POLÍTICA CORPORATIVA DE GERENCIAMENTO DE INCIDENTES E PLANO DE RESPOSTA A INCIDENTES – MONCALIERI CAPITAL

1. Objetivo

Estabelecer diretrizes e procedimentos formais para o gerenciamento de incidentes na MONCALIERICAPITAL, garantindo resposta rápida e eficaz a quaisquer ocorrências que ameacem a confidencialidade, integridade ou disponibilidade de ativos de informação e serviços financeiros. A política visa minimizar impactos operacionais, financeiros e reputacionais, preservando a continuidade dos negócios e cumprindo requisitos legais e regulatórios.

2. Escopo

Aplica-se a todos os incidentes que afetem recursos da MONCALIERICAPITAL, incluindo: incidentes de segurança da informação (acessos indevidos, vazamento de dados, ransomware); incidentes tecnológicos (falhas de sistemas, rede ou nuvem); incidentes cibernéticos (DDoS, malware, phishing); incidentes regulatórios (violação de normas do setor financeiro); incidentes operacionais e de terceiros (falha de fornecedor crítico, interrupção de serviços); e incidentes de dados pessoais (violação de dados pessoais conforme LGPD).

O escopo cobre toda a organização, seus empregados, sistemas internos e prestadores de serviço terceirizados críticos. Inclui detecção, registro, resposta, comunicação e análise pós-incidente de cada evento relevante.

3. Fundamentos Normativos e Doutrinários

A política fundamenta-se em padrões e regulamentos nacionais e internacionais reconhecidos, visando aderência às melhores práticas e exigências legais, entre eles:

- ✓ ISO/IEC 27035 (gestão de incidentes de segurança da informação).
- ✓ ISO/IEC 27001 (especialmente controles do Anexo A.16 sobre gestão de incidentes).
- ✓ NIST SP 800-61 (guia de manejo de incidentes de segurança).
- ✓ Resolução CMN nº 4.893/2021 do Banco Central (política de segurança cibernética e plano de resposta a incidentes para instituições financeiras).
- ✓ Lei Geral de Proteção de Dados (Lei 13.709/2018) – enfatizando as obrigações de notificação de incidentes de segurança que envolvam dados pessoais, conforme art. 48.

Outros referenciais incluem práticas de gestão de riscos de tecnologia e frameworks de resposta a incidentes reconhecidos pelo mercado financeiro.

4. Princípios Orientadores

Tais princípios estão alinhados às normas ISO/IEC e NIST, que recomendam ciclo de vida abrangente de incidentes bem como aos requisitos da Resolução CMN (prevenção, registro e análise de causas).

- ✓ Prevenção: implementar controles de segurança proativos (p. ex. autenticação forte, criptografia, atualizações regulares, segmentação de rede) para reduzir a probabilidade de incidentes.
- ✓ Detecção: manter monitoramento contínuo e sistemas de alerta (SIEM, IDS/IPS, logs) para identificação oportuna de ameaças e anomalias.
- ✓ Resposta: agir rapidamente para conter e erradicar incidentes, seguindo procedimentos predefinidos e designando equipes de resposta (CSIRT) internas ou externas.

- ✓ Recuperação: restaurar serviços afetados à operação normal com segurança, apoiada por planos de continuidade e backup comprovados.
- ✓ Melhoria Contínua: após cada incidente relevante, analisar lições aprendidas para ajustar controles, processos e treinamento, fechando o ciclo PDCA de segurança.

5. Integração com Políticas e Controles Afins

Esta política de incidentes integra-se de forma sistêmica às demais normas internas da MONCALIERICAPITAL: O plano de resposta a incidentes integra-se diretamente ao Plano de Continuidade de Negócios (PCN), garantindo que a recuperação de serviços críticos ocorra em conformidade com os RTOs e RPOs definidos. Durante incidentes de grande impacto, o acionamento do PCN é coordenado em conjunto com o CSIRT e as áreas de negócio, assegurando alinhamento entre contenção, comunicação e retomada operacional.

- ✓ Política de Segurança da Informação – compartilhando objetivos de confidencialidade, integridade e disponibilidade; incidentes reportados alimentam o processo de gestão de riscos de segurança.
- ✓ Política de Continuidade de Negócios e DRP – cenários de incidentes críticos são contemplados nos testes de continuidade (Conforme Res. CMN); ações de recuperação de incidentes utilizam procedimentos do DRP.
- ✓ Política de Gestão de Riscos – avaliação de impacto de incidentes contribui para a revisão de riscos tecnológicos e operacionais.

  A governança corporativa promove diretrizes coerentes entre as políticas, evitando lacunas entre resposta a incidentes,

continuidade de negócios e gestão de risco operacional e tecnológico.

6. Estrutura de Governança e Responsabilidades

A alta administração da MONCALIERICAPITAL é responsável por aprovar e dar suporte à política de incidentes. A instituição designa um responsável executivo (conforme art. 7º da Resolução CMN 4.893) pelo programa de segurança cibernética e pela execução do plano de resposta a incidentes, normalmente o Diretor de Segurança da Informação ou equivalente. Este executivo coordena o Escritório de Segurança da Informação (CISO office) e a equipe de resposta a incidentes (CSIRT), definindo papéis claros:

Responsável Formal: A Diretoria de Segurança da Informação é a responsável oficial pela implementação e manutenção deste plano, conforme designação formal nos registros corporativos. O Diretor de Segurança ou CISO atua como ponto focal perante a alta administração, reguladores e demais stakeholders internos ou externos.

- ✓ Gestor de Incidentes/CSIRT Leader: supervisiona a triagem e mitigação de cada incidente, convoca especialistas técnicos e avalia escalonamentos.
- ✓ Responsável de Contato com Autoridades (Compliance): providencia comunicação a órgãos reguladores (BACEN, ANPD) e autoridades de segurança.
- ✓ Encarregado de Dados (DPO): conduz notificações a titulares e ANPD nos incidentes que envolvam dados pessoais.
- ✓ Gerentes de Negócios e Operações: notificam o CSIRT sobre problemas em seus processos e executam ações de contenção local.

- ✓ Colaboradores e Terceirizados: reportam incidentes suspeitos imediatamente, seguindo os canais e formulários oficiais.
  Essa estrutura garante governança distribuída, com comitês internos (p. ex. Comitê de Segurança ou de Auditoria) avaliando periodicamente a eficácia do gerenciamento de incidentes.

7. Ciclo de Vida de um Incidente

O tratamento de incidentes segue o ciclo de vida clássico recomendado por NIST e ISO, com fases definidas:

- ✓ Registro e Relato: Documentação inicial de todos os incidentes (eventos suspeitos ou confirmados) em sistema de ticket ou banco de dados central. Inclui data/hora, origem, descrição preliminar e pessoa responsável pelo registro. Todas as ocorrências, mesmo de baixo impacto, devem ser registradas para rastreabilidade.
- ✓ Triagem e Classificação: O CSIRT avalia o incidente quanto à gravidade e prioridade, de acordo com critérios pré-definidos (Seção 11.2). Exemplo de níveis de gravidade: Crítico (serviço essencial indisponível ou grande vazamento de dados), Alto (impacto significativo em função crítica), Médio e Baixo (impacto reduzido). O número e tipos de categorias podem ser definidos internamente (p. ex. conforme Atlassian, GRAV-1,2,3).
- ✓ Análise Detalhada: Investigação da causa raiz, vetores de ataque ou falha sistêmica. Coleta de evidências (logs, capturas de tela, imagens forenses) preservadas em repositório seguro, respeitando procedimentos de cadeia de custódia, especialmente para incidentes puníveis judicialmente. Esta fase define alcance real do incidente (ativos afetados, dados comprometidos).
- ✓ Contenção: Ações imediatas para limitar o impacto, como isolar máquinas afetadas, bloquear comunicações suspeitas ou ativar

redundâncias. O plano de resposta prevê estratégias rápidas para minimizar danos sem comprometer evidências.

- ✓ Erradicação: Eliminação da causa do incidente, como remoção de malware, correção de vulnerabilidades exploradas, encerramento de acessos maliciosos. Envolve aplicação de patches, limpeza de sistemas infectados e revisão de configurações de segurança.
- ✓ Recuperação: Restauração dos serviços e ativos à operação normal. Recupera-se dados a partir de backups validados e reconecta-se sistemas confiáveis à rede de produção. Testes confirmam que os sistemas reinstaurados não apresentam falhas ou brechas remanescentes.
- ✓ Lições Aprendidas (Pós-Incidente): Após resolução, realiza-se reunião (post-mortem) com stakeholders para analisar o ocorrido, documentar o impacto real, avaliar a eficácia da resposta e propor melhorias de processos, controles ou treinamentos. Resultados são repassados à alta gestão e incorporados nos planos de ação futuros. Esta etapa de aprendizado contínuo está alinhada à ISO 27035 e à prática do PDCA, permitindo que a organização evolua sua segurança a cada incidente tratado.

8. Comunicação e Notificação

A comunicação de incidentes obedece a protocolos formais:

Canal de Reporte Externo: A MONCALIERICAPITAL disponibiliza o e-mail incidentes@MONCALIERICAPITAL.com.br para que terceiros (clientes, fornecedores e parceiros) possam relatar eventuais incidentes de segurança. As mensagens recebidas por esse canal serão triadas pela equipe CSIRT em até 24 horas úteis, com envio de resposta inicial ao remetente confirmando o recebimento e início da análise.

- ✓ Comunicação Interna: Em todo incidente, informa-se imediatamente o gestor de incidentes e o Comitê Executivo, em paralelo ao acionamento do CSIRT. Informações resumidas são enviadas periodicamente aos níveis executivos durante a gestão do incidente. Após encerramento, reporte detalhado (relatório de incidente) é disponibilizado à alta direção.
- ✓ Comunicação a Autoridades e Reguladores: Cumpre-se a legislação aplicável. Em caso de incidentes cibernéticos graves, incidentes de compliance ou de dados pessoais, notificações obrigatórias são feitas às autoridades competentes. Incidentes de grande escala ou que afetem sistemas críticos podem requerer comunicação imediata ao Banco Central (BACEN) e, quando aplicável, a outros órgãos reguladores (ex. CVM, SUSEP).
- ✓ Comunicação a Terceiros e Parceiros: Fornecedores e parceiros afetados são alertados conforme protocolos estabelecidos em contratos de serviço. Quando incidentes envolvem terceiros, as cláusulas contratuais de resposta a incidentes são acionadas, mantendo fornecedores engajados na contenção e recuperação.
- ✓ Comunicação Externa/Ciência Pública: Em situações de crise (ex. incidente que afeta clientes), um Plano de Comunicação de Crise rege os anúncios públicos. Avalia-se cronograma e conteúdo de comunicados à imprensa, redes sociais e clientes, sempre em linguagem clara. Caso dados pessoais sensíveis sejam expostos, os titulares devem ser informados imediatamente sobre riscos e medidas de mitigação. A atuação conjunta com assessoria de imprensa e o departamento jurídico garante adequação das mensagens.

Todas as comunicações seguem princípios de transparência, agilidade e conformidade legal. O desenho de fluxo de comunicação (quem comunica, quando e como) faz parte do Plano de Resposta.

9. Treinamentos e Auditoria

São realizados treinamentos periódicos para todas as equipes sobre identificação e notificação de incidentes (filtros de phishing, uso de senhas, canais de reporte). Simulações de resposta (tabletop exercises) englobam cenários diversos (ataques cibernéticos, falhas críticas) para testar a efetividade do plano. Auditores internos/externos avaliam periodicamente a aderência ao processo de gerenciamento de incidentes, revisando registros e protocolos. As descobertas das auditorias servem de insumo para revisões futuras da política e do plano de resposta.

10. Atualização e Revisão

Esta política e o plano de resposta associados são revisados anualmente ou sempre que mudanças significativas ocorrerem (atualizações regulatórias, incidentes relevantes, alterações na estrutura tecnológica). Revisões devem envolver área de Segurança da Informação, Compliance e demais stakeholders. Toda versão atualizada é aprovada pelo Conselho de Administração ou Diretoria (nos termos da Res. CMN) e comunicada às áreas afetadas.

11. Plano de Resposta a Incidentes

11.1 Categorias e Níveis de Gravidade

O Plano define categorias de incidentes e escalas de gravidade para facilitar resposta estruturada. As categorias podem incluir, entre outras:

- ✓ Incidentes de Segurança da Informação (acesso não autorizado, vazamento de dados, malware/ransomware);

- ✓ Incidentes Tecnológicos (queda de sistema, falha de hardware, indisponibilidade de rede ou nuvem);
- ✓ Incidentes Cibernéticos (ataques DDoS, vírus, phishing direcionado);
- ✓ Incidentes Regulatórios (falta de reportes obrigatórios, falhas de conformidade);
- ✓ Incidentes Operacionais/Fornecedores (parada de serviço de terceiros críticos, desabastecimento tecnológico);
- ✓ Incidentes de Dados Pessoais (vazamentos, acesso irregular a dados de clientes).

Para cada categoria, atribuem-se níveis de gravidade. Conforme prática de mercado, níveis menores significam maior impacto. Exemplificando, Gravidade 1 corresponde a "incidente crítico de impacto muito alto" (todos os clientes afetados, sistemas vitais paralisados), Gravidade 2 é "impacto significativo" (serviço importante degradado), e Gravidade 3 "impacto baixo". A determinação do nível influencia a mobilização de recursos e o SLA de resposta.

11.2 Critérios de Classificação

Cada incidente é classificado considerando:

- ✓ Impacto: extensão dos serviços afetados (quantidade de usuários/clientes e processos críticos interrompidos), impacto financeiro e reputacional.
- ✓ Urgência: rapidez com que o incidente ameaça piorar (p. ex. situação de sequestro de dados em andamento requer urgência máxima).
- ✓ Tipo de Ativo Afetado: sensibilidade do sistema ou informação envolvida (dados sensíveis, sistemas de transações financeiras, infraestrutura de comunicação).

- ✓ Origem Potencial: se o incidente é interno (falha de equipamento, erro humano) ou externo (ataque cibernético), ajudando na priorização técnica.

A combinação de impacto e urgência define a prioridade final (por exemplo, Metodologia ITIL de prioridade baseada em impacto vs. urgência). Critérios concretos são documentados em matrizes internas de priorização, adotadas pela equipe de triagem para determinar escalonamento adequado e tempo de resposta.

11.3 Procedimentos de Tratamento por Tipo de Incidente

O Plano detalha procedimentos específicos para cada categoria de incidente:

- ✓ Incidentes de Segurança da Informação e Cibernéticos: seguem o fluxo padrão (preparação, detecção, contenção, erradicação, recuperação, lições aprendidas) com ênfase em ações como isolamentos de rede, forense digital, renovação de credenciais.
- ✓ Incidentes Tecnológicos: acionam imediatamente as equipes de infraestrutura/TEC, com procedimentos de failover para servidores, rollback de sistemas, acionamento de redundância. Inclui diagnóstico de causa raiz de falhas físicas ou de software.
- ✓ Incidentes Regulatórios: definem passos para investigação interna e remediação de não conformidades, atualizações de documentação exigida e comunicação regulamentar (ex. relatórios ao BACEN).
- ✓ Incidentes Operacionais/Fornecedores: ativam planos de contingência de fornecedores alternativos; o gestor de fornecedores executa cláusulas contratuais de continuidade ou substituição.

- ✓ Incidentes de Dados Pessoais (LGPD): seguem protocolo de comunicação à ANPD e titulares quando houver risco relevante, além de medidas imediatas de bloqueio de acesso ou correção da vulnerabilidade.

Para cada tipo de incidente existe um checklist de ações (por exemplo, verificar backups antes de recovery; notificar DPO se dados pessoais estiverem envolvidos). Esses procedimentos são revisados periodicamente e treinados em exercícios.

11.4 Templates de Registro e Relato

O Plano anexa modelos padronizados para documentação de incidentes:

- ✓ Formulário de Notificação de Incidente: para relato inicial, contendo campo para descrição do evento, sistemas afetados, dados comprometidos e pessoa que reporta.
- ✓ Relatório de Incidente: documento pós-morte formalizando cronologia, avaliação de impacto, ações tomadas, lições aprendidas e recomendações. Esses templates garantem consistência na coleta de informações e servem como base para auditorias e evidências em eventuais processos legais.

11.5 Métricas de Desempenho

Para monitorar a eficácia do processo, utiliza-se indicadores-chave:

- ✓ MTTD (Mean Time to Detect): tempo médio até a detecção de um incidente após sua ocorrência.
- ✓ MTTR (Mean Time to Recovery): tempo médio para restaurar os sistemas afetados ao estado operacional seguro.
- ✓ MTTC (Mean Time to Contain): tempo total desde a Hdetecção até a contenção completa, integrando MTTD e MTTR.

- ✓ Número de Incidentes por Tipo/Gravidade: volume de incidentes categorizados, para identificar tendências.
- ✓ % de Incidentes com Detecção Automatizada vs. Manual: mede maturidade das ferramentas de monitoramento.

Essas métricas, acompanhadas em painel de gestão, permitem avaliar melhorias (redução de MTTD/MTTR ao longo do tempo) e determinar investimento em controles. Alvo: diminuir continuamente o tempo de resposta, conforme prescrito por boas práticas do setor.

11.6 Relação com Terceiros e Fornecedores

O Plano detalha acordos com fornecedores críticos: cada contrato de serviço estratégico prevê cláusulas de segurança e resposta a incidentes em conformidade com as exigências internas e regulatórias (especialmente Res. CMN 4.893). São definidas responsabilidades compartilhadas: por exemplo, provedores de nuvem devem informar a MONCALIERICAPITAL imediatamente sobre incidentes em seus ambientes. Procedimentos de escalonamento incluem o fornecedor assim que detectado qualquer incidente que afete dados ou serviços da MONCALIERICAPITAL. A governança de terceiros envolve avaliações periódicas de segurança e testes de resposta conjunta para serviços terceirizados essenciais (banco de dados em nuvem, processadores de cartão etc.), de forma a garantir interoperabilidade de planos de contingência.

11.7 Fluxo de Resposta e Escalonamento

O fluxo de resposta operacionaliza o plano com etapa a etapa:

1. Recebimento do Relato pelo Service Desk ou canal automático (e-mail, sistema de monitoramento);
2. Análise Inicial pela Equipe de Triagem (CSIRT Secundária) e classificação de gravidade;

3. Acionamento Imediato do Nível Relevante: por ex., incidentes GRAV-1 disparam alerta ao administrador de plantão e mobilizam time de emergência 24/7; incidentes GRAV-2 mobilizam equipe no horário comercial etc.
4. Escalonamento para Diretores: incidentes críticos (red team) devem ser reportados imediatamente ao Diretor de Segurança e ao Comitê Executivo para decisão de crise.
5. Comunicação Externa: se o incidente atingir marca definidora (por ex. RTO em risco, dados de clientes expostos), o Presidente/CEO e o Jurídico avaliam divulgação pública e notificação às autoridades segundo cronograma predefinido.

Esta cadeia de escalonamento formal garante que incidentes de alta gravidade recebam atenção imediata de níveis elevados da gestão, sem burocracias indevidas.

11.8 Plano de Comunicação de Crise

Inclui procedimentos de comunicação para grandes incidentes com potencial de repercussão pública. Define papéis (quem fala pela empresa) e mensagens-chave:

- ✓ Notificação ao BACEN: conforme regulamentações do setor financeiro, incidentes que impactem sistemas críticos ou evidenciem falha estrutural devem ser comunicados ao Banco Central em prazos definidos (ex. por meio de relatório interno de falhas).
- ✓ Comunicação à ANPD: incidentes com dados pessoais graves são reportados formalmente à Autoridade de Proteção de Dados, obedecendo requisitos de confidencialidade e prazos legais.
- ✓ Contato à Imprensa e Redes: estabelece, em conjunto com Marketing/PR e Jurídico, release preparado com antecedência

para casos como indisponibilidade ampla de serviços ou vazamento de dados, explicando medidas adotadas e mitigação.

- ✓ Informação a Clientes e Parceiros: orientações via e-mail, SMS ou portal informam usuários afetados sobre a situação e instruções de segurança.

Todos os comunicados externos são validados pela diretoria executiva e equipe legal para assegurar coerência e alinhamento com responsabilidades legais e de mercado.

Esta política será revisada anualmente ou sempre que houver alterações significativas no ambiente regulatório, tecnológico ou organizacional.
A MONCALIERICAPITAL promoverá a disseminação desta política por meio de treinamentos periódicos, ações de comunicação interna e disponibilização em repositório acessível a todos os colaboradores. A adesão e compreensão são obrigatórias.

MONCALIERICAPITAL™ Compliance Corporativo. Aprovado em 16/06/2025.