



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

A Cooperativa elaborou o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, contemplando, no mínimo, as seguintes informações:

I - Efetividade

A implementação das ações foi desenvolvida para adequar a estrutura organizacional e operacional da cooperativa e aos princípios e às diretrizes da política de Segurança Cibernética.

a) Ações de Prevenção

Os mecanismos de monitoramento de todas as ações de proteção foram implementadas e garantiram o bom funcionamento e efetividade da segurança cibernética da Cooperativa por meio das seguintes ações:

- foram mantidos inventários atualizados de hardware e software, bem verificados com frequência para identificar elementos estranhos à cooperativa. Por exemplo, computadores não autorizados ou software não licenciado;
- os sistemas operacionais e softwares de aplicação foram atualizados e instalados e com as atualizações sempre disponibilizadas;
- diariamente as rotinas de backup foram executadas com testes regulares de restauração dos dados;
- foram realizadas análises de vulnerabilidades na estrutura tecnológica, periódica ou sempre que houve mudança significativa em tal estrutura;
- Periodicamente foram testados os procedimentos de resposta a incidentes simulando os cenários.

II - Resumo dos Resultados Obtidos

Os resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias utilizados na prevenção e na resposta a incidentes considerou:

a) Tecnologia – Backups

A FACIL INFORMÁTICA (CONTRATADA) manteve cada um dos backups efetuados sob a política cíclica de armazenamento o que garantiu 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 99,95% de disponibilidade), inclusive nos sábados, domingos e feriados nacionais;
- os backups foram testados semanalmente (restauração em ambiente de homologação) para garantindo sua integridade;
- A CONTRATADA disponibilizou, sob demanda, arquivo contendo o backup lógico do banco de dados da Cooperativa (CONTRATANTE). Por questões de segurança, o arquivo foi disponibilizado através de conexão criptografada, no formato EXPDP do Oracle, compactado através de ZIP e protegido por uma chave de segurança.

III - Incidentes relevantes

Foram analisados os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

Não houveram no período incidentes relevantes relacionados com o ambiente cibernético 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: Baixo, Médio e Alto.

IV - Continuidade de Negócios

Foram realizados no período, testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes prevenindo eventuais perdas de ativos da informação após um incidente crítico, com monitoramento de:

a) Testes

- testes de intrusão na base de dados contendo Informações Sensíveis da Cooperativa;
- tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;



COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS EMPREGADOS DA TEKSID DO BRASIL LTDA., NEMAK ALUMÍNIO DO BRASIL LTDA. E TUPY MINAS GERAIS LTDA.,
Rua Senador Giovanni Agnelli, 230, Distrito Industrial Paulo Camilo Norte – Betim/MG Telefone: 31-33168380 CEP: 32681-080 Site: www.cooptek.com.br - CNPJ: 04.249.235/00001-72

- prazo estipulado para reinício e normalização das atividades ou dos serviços relevantes interrompidos, relacionados com o ambiente cibernético;
- análise de impacto nos negócios e testes periódicos de recuperação de desastres.

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

a) 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) 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 COOPTTEK, bem como das providências para o reinício das suas atividades.

V - Tratamento de Incidentes não Planejados de Segurança da Informação

Não houveram no período incidentes não planejados que afetassem a continuidade dos negócios da Cooperativa, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão (cabramento);
- Servidor fora do ar;
- Ausência de conexão com internet;
- Sabotagem (interna);
- Indisponibilidade de acesso a Cooperativa;
- Ataques de hacker.

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.



COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS EMPREGADOS DA TEKSID DO BRASIL LTDA., NEMAK ALUMÍNIO DO BRASIL LTDA. E TUPY MINAS GERAIS LTDA.,
Rua Senador Giovanni Agnelli, 230, Distrito Industrial Paulo Camilo Norte – Betim/MG Telefone: 31-33168380 CEP: 32681-080 Site: www.cooptek.com.br - CNPJ: 04.249.235/00001-72

A Cooperativa estabeleceu Plano de Ação e de Resposta a Incidentes semestralmente, sendo parte integrante da Política de Segurança Cibernética, aprovada/atualizada em Ata de Diretoria de 30/09/2022.

Betim 31 de dezembro de 2022.

German Bretas Lage
Diretor Administrativo
Responsável pela Política de Segurança Cibernética