	Número	Nome		Disposições Normativas
cateno	PL.000005	Política de Segurança da Informação e Cibernética		
	Gestor	Diretoria de Projetos, Processos, Riscos e Compliance		
	Versão	09/08/2024	Vigência	09/08/2025 – 18:00

1. Objetivo

1.1. Estabelecer as diretrizes e nortear procedimentos referentes à segurança da informação e cibernética de forma a proporcionar disponibilidade, integridade e confidencialidade, bem como prevenir, detectar e reduzir a vulnerabilidade a incidentes no que tange ao ambiente cibernético, aos dados e sistemas de informação utilizados.

2. Abrangência

2.1. Política aplicável a todos os membros do Conselho de Administração, dos Comitês de Assessoramento e da Diretoria-Executiva ("Administradores"), membros do Conselho Fiscal e demais colaboradores, fornecedores e prestadores de serviços da Cateno Gestão de Contas de Pagamentos S.A. (“Cateno ou Companhia”).

3. Regulamentação

3.1. Para segurança da informação e cibernética, a Companhia baseia-se nos documentos relacionados a seguir:

3.1.1. Resolução BCB n° 85/2021.

3.1.2. Resolução CMN n° 4.893/2021.

3.1.3. Circular BACEN nº 3.909/2018.

4. Responsabilidades

4.1. Conselho de Administração:

4.1.1. Deliberar sobre a aprovação desta Política, podendo utilizar de seus respectivos Comitês de Assessoramento;

4.1.2. Avaliar e aprovar o Plano de Ação e de Resposta a Incidentes visando à implementação da política de segurança cibernética até 31 de março do ano seguinte ao da data-base.

4.2. Diretoria Executiva:

4.2.1. Assegurar o comprometimento de todos os administradores, colaboradores, fornecedores e terceiros, com atuação ética e responsável quando da ocorrência e comunicação de incidentes;

4.2.2. Compartilhar informações com os responsáveis pelo seu tratamento em tempo hábil, tomando todas as ações cabíveis para minimizar os potenciais danos;

4.2.3. Ser responsável pelo cumprimento desta Política e pela melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética;

4.2.4. Submeter esta Política para deliberação do Conselho de Administração.

4.3. Diretoria de Tecnologia:

4.3.1. Elaborar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro de cada ano;

4.3.2. Efetuar periodicamente os testes de intrusão e de vazamento de informações para avaliar a segurança dos acessos aos sistemas e rede;

4.3.3. Adotar procedimentos e controles para reduzir a vulnerabilidade da Companhia a incidentes e atender aos objetivos de segurança cibernética com relação às medidas de segurança;

4.3.4. Assegurar a implementação dos controles específicos voltados para a rastreabilidade no tratamento de informações sensíveis para o negócio;

4.3.5. Orientar a atuação dos gestores de informação para que definam os requisitos de elaboração de perfis de acesso dos sistemas sob sua influência.

4.4. Diretoria de Projetos, Processos, Riscos e Compliance:

4.4.1. Assegurar a implantação, acompanhar e monitorar o cumprimento das diretrizes desta Política, revisá-la anualmente e mantê-la atualizada;

4.4.2. Analisar e propor ao Conselho de Administração eventual necessidade de alteração no documento, bem como esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação;

4.4.3. Emitir recomendações específicas de prevenção ou mitigação de riscos inerentes à segurança da informação e cibernética às áreas internas da Companhia toda vez que identificada tal necessidade, usando, como insumos, os resultados de tratamentos de incidentes promovidos pela Gerência Executiva de Tecnologia;

4.4.4. Realizar o monitoramento das regras e critérios relacionados ao ambiente de segurança da informação, interagindo com a Gerência Executiva de Tecnologia para a implementação de medidas saneadoras, caso necessárias;

4.4.5. Acompanhar os relatórios de testes de intrusão e de vazamento de informações conduzidos pela Gerência Executiva de Tecnologia.

4.5. Colaboradores, Fornecedores e Terceiros:

4.5.1. Atuar de forma ética e responsável pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, como de seus clientes, parceiros e fornecedores, dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas e em cumprimento a esta Política.

4.6. Auditoria Interna:

4.6.1. Avaliar, conforme plano de auditoria elaborado, a efetividade da política de segurança da informação e cibernética, do plano de ação e de resposta a incidentes e dos demais requisitos relacionados à segurança da informação e cibernética.

5. Diretrizes

5.1. A Cateno, para garantir a segurança da informação e cibernética, exerce suas atividades com base nos seguintes pilares:

5.1.1. Disponibilidade: garantir que a informação estará disponível sempre que for necessário.

5.1.2. Integridade: garantir que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não.

5.1.3. Confidencialidade: garantir que a informação somente estará acessível para pessoas autorizadas.

5.2. Independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para as suas respectivas finalidades, sendo sujeitos a monitoramento e auditoria.

5.3. A Cateno estabelece que todo ativo de informação de sua propriedade possua um responsável, bem como seja devidamente classificado de acordo com critérios estabelecidos em norma específica e adequadamente protegido de quaisquer riscos e ameaças que possam comprometer os pilares de segurança das informações.

5.4. Todas as funções e responsabilidades em relação à segurança da informação e cibernética são definidas, estabelecidas e comunicadas.

5.5. Requisitos de segurança da informação e cibernética são estabelecidos levando-se em consideração a avaliação dos riscos que possam afetar negativamente a estratégia e os objetivos gerais de negócios da Companhia, o cumprimento de exigências legais, estatutárias, regulamentares e contratuais e proteção das informações em todo o seu ciclo de vida, em meios físicos ou digitais.

5.6. Na gestão da informação, a integridade, a confidencialidade e a disponibilidade são asseguradas durante todas as fases de tratamento, bem como as atribuições e áreas de responsabilidades conflitantes devem ser segregadas.

5.7. Informações relacionadas a ameaças à segurança da informação e cibernética devem ser coletadas e analisadas para apoiar o aprimoramento dos recursos de proteção.

5.8. Para gerenciar o ciclo de vida dos ativos de informação deve haver uma coordenação das ações dos gestores de informação, que são responsáveis por definir os requisitos de elaboração de perfis de acesso dos sistemas sob sua influência.

5.9. As solicitações, autorizações, administração e auditorias de acessos devem ser segregadas.

5.10. No gerenciamento de identidades, os privilégios de acesso devem estar associados a cada pessoa.

5.11. A segurança da informação e cibernética é aplicada em todas as fases do ciclo de vida dos sistemas e outros ativos de informação.

5.12. Na contratação de serviços ou de pessoas e no relacionamento com colaboradores, parceiros, intermediários, contratados e estagiários são observados os mesmos quesitos de segurança adotados pela Cateno.

5.13. Os requisitos de segurança da informação e cibernética são incluídos nos planos de continuidade de negócios, que são desenvolvidos, implementados, testados, revisados e avaliados periodicamente.

5.14. Nos casos de violação ou divulgação indevida de informações, a ocorrência é analisada sob o aspecto legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo-se as vulnerabilidades.

5.15. Com relação às diretrizes de segurança da informação e cibernética, a Cateno se compromete a:

5.15.1. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas.

5.15.2. Classificar os dados e informações quanto à relevância para o negócio, garantindo a continuidade dos negócios, a partir de diretrizes emanadas por essa Política.

5.15.3. Efetuar regularmente procedimentos para identificar, analisar, avaliar e tratar os riscos por uso indevido da informação, fraudes ou ato que possa danificar ou impedir o acesso aos dados e sistemas de informação.

5.15.4. Treinar e avaliar periodicamente os colaboradores sobre Segurança da Informação e Cibernética, incluindo a disseminação da cultura de segurança e orientações sobre precauções ao usar produtos e serviços.

5.15.5. Adotar procedimentos e controles para reduzir a vulnerabilidade da Companhia a incidentes e atender aos objetivos de segurança cibernética com relação às medidas de segurança, dentre eles:

5.15.5.1. A autenticação;

5.15.5.2. A criptografia;

5.15.5.3. A prevenção e a detecção de intrusão;

5.15.5.4. A prevenção de vazamento de informações;

5.15.5.5. A realização periódica de testes e varreduras para detecção de vulnerabilidades;

5.15.5.6. A proteção contra softwares maliciosos;

5.15.5.7. O estabelecimento de mecanismos de rastreabilidade;

5.15.5.8. Os controles de acesso e de segmentação da rede de computadores;

5.15.5.9. E a manutenção de cópias de segurança dos dados e das informações.

5.15.6. Aplicar procedimentos e controles, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Companhia.

5.15.7. Conceder a terceiros somente o acesso às informações necessárias ao exercício de suas atividades, desde que tal acesso não implique o descumprimento de legislação ou regulamentação em vigor, observando-se, ainda, o contido na cláusula contratual de confidencialidade do uso.

5.15.8. Tratar as ocorrências por uso indevido de informações corporativas sob o aspecto legal e disciplinar.

5.15.9. Aplicar proteção aos serviços de processamento e armazenamento de dados em nuvem, servidores, sistemas operacionais e demais componentes que compõem o ambiente de infraestrutura, para garantia da segurança da informação e cibernética.

5.15.10. Considerar medidas de continuidade de negócio definidas em documentação específica, no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, podendo considerar a substituição da empresa contratada, visando o reestabelecimento da operação normal da Companhia.

5.15.11. Permitir a terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior, seguindo critérios específicos de decisão para matéria desta natureza.

5.15.12. Assegurar que a engenharia dos sistemas de informação em uso, desenvolvidos ou mantidos pela Companhia, os fornecidos por terceiros ou outras tecnologias adotadas concorram para o cumprimento das demais diretrizes desta Política.

5.15.13. Assegurar que um plano de ação e de resposta a incidentes esteja estabelecido visando à implementação desta política.

5.15.14. Assegurar a prática da gestão e da elaboração dos cenários de incidentes de segurança da informação e cibernética, com relevância determinada a partir de níveis mínimos de gravidade e tendência dos impactos e de urgência do restabelecimento da normalidade.

5.15.15. Assegurar a completa gestão do ciclo de tratamento de incidentes relevantes à segurança da informação no negócio, incluindo no mínimo: registro; coleta de informações internas e de empresas prestadoras de serviço a terceiros envolvidas; análise da causa e do impacto; estipulação de prazo de reinício ou normalização dos processos afetados; controle dos efeitos e comunicação tempestiva.

5.15.16. Adotar iniciativas para compartilhamento de informações sobre os incidentes relevantes por meio de filiação em fóruns de discussão.

5.15.17. Adotar os procedimentos que garantam a recuperação dos dados e sistemas de informação corporativos para a continuidade dos negócios, os quais devem contemplar a execução periódica de testes, a partir de cenários de incidentes relevantes e de substituição da empresa contratada.

5.15.18. Assegurar a prática de procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados, inclusive, por empresas prestadoras de serviços a terceiros e que manuseiem dados ou informações sensíveis do negócio ou que sejam relevantes para a condução das atividades operacionais. Essa prática deve contemplar níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela Companhia.

5.15.19. Elaborar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

5.15.20. Emitir as recomendações específicas de prevenção ou mitigação de riscos inerentes à segurança da informação e cibernética às áreas internas da Companhia toda vez que identificada tal necessidade.

5.15.21. Efetuar os testes de intrusão e de vazamento de informações para avaliar a segurança dos acessos aos sistemas e rede.

5.15.22. Garantir o cumprimento dos períodos de retenção e expurgo de informações relacionadas à gestão da segurança da informação e cibernética, conforme determinações das entidades reguladoras da operação da Companhia.

5.15.23. Assegurar que este documento e os objetivos da segurança da informação e cibernética estejam estabelecidos e sejam compatíveis com a direção estratégica da organização, demonstrando sua liderança e comprometimento em relação ao sistema de gestão de segurança e sua melhoria contínua.

5.15.24. Assegurar a implementação dos controles específicos voltados para a rastreabilidade no tratamento de informações sensíveis para o negócio.

5.15.25. Elaborar inventário dos cenários de crises cibernéticas, relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços, realizar testes periódicos para avaliar a eficácia dos processos e controles, a fim de garantir a identificação e correção de eventuais deficiências, além de produzir um relatório periódico de resposta a incidentes no ambiente tecnológico Cateno.

5.15.26. Assegurar que esta política seja divulgada aos funcionários da Companhia e às empresas prestadoras de serviços a terceiros da Companhia, além de mantê-la num local de fácil acesso a todos que se relacionam com a Cateno.

6. Disposições Gerais

6.1. É competência da Diretoria de Projetos, Processos, Riscos e Compliance da Cateno sugerir alterações a esta Política, sempre que se fizer necessário.

6.2. Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração e revoga quaisquer documentos em contrário.

6.3. Comunicamos que os colaboradores, fornecedores ou outros *stakeholders* que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato no Canal de Conduta Ética da Cateno (www.canaldeeticacateno.com.br ou 0800 377 8008), podendo ou não se identificar.

6.4. Internamente, a não observância das determinações desta Política acarretará ações de gestão de consequência que poderão variar desde uma orientação sobre como proceder para anular ou, ao menos, minimizar os eventuais problemas criados, até a demissão por justa causa dos responsáveis.

6.5. Para os casos externos, o descumprimento das diretrizes desta Política enseja a aplicação de medidas cíveis e/ou criminais, conforme a respectiva gravidade do seu descumprimento.

6.6. Esta Política deverá ser submetida a atualizações anualmente.

São Paulo, 09 de agosto de 2024.

(Política de Segurança da Informação e Cibernética aprovada em Reunião Ordinária do Conselho Administração da Cateno Gestão de Contas de pagamento S.A em 09 de agosto de 2024).

Protocolo de assinaturas

Este protocolo de assinatura foi gerado para o arquivo **Política de Segurança da Informação Cibernética.pdf** no dia 14/08/2024 - 10:46 (GMT -03:00), Horário Padrão de Brasília.

O arquivo foi assinado eletronicamente através do Fusion Platform e sua autenticidade pode ser verificada por meio do **QR Code** ou no **link abaixo**:

https://neomindprd.cateno.com.br/fusion/link/electronic-sign/validate/cb8ef401-6373-43aa-8f46-aae0578dcd20

Caso necessário, acesse o site **https://neomindprd.cateno.com.br/fusion/link/electronic-sign/validate** e informe o **código abaixo** para verificar a autenticidade das assinaturas:

Código do arquivo: cb8ef401-6373-43aa-8f46-aae0578dcd20

Assinaturas eletrônicas

FERNANDO PACHECO MACHADO DIAS

13/08/2024 - 16:59 IP: 10.10.9.129

FERNANDO DE ROSA

13/08/2024 - 17:00 IP: 10.10.9.22