenvolvidas pela **CREDES** para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II. 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

III. a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Será elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, que deverá abordar, no mínimo:

I. a efetividade da implementação das ações a serem desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética

II. o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

III. os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV. os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório será apresentado a Diretoria Executiva até 31 de março do ano seguinte ao da data-base. O plano de ação e de resposta a incidentes mencionado deve ser aprovado pela Diretoria Executiva.

2.8.7. Aplicação

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

2.8.8. Serviços de Rede

A **CREDES** utiliza os drivers da rede que são segmentadas para garantir a segurança e desempenho.

O controle de acesso deverá assegurar que os usuários de computadores, conectados à rede, não comprometam a segurança de qualquer sistema operacional ou produto. Toda e qualquer alteração indevida deverá ser comunicada ao gerente para a tomada de decisão.

Além disso, todos os computadores/notebooks devem estar com antivírus corporativo devidamente instalados.

A inserção de qualquer nova informação, realizada por meio de dispositivos removíveis só será liberada mediante autorização do gerente. Antes de efetuar a liberação, deverá ser verificado se a estação de trabalho realmente possui antivírus instalado e atualizado.

O acesso a serviços computacionais deverá sempre ocorrer através de um procedimento seguro no qual o usuário conecta-se a um sistema de controle utilizando seu usuário e senha, devendo ser planejado para minimizar os riscos de acesso não autorizados.

O acesso às estações de trabalho de forma remota só deverá ocorrer mediante autorização do usuário da estação de trabalho, proporcionando assim o acesso remoto seguro.

Qualquer acesso remoto, que seja efetuado por terceiros utilizando programas não licenciados e/ou não autorizados pela **CREDES** será de responsabilidade do prestador de serviço.

Redes Wifi só serão permitidas com uma internet exclusiva para tal serviço. É totalmente proibido a utilização de Wifi conectada à mesma rede corporativa da **CREDES** sem que haja autorização prévia.

2.8.9. Armazenamento de Dados

A **CREDES** realiza o backup de servidor através de 2 HD's externos criando backups separado todos os dias. Um HD fica acoplado no servidor na segunda, quarta e sexta o outro na terça e quinta sendo assim alternados todos os dias. Assim, se houver necessidade de voltar o backup por algum motivo não haverá muitas perdas de arquivos. Nesses backups só terão arquivos apagados do servidor principal por um período de aproximadamente 10 a 15 dias.

Também é executado um backup incremental da pasta público do servidor principal que fica em um computador na rede. Neste backup ficam todos os arquivos contidos na pasta público, inclusive os que já foram apagados da pasta público principal. Lembrando que esse tipo de backup é vulnerável em caso de ataque de hackers ou em caso de queima de disco rígido. Total de 3 backups sendo 2 backups diários um sendo feito as 19:30 e outro a 23:00.

As informações operacionais, financeiras, contábeis, fiscais e indicadores são gerenciadas através do **Sistema Syscoop 32**, fornecido pela empresa Prodaf Informática.

Com isso seu armazenamento de dados (backup) é realizado de forma segregada a ser apresentada nos itens a seguir descritos.

2.8.10. Prodaf Informática LTDA

A Prodaf, através do Syscoop32, realiza o gerenciamento sistêmico e o armazenamento de dados, onde há 11 módulos integrados que controla toda a parte operacional, financeira e contábil da cooperativa:

- Administração;
- Contabilidade;
- Banco;
- Associado;
- Capital;
- Empréstimo;
- Conta Corrente;
- Convênio;
- Cobrança;
- Outras Contas;
- Extrato.

A **CREDES** optou por inserir as informações citadas em nuvem (cloud) através do contrato firmado com a Prodaf onde estão definidas as regras de segurança.

Os contratos com a Prodaf envolvem as empresas subcontratadas Dedalus, que representa a empresa Amazon no Brasil, a qual é responsável pela guarda dos dados gerados pela **CREDES**.

As principais qualidades que o sistema de gestão e a tecnologia Cloud, desenvolvidas pela Prodaf, agregam aos serviços oferecidos para **CREDES** são praticidade, agilidade e segurança.

A **CREDES** que está hospedada no cloud, nuvem da Prodaf, ambiente AWS – AMAZON, o nível de segurança ainda terá ferramentas de firewall, antivírus, ambos atualizados e monitorados diariamente, e análises constantes para detecção de possíveis ataques cibernéticos.

Com relação à política de back-up o ambiente cloud da Prodaf, tem Snaphots dos servidores, que são a imagem idêntica dos mesmos, armazenados 3 por dia. Com essas imagens é possível restaurar o servidor com todas as configurações e discos

Além dos Snaphots, o sistema Prodaf disponibiliza para a **CREDES** a ferramenta Bacula, onde há back-ups diários de arquivos, (back-up granular), das bases de dados da cooperativa, Banco Sybase, armazenados por 90 dias no S3/GLACIER (repositórios da AMAZON).

Os servidores são numerados e há um para cada serviço: internet, banco de dados, e-mail etc. Quando se conecta a um serviço, o computador acessa essa porta e usa um protocolo (essencialmente, um arquivo de texto descrevendo a comunicação entre as duas partes) para lidar com o servidor.

Os conteúdos das nuvens são mediados para o usuário da **CREDES** por meio da internet. O protocolo usado para acessar dados é o HTTP (o mesmo para acessar um site qualquer). Usando o protocolo e o domínio, se obtém exatamente na máquina com seus dados.

Para garantir a segurança, existe a barreira de login e senha e, servidores avançados, como o contratado pela **CREDES**, também criptografam a comunicação com os associados. Além disso, toda informação enviada é particionada em vários pedaços para confundir um possível ataque hacker. Essa divisão não precisa ser necessariamente dentro do mesmo data center.

2.8.11. Relatório de Testes de Segurança das Informações

Sempre que solicitado pela **CREDES**, o departamento de TI da Prodaf, realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos colaboradores, individualização dos usuários, dentre outros.

Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes pontos:

a) Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;

b) Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;

c) Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

d) Criação de plano de resposta e recuperação de incidentes que contenha comunicação interna e externa, se necessário. Serão realizados testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;

e) Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas na **CREDES** como evidência em eventuais questionamentos internos ou de órgãos reguladores.

2.8.12. Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação, é implementado para minimizar os impactos, e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através de: combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

2.8.13. Responsabilidades CREDES

A **CREDES** poderá obter dados cadastrais de seus associados, em algumas situações específicas, tal como via importação cadastral (realizada mensalmente através do sistema nuvem Prodaf Informática) possibilitando atualização de dados cadastrais dos associados. Os dados fornecidos pelos associados serão mantidos em absoluto sigilo e, por esta razão, a **CREDES** assegura que os mesmos não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

Além das disposições contidas neste documento, a **CREDES** afirma a sua conduta ética obrigando-se a cumprir, com rigor, as disposições legais vigentes no Brasil que tratam da privacidade, sigilo e segurança das informações que receber de seus associados, com a finalidade maior de resguardar os direitos dos mesmos.

O principal objetivo dessa política é continuar demonstrando aos associados a forma ética aplicada pela **CREDES** em seus relacionamentos, sempre no intuito de buscar o melhor atendimento.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Periodicamente, os acessos concedidos devem ser revistos pelo responsável da **CREDES**.

O identificador da rede e dos sistemas (login/senha) é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Seguem alguns cuidados que devem ser tomados:

a) Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não informar a ninguém e não a anotar em papel;
b) Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
c) Selecionar senhas de qualidade, que sejam de difícil adivinhação;
d) Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
e) Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

2.8.14. Considerações Finais

A **CREDES** deverá: designar diretor responsável pelo cumprimento da Política de Risco Cibernético.

A Política de Risco Cibernético será aprovada e revisada, a cada 2 (dois) anos, ou quando houver exigências / alterações dos órgãos normativos pela Diretoria Executiva da **CREDES** que deverá assegurar sua divulgação, bem como manter documentação relativa à disposição do Banco Central do Brasil.

.

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos. Estrutura completa no **ANEXO I - ESTRUTURA DE CONTROLES INTERNOS E GERENCIAMENTO DE RISCOS** destacada no grupo: 1. Estrutura, item: **1.1 – ESTRUTURA DE CONTROLES INTERNOS**.

Vitória, 27 de dezembro de 2023.

VINICIUS BIS LIMA FALQUETO:05566119778
Assinado de forma digital por VINICIUS BIS LIMA FALQUETO:05566119778
Dados: 2023.12.27 14:36:39 -03'00'

Vinicius Bis Lima Falqueto
Diretor Presidente

DEULIRA ELIZEU DA COSTA:19027001634
Assinado de forma digital por DEULIRA ELIZEU DA COSTA:19027001634
Dados: 2023.12.27 13:09:53 -03'00'

Deulira Elizeu da Costa
Diretora Financeira