Relatório de Incidentes – Exercício de 2024

1. Objetivo e Escopo

Este relatório tem como finalidade apresentar, de forma abrangente e estruturada, os resultados do processo de monitoramento, análise e tratamento de incidentes relacionados à segurança cibernética, riscos operacionais e falhas de continuidade de negócios ocorridos no período de 01 de janeiro a 31 de dezembro de 2024. O documento reflete a atuação coordenada entre as linhas de defesa da organização, em especial as áreas de Tecnologia, Riscos, Compliance e Operações, assegurando resposta tempestiva e aderente às melhores práticas regulatórias.

O escopo inclui:

- Monitoramento de ameaças cibernéticas, como tentativas de intrusão, phishing e malware;

- Registro e tratamento de falhas operacionais, oriundas de erro humano, falha sistêmica ou de terceiros;

- Avaliação de interrupções e indisponibilidades em serviços críticos à operação;- Análise de impactos financeiros, reputacionais, legais e regulatórios dos eventos identificados;

- Verificação da eficácia dos planos de resposta a incidentes e continuidade de negócios;

- Garantia do cumprimento das obrigações regulatórias estabelecidas pelas Resoluções BCB nº 85/2021, BCB nº 368/2024 (em substituição à Resolução CMN nº 4.893/2021), CMN nº 4.557/2017, Resolução CVM nº 50/2021, Resolução CVM nº 35/2021, Instrução CVM nº 505/2011 e LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

2. Sumário Executivo

No período analisado, a instituição manteve operação normal, sem registro de incidentes classificados como relevantes para fins de reporte regulatório. Os eventos identificados foram isolados, de baixa criticidade, e prontamente tratados. Destaca-se a efetividade dos controles implementados, o engajamento das áreas envolvidas e a resiliência dos processos críticos frente a ameaças cibernéticas e falhas operacionais.

3. Metodologia de Monitoramento

A abordagem adotada combina automação, análise especializada e governança estruturada. As atividades de monitoramento e resposta a incidentes foram conduzidas conforme os seguintes pilares:

- Ferramentas de monitoramento contínuo (SIEM, IDS/IPS, antivírus corporativo com análise de comportamento);

- Análise diária de alertas de segurança e eventos operacionais;

- Registro de todos os eventos em sistema de ticket com categorização e priorização conforme matriz de risco;

- Reuniões quinzenais do comitê de eventos com participação das áreas de Riscos, Compliance, TI e Jurídico;

- Reavaliação de controles preventivos e planos de resposta com base em lições aprendidas;

- Simulações periódicas de incidentes e testes de resiliência operacional.

4. Eventos Monitorados

A ActivTrades CCTVM mantém um processo contínuo de identificação, registro e análise de eventos relevantes que possam representar riscos operacionais, cibernéticos ou de continuidade. Abaixo estão listadas as categorias de eventos monitorados pela instituição, acompanhadas de sua avaliação de risco e das respectivas ações adotadas para mitigação ou aprimoramento de controles internos.

Tipo de Evento	Avaliação de Risco	Ação Tomada
Tentativas de phishing	Baixo – mitigado por bloqueios automáticos e awareness	Reforço em campanhas educativas e simulação de phishing interno
Falhas sistêmicas de login	Muito baixo – tratadas sem impacto ao cliente	Aplicação de patches corretivos e revisão de autenticação
Incidentes operacionais internos	Moderado – erro humano, sem impacto financeiro	Aprimoramento de processos e capacitação da equipe envolvida
Eventos de quase perda (near misses)	—	—
Perdas financeiras	—	—
Vazamento de dados	—	—

5. Conclusão

No período analisado, a instituição operou dentro da normalidade, sem registro de incidentes que se enquadrassem nos critérios de relevância estabelecidos pelas normas do Banco Central do Brasil, como aqueles com impacto significativo sobre clientes, sistemas críticos, obrigações legais, reputação institucional ou continuidade dos negócios.

Foram monitoradas e analisadas categorias específicas de eventos, incluindo: tentativas de phishing, falhas sistêmicas de login, incidentes operacionais internos, eventos de quase perda (near misses), perdas financeiras e vazamento de dados.

Destaca-se a efetividade dos controles internos e dos mecanismos de monitoramento, detecção e resposta a incidentes, além do engajamento ativo das áreas de Riscos, Tecnologia da Informação, Compliance e Operações, que atuaram de forma coordenada no cumprimento dos protocolos internos.

Por fim, ressalta-se a resiliência da infraestrutura crítica da instituição, resultado da aplicação consistente de políticas de segurança, da maturidade nos processos operacionais e do investimento contínuo em governança, prevenção de riscos e cultura organizacional voltada à integridade e continuidade dos negócios.

6. Declaração Formal

Declaramos, para os devidos fins e em conformidade com as exigências regulatórias aplicáveis, que não foram registrados, durante o período de 01/01/2024 a 31/12/2024, incidentes relevantes de natureza operacional, cibernética ou de continuidade de negócios que configurassem obrigação de reporte ao Banco Central do Brasil, conforme os critérios estabelecidos nas seguintes normativas:

- Resolução BCB nº 85/2021 – que dispõe sobre os requisitos de segurança cibernética aplicáveis às instituições autorizadas a funcionar pelo Banco Central;

- Resolução BCB nº 368/2024 – que estabelece requisitos de governança, controles internos e gerenciamento de riscos, substituindo a Resolução CMN nº 4.893/2021 para fins regulatórios;

- Resolução CMN nº 4.557/2017 – que estabelece a estrutura de gerenciamento de riscos e de capital;

- Resolução CVM nº 50/2021 – exige que prestadores de infraestrutura reportem imediatamente falhas operacionais ou incidentes relevantes à CVM, informando impactos e medidas adotadas;

- Resolução CVM nº 35/2021 – obriga agentes de custódia e escrituração a comunicar incidentes que afetem a segurança ou integridade de informações ou serviços prestados;

- Instrução CVM nº 505/2011 – prevê que corretoras mantenham controles operacionais eficazes e comuniquem à CVM falhas relevantes que impactem o mercado ou os investidores;

- LGPD (Lei nº 13.709/2018) – determina o reporte de incidentes de dados pessoais à ANPD, titulares e, quando aplicável, à CVM, caso haja risco ou dano relevante.

A instituição manteve, durante todo o período, controles efetivos, mecanismos adequados de prevenção e resposta, bem como monitoramento contínuo de eventos, garantindo a conformidade com o arcabouço regulatório vigente e a preservação da integridade dos seus processos críticos.