FUNDCOOP

PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES
Exercício de 2024

Cooperativa de Economia e Crédito Mútuo dos Empregados da Tupy Minas Gerais Ltda e Nemak Alumínio do Brasil Ltda –FUNDCOOP atendendo ao art. 6º da Resolução CMN nº 4.893/2021, estabeleceu Plano de Ação e de Resposta a Incidentes relativo ao **exercício de 2024**, abrangendo:

- Ações que foram desenvolvidas pela Cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes de segurança cibernética previstas;

- As rotinas, os procedimentos, os controles e as tecnologias foram utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança e contendo:

I - Os incidentes relevantes relacionados com ambiente cibernético ocorridos no período;

II - Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

1. **Incidentes de Segurança**

Um conjunto amplo de regras internas foi designado, abrangendo as áreas:

- Uso dos Recursos de Tecnologia;
- Uso do Computador;
- Uso da Internet;
- Uso do Correio Eletrônico;
- Uso do Telefone;
- Linhas Gerais do Comportamento Seguro.

Os incidentes de segurança foram classificados conforme sua relevância e de acordo com a classificação dos Dados e Informações envolvidos; e o impacto na continuidade dos negócios da Cooperativa nas seguintes categorias:

1.1 Baixo – causa lentidão ou indisponibilidade no acesso a sistemas e/ou Dados, sem, entretanto, afetar o atendimento ao cooperado ou a realizações de transações;

1.2 Médio – causa lentidão no atendimento ao cooperado, podendo, ainda, impedir o acesso a alguns serviços não essenciais; e

1.3 Alto – impede o atendimento ao cooperado e/ou a realização de transações.

2. Ações de Prevenção

Foram criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da Cooperativa por meio das seguintes ações:

2.1 Mantidos inventários atualizados de hardware e software, bom como verificado com frequência para identificar elementos estranhos à cooperativa. Por exemplo, computadores não autorizados ou software não licenciado;

2.2 Mantidos os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;

2.3 Monitorados diariamente, as rotinas de backup, executando testes regulares de restauração dos dados;

2.4 Realizados análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura;

2.5 Periodicamente testados os procedimentos de resposta a incidentes simulando os cenários.

3. Tratamento de Incidentes de Segurança da Informação

3.1 Foram monitorados os incidentes relativos a interrupções de sistema não planejadas e que ocorrem de várias naturezas e afetam os negócios da Cooperativa, como por exemplo:

• Queda de energia elétrica;

• Falha de um elemento de conexão (cabeamento);

• Servidor fora do ar;

• Ausência de conexão com internet;

• Sabotagem (interna);

• Indisponibilidade de acesso a Cooperativa;

• Ataques de hacker.

3.2 Qualquer Colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

3.3 O Diretor responsável pela Política de Segurança Cibernética deverá avaliar o impacto do incidente nos diversos riscos envolvidos.

3.4 A recuperação nessa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada.

3.5 A retomada desta fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar à operação normal, reconstrução de eventuais sistemas, eventuais mudanças e medidas de prevenção.

3.6 Os responsáveis pelos Dados/Informações na cooperativa devem supervisionar e monitorar com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

4. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios da Cooperativa relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, retornando à operação 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. Referido processo considera, ao menos, os seguintes cenários para a realização de testes de continuidade de negócios:

a) Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e /ou a extração de Informações e Dados internos e/ou confidenciais do ambiente lógico da Cooperativa;

b) Realização de testes de intrusão a base de dados contendo Informações Sensíveis da Cooperativa;

c) Tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;

Ainda no tocante à continuidade de negócios, a Cooperativa deve adotar procedimentos para o gerenciamento de riscos, considerando:

a) o tratamento previsto para mitigar os efeitos dos incidentes relevantes para as atividades da Cooperativa e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

b) o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, relacionados com o ambiente cibernético; e

c) a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes relacionados com o ambiente cibernético que configurem uma situação de crise pela FUNDCOOP, bem como das providências para o reinício das suas atividades;

d) Estabelecer e documentar os critérios que configurem uma situação de crise para a FUNDCOOP.

5. Registros de Eventos Ocorridos

No período de 01 de janeiro de 2024 a 31 de dezembro de 2024 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

Não foi detectado por qualquer colaborador incidente de segurança da informação que necessitasse ser levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

A Cooperativa estabeleceu Plano de Ação e de Resposta a Incidentes, sendo parte integrante da Política de Segurança Cibernética aprovada e atualizada em 20/05/2024.

Diretor Responsável

Foi designado diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

Betim/MG, 31 de dezembro de 2024.

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