2.8. POLÍTICA DE RISCO CIBERNÉTICO

MANUAL DE CONTROLES INTERNOS

SUMÁRIO

2.8. Política de Risco Cibernético

A política de segurança cibernética tem como objetivo atender à Resolução nº 4.893 de 26 de fevereiro de 2021 do Banco Central do Brasil (BACEN) 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 adotadas pela **COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS FUNCIONÁRIOS DO GRUPO COSAN - BARRACRED COSAN**.

O conselho de administração 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 **BARRACRED COSAN** e o fato da cooperativa utilizar a rede de computação da empresa mantenedora.

2.8.1. Objetivos

A **BARRACRED COSAN** 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 **BARRACRED COSAN**, 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 de política de Risco Cibernético, normas e procedimentos internos aplicáveis as suas atividades diárias;

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

2.8.2. 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 voluntaria ou involuntariamente dados restritos e 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.

2.8.3. Controles da Segurança da Informação

São exigidos alguns controles básicos de segurança da informação:

a) política de segurança cibernética que precisa ser aprovado pelo conselho de administração;

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, 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:

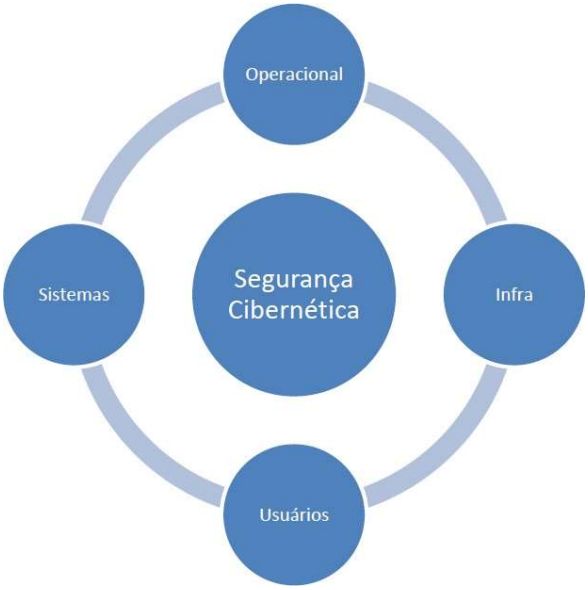
a) identificação da causa e impactos dos incidentes;
b) área específica para os registros de incidentes;
c) plano de continuidade de negócio e relatório anual;
d) revisão anual pela direção ou conselho administração;
e) tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

2.8.5. 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.

2.8.6. Procedimentos para Proteção da Informação

Os procedimentos de segurança devem atender os seguintes componentes na figura abaixo:



2.8.6.1. Infraestrutura Cosan

A **BARRACRED COSAN** é uma cooperativa fechada aos colaboradores do Grupo Cosan e por estar alocada dentro da empresa, por questões de eficiência e segurança, é utilizada toda a infraestrutura da empresa mantenedora, que possui governança de ponta, gerenciada pelo *framework* de segurança corporativo do grupo:

i. Restauração de cópia de segurança;
ii. Due Diligence Infra;
iii. Teste de segurança e continuidade;
iv. Controle de incidentes.

a. Data Center

As aplicações Savemais - empresa terceirizada contratada -, seus bancos de dados, bem como as demais ferramentas administrativas (e-mail, pacote office, entre outros), estão alocados no Datacenter Cosan, e possui os seguintes itens de segurança:

i. Sistema anti-incêndio;

ii. Controle de acesso;

iii. Sala climatizada;

iv. Monitorada tanto lógica como fisicamente 24x7;

v. Câmeras de segurança.

b. Backup

Os backups dos bancos de dados e das aplicações são gravados. Na política de armazenagem da empresa mantenedora (Raizen/Cosan) está descrito da seguinte forma:

c. Aplicação

i. Backup diário armazenado por 7 dias;
ii. Semanal armazenado por 36 dias.

d. Banco de Dados

i. Backup diário armazenado por 14 dias;
ii. Semanal armazenado por 36 dias.

e. Servidores

Os servidores das aplicações e bancos de dados também são gerenciados pelo departamento de TI da Cosan, seguindo as melhores práticas de mercado, contando com o monitoramento de performance e vulnerabilidades, proteção antivírus e WAF (*Web Application Firewall*), além de sistema de controle para ataques Dos/DDoS (*Distributed Denial-of-Service*) quando abertos para ambiente externo.

Quanto às informações guardadas de forma local, em computadores também que são de propriedade da mantenedora, a **BARRACRED COSAN** adota o procedimento de backup diário por meio de Hard Disk (HD) externo, no qual o mesmo está armazenado fora das dependências da mesma, em local seguro e inviolável. Este mesmo procedimento é realizado para outros equipamentos que eventualmente sejam de propriedade da **BARRACRED COSAN**, garantindo assim sua recuperação caso necessário.

O responsável pela guarda será o coordenador e/ou contadora, por meio de planilha de controle sobre o último backup realizado.

2.8.6.2. Sistema Operacional Savemais

A **BARRACRED COSAN,** mantém contrato de prestação de serviços com a empresa SAVEMAS Tecnologia - Contrato De Licença De Uso De Software E Outras Avenças - que, dentre as atividades contratadas, está a garantia do serviço de suporte à **BARRACRED COSAN.** Uma vez solicitado o serviço de suporte, a SAVEMAIS diagnosticará o problema e elucidará as dúvidas conforme as especificações da **BARRACRED COSAN**. Considerando a prioridade de cada problema, a SAVEMAIS terá os seguintes prazos máximos para prestar tal informação a **BARRACRED COSAN**:

Prioridade 1 – até 4 (quatro) horas. Nesta prioridade estão incluídos:

a) mau funcionamento que impossibilite completamente o uso do sistema Savemais;

b) mau funcionamento que impossibilite a execução de atividades imprescindíveis e de missão crítica que não possam ser executadas adequadamente de outra forma;

c) mau funcionamento que permita qualquer vulnerabilidade relacionada com a segurança das informações ou de acesso ao sistema Savemais;

d) mau funcionamento que cause perdas de dados registrados no sistema Savemais.

Prioridade 2 – até 1 (um) dia útil. Nesta prioridade estão incluídos:
a) mau funcionamento que represente significativa degradação na performance de processamento no sistema Savemais;
b) mau funcionamento que provoque falhas frequentes, mas sem perda de dados registrados no sistema Savemais.

Prioridade 3 – até 10 (dez) dias úteis. Estão incluídas nesta prioridade qualquer solicitação que não se enquadre nas hipóteses anteriores (Prioridades 1 e 2).

Os prazos definidos acima passam a contar da data e hora do recebimento da solicitação do serviço e de todos os insumos como relatórios, base de dados, memória de cálculo ou planilhas que tenham sido solicitados pela SAVEMAIS Tecnologia, respeitando o intervalo de funcionamento horário de funcionamento de sua equipe técnica de atendimento.

No contrato ainda há previsão da cláusula de confidencialidade sendo que a SAVEMAIS Tecnologia deverá manter sigilo sobre toda espécie de informação a que tiver acesso, inclusive dados pessoais de cooperados e colaboradores, não podendo divulgá-las a quem quer que seja ou por qualquer meio, nem tampouco fazer uso das mesmas, para finalidade diversa da prevista no contrato, respondendo por tal obrigação, inclusive em relação a seus funcionários e prepostos,sendo que uma vez caracterizada a quebra do sigilo de informações por parte da SAVEMAIS Tecnologia, a **BARRACRED COSAN** poderá adotar as medidas cabíveis,visando preservar seus direitos e informações, bem como fará jus à indenização cabível, na forma da lei vigente.

A **BARRACRED COSAN** realiza *Due diligence* na SAVEMAIS Tecnologia, anualmente, e sempre que entender necessária tal ação.

2.8.6.3. Testes de Segurança das Informações

Periodicamente são realizados *Pentests* (Penetration Test – teste de invasão), 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 TI da Cosan juntamente com a equipe da Savemais Tecnologia, buscando 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 um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário e terá 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 **BARRACRED COSAN** como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

2.8.7. Estratégias e Governança

O GRUPO COSAN, responsável pelos serviços de processamento e armazenamento de dados de cooperados, colaboradores, parceiros e prestadores de serviços da BARRACRED COSAN, dispõe de equipe de Controle, Risco e Governança de Tecnologia que administra as práticas e políticas de Segurança da Informação em todo o Grupo, inclusive de dados disponibilizados pela BARRACRED.

Um time de especialistas altamente capacitados, atua no desenvolvimento de meios cada vez mais eficientes para garantir a proteção dos negócios das empresas do GRUPO COSAN, contra ameaças cibernéticas, humanas, naturais ou de natureza geopolítica.

Dentre as atividades deste time, está o fornecimento de diretrizes quanto à gestão dos riscos e ativos de segurança da informação, com foco nas áreas organizacionais abaixo:

- Risco em aplicações;
- Arquitetura, governança e conformidade;
- Resiliência dos negócios;
- Segurança da informação;
- Resposta a incidentes;
- Gestão de acesso e identidade;
- Gestão de Segurança de operações;
- Privacidade de dados;
- Riscos de terceiros;
- Gestão de Continuidade de Negócios.

2.8.8. Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo à 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 da 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.

2.8.9. Responsabilidades da mantenedora

A **BARRACRED COSAN** poderá obter dados cadastrais de seus associados, em algumas situações específicas, tais como associação, atualização de dados, cadastro de endereço de e-mail, participação em promoções ou sorteios.

Os dados fornecidos pelos associados serão mantidos em absoluto sigilo e, por esta razão, a **BARRACRED COSAN** 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 **BARRACRED COSAN** 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 **BARRACRED COSAN** 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 gestor da **BARRACRED COSAN**.

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 contá-la a ninguém e não anotá-la 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).

Adicionalmente às presentes instruções, todos os Colaboradores da BARRACRED COSAN, recebem, constantemente, treinamentos específicos relativos à Segurança da Informação. Ainda, estão formalmente cientificados dos riscos pelo descumprimento das regras deste tema, o qual gerará consequências contratuais, civis e penais.

2.8.10. Considerações Finais

A Política de Risco Cibernético será aprovada e revisada, periodicamente, pelo conselho de administração da **BARRACRED COSAN**.

A **BARRACRED COSAN** possui diretor responsável pelo cumprimento da Política de Risco Cibernético, o qual observa, dentre suas atribuições, a divulgação interna e externa das diretrizes constantemente atualizadas. Ainda, é responsável pela manutenção da documentação correlata, que está à disposição do Banco Central do Brasil.

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos. A estrutura completa se encontra no ANEXO **I –**

ESTRUTURA DE CONTROLES INTERNOS E GERENCIAMENTO DE RISCOS destacada no grupo, 1. Estrutura, item: **1.1 – ESTRUTURA DE CONTROLES INTERNOS**.

2.8.11. Comunicação

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail privacidade@barracred.com.br

Esta política foi aprovada em reunião do Conselho de Administração realizada em 23 de julho de 2021.