

Política de Segurança Cibernética

Essa política foi desenvolvida com o objetivo de assegurar que todas as informações que são dispostas aos colaboradores, clientes, terceiros e a Alta Administração sejam tratadas com segurança e privacidade. Para que isso se torne efetivo esta política visa garantir a proteção, manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações sobre os cuidados da CloudPayments, além de prevenir, detectar, e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

A primeira resolução de 2018, o Bacen estabeleceu critérios a serem cumpridos pelas instituições financeiras com relação a aplicação da segurança cibernética, dando a diretriz para que as instituições reguladas busquem assegurar a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados.

Princípios da segurança Cibernética:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada.
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade.
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Stone.
- Garantir que os sistemas e as informações sob responsabilidade da Stone estejam adequadamente protegidos.
- Garantir a continuidade do processamento das informações críticas de negócios.
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.
- Comunicação imediatamente à área de Segurança da Informação, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

Resoluções: a resolução CMN nº 4.893 e BCB nº85, informar medidas para o mercado financeiro, em específico para instituições financeiras, condutas para a contratação de serviços de processamento e armazenamento de dados e computação em nuvem , devendo

ser compatível com o porte , o perfil de risco e o modelo de negócio , bem como a natureza das operações e a sensibilidade dos dados e das informações tratadas.

Para uma segurança completa dos dados deve-se implementar na política a prevenção de incidentes e vazamento de dados conforme Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18).

“no art. 46, dispõe sobre a necessidade de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como o dever de indenizar em dano patrimonial, moral, individual ou coletivo, na hipótese de causar violação a LGPD, conforme previsto no art. 42.”

Ainda dispõe que o controlador deverá comunicar à Autoridade Nacional de Proteção de Dados Pessoais e ao titular a ocorrência de incidente de segurança que envolva dados pessoais que possa acarretar risco ou dano relevante aos titulares. Vale destacar o prejuízo financeiro que isso pode acarretar, mas também o reputacional.

O Plano de ação para o tratamento de incidentes foi desenvolvido conforme art.6º da resolução BCB nº85:

I - As ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Ainda segundo a mesma resolução, se faz necessário a elaboração de um relatório anual, conforme descrito no Art. 8º “As instituições de pagamento devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6º, com data-base de 31 de dezembro”

§ 1º O relatório de que trata o caput deve abordar, no mínimo:

I - A efetividade da implementação das ações descritas no art. 6º, parágrafo único, inciso I;

II - O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos no art. 6º, parágrafo único, inciso II;

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV - Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

§ 2º O relatório mencionado no caput deve ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base.

Responsabilidades e controles: Para garantir o cumprimento dos princípios da segurança da segurança cibernética, fica disposto a responsabilidade do departamento de Segurança da informação desenvolver e aplicar todos os métodos de segurança, aplicar controles de acompanhamento de todos os dados tratados pela CloudPayments, bem como o seu armazenamento, garantido assim a confidencialidade, integridade e disponibilidade das informações. Além disso aplica a realização de treinamentos periódicos e monitoramento interno, sendo de responsabilidade do *compliance*.

A CloudPayments prevê em seus controles:

- Controle de acesso e gerenciamento: regras de acesso e permissões de acordo com o cargo e departamento;
- Gerenciamento de risco e segurança da rede (vulnerabilidade): controle por mesmo da TI (tecnologia da informação), através de sistema de Firewall, aplicação de antivírus e gestão da rede interna.
- Armazenamento de dados: criptografia e gestão do armazenamento em nuvem;
- Autenticação de acesso aos sistemas: gestão de identificação aos sistemas internos e de sistema de acesso do portal cliente.

Tratamentos de incidentes: Para gestão de tratamento de incidentes e plano de ação a CloudPayments elege um comitê, onde envolverá os procedimentos de monitoramento e relatórios e testes da área de segurança da informação, as áreas afetadas e o diretor

responsável para aprovação e execução do plano de ação para prevenção e resposta de incidentes, com base no plano de ação da resolução BCBnº85;

Processamento e armazenamento de dados: A Cloudpayments deve assegurar que as políticas, estratégias e estruturas de gerenciamento dos riscos, especificamente na hipótese aos critérios de contratação de serviços de terceirização, no tocante aos serviços de processamento e armazenamento de dados e de computação em nuvem, no Brasil ou no exterior, realizem o processamento e armazenamento dos dados de forma correta.

A contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

I - A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II - A verificação da capacidade do potencial prestador de serviço de assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Os serviços de computação em nuvem previstos na Resolução, são os seguintes:

I - Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou

executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II - Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

Importante observar que instituição contratante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

Histórico da Política

Data de Criação/Atualização	Elaborado por	Versão	Código do Documento	Data de aprovação	Aprovado por
17/01/2023	Virginia Martins	01	CP012	19/02/2023	Sallen Moraes

Este documento foi desenvolvido e validado pela GRC e seu uso é de acesso restrito e exclusivo para a Cloudpayments

