POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

INOVANTI INSTITUIÇÃO DE PAGAMENTO S.A.

Data: 28/09/2023

Versão: 002

REGISTRO DAS ALTERAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA DA INOVANTI INSTITUIÇÃO DE PAGAMENTO S.A.

Versão	Data	Autor	Data de Aprovação	Aprovadores	Justificativa
001	02/03/2022	Riscos e Compliance	02/03/2022	AGE	Primeira redação
002	28/09/2023	Riscos e Compliance	05/12/2023	AGE	Reestruturação de toda a Política, em atendimento às atualizações nas normas aplicáveis

SUMÁRIO

A. ESCOPO DESTA POLÍTICA

1. Apresentação e Objetivo

Esta Política tem por objetivo estabelecer as diretrizes que permitem a INOVANTI INSTITUIÇÃO DE PAGAMENTO S.A. ("Inovanti"), preservar e proteger as informações de seus Clientes, Colaboradores, Fornecedores, partes interessadas e da própria instituição contra ameaças e riscos relacionados à segurança da informação e cibernética, implementar controles e procedimentos que visam a reduzir a vulnerabilidade da Inovanti a incidentes, bem como dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A Inovanti oferece solução de pagamento para seus Cliente, de abertura de contas de pagamento, gestão das contas e dos recursos financeiros, e pagamentos recorrentes, que poderão ser indicados por Parceiros, possibilitando o recebimento e a realização de pagamentos por meio das Transações.

A Inovanti deve implementar e manter esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

2. Normas Aplicáveis

Todos aqueles a quem a presente Política for aplicável deverão observar as leis e normas abaixo indicadas (em conjunto "Legislação Aplicável"):

a) **Lei 12.865/2013:** Dispõe sobre os Arranjos de Pagamento e as Instituições de Pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB);
b) **Resolução BCB nº 80/2021:** Dispõe sobre a constituição, o funcionamento e a prestação de serviços de pagamento por parte das instituições de pagamento, e estabelece os parâmetros para ingressar com pedidos de autorização de funcionamento junto ao Banco Central do Brasil; e,
c) **Resolução BCB nº 85/2021:** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

As leis e normas são citadas de forma exemplificativa e contemplam apenas as diretrizes em vigor na data de elaboração desta Política, não esgotando toda a Legislação Aplicável às atividades da Inovanti.

O Diretor responsável pela Segurança Cibernética, nomeado perante o Bacen pela Assembleia Geral Extraordinária do Inovanti, será o responsável por verificar eventual atualização, revogação e a edição de novas normas atinentes a esta Política.

3. Definições

a) **Administradores**: diretores da Inovanti;
b) **AGE** ou **Assembleia**: assembleia geral extraordinária que deliberar sobre algum assunto referido no texto desta Política;
c) **Ativos**: todas as formas tratamento de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.;
d) **Bacen** ou **BCB**: Banco Central do Brasil;
e) **Clientes** ou **Usuários**: queles que contratam e utilizam produtos e/ou serviços da Inovanti;
f) **Colaboradores**: empregados, prestadores de serviços sem vínculo empregatício, trainees e estagiários da Inovanti;
g) **Comitê de Segurança da Informação e Segurança Cibernética:** comitê formado por Colaboradores indicados pelos Administradores e aprovado pela AGE, com o objetivo de deliberar a respeito de assuntos relacionados à Segurança da Informação e Segurança Cibernética;
h) **Conta de Pagamento**: conta de registro detida em nome do Cliente, utilizada para a execução de Transações;
i) **Diretor responsável pela Segurança Cibernética:** diretor responsável pela implementação, execução e manutenção da política, pelo plano de ação e resposta a incidentes da Inovanti, bem como, pela convocação das reuniões periódicas do comitê de segurança da informação e segurança cibernética, quando e se implementado;
j) **Fornecedores:** toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de comercialização de produtos ou prestação de serviços para a Inovanti;

k) **Gestão de Ativos:** são as boas práticas utilizadas pela Inovanti em seu processo de controle de ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas e materiais, *know-how*), que buscam alcançar um resultado desejado e sustentável para a operação;

l) **Informações Sensíveis:** que tem valor estratégico para o desenvolvimento dos negócios e das operações da Inovanti, ganhando tangibilidade por meio de transações, processamentos, bancos de dados, entre outras formas, e que serão tratados com base no legítimo interesse da instituição, estritamente necessários para a finalidade pretendida nos termos desta Política e da legislação em vigor;

m) **Instituição de Pagamento**: para fins desta Política, é a Inovanti como emissora de moeda eletrônica, cuja atividade consiste em gerenciar a conta de pagamento de Clientes, utilizada para o carregamento e o pagamento de transações pré-pagas;

n) **Parceiros:** toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, que celebra contratos com a Inovanti, com a finalidade de, mediante retribuição, colaborar com os negócios da Inovanti;

o) **Política:** esta Política de Segurança da Informação e Cibernética;

p) **Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da Inovanti contra-ataques, danos, ameaças ou acesso não autorizado;

q) **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da Inovanti;

r) **Sistema de Pagamentos:** serviços da Inovanti relacionados à abertura de Conta de Pagamento e realização de Transações de carregamento, transferência e resgate de recursos pelo Cliente;

s) **Transação:** operação em que o Cliente realiza a movimentação de sua Conta de Pagamento, realizando o carregamento de recursos, a transferência de recursos ou o resgate de recursos para contas bancárias ou contas de pagamento.

4. Abrangência

A Política de Segurança da Informação e Cibernética se aplica a todos os Administradores, Colaboradores, Parceiros e Fornecedores, responsáveis pela segurança cibernética da Inovanti, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da instituição, e que devem, no que couber: (i) cumprir as

normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política; (ii) informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivo, serviço ou processo relacionado à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva; (iii) utilizar as informações relacionadas à esta Política, como patrimônio da Inovanti, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

Esta Política foi elaborada e revisada pelo Diretor responsável pela segurança da informação e cibernética, e aprovada pelos Administradores, e será revisada com a periodicidade mínima anual. A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.
Além da Política, o referido Diretor será responsável pela execução do plano de ação e de resposta a incidentes.

Esta Política será compatível com:

a) O porte, o perfil de risco e o modelo de negócio da Inovanti;
b) A natureza das atividades da Inovanti e a complexidade dos seus produtos e serviços oferecidos; e
c) A sensibilidade dos dados e das informações sob responsabilidade da instituição.

B. PRINCÍPIOS

A Inovanti tem o compromisso garantir a segurança e o tratamento adequado das informações. Para tanto, adota atividades que se baseiam nos seguintes princípios:

a) **Autenticidade:** garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação;
b) **Confidencialidade**: garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
c) **Disponibilidade**: garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário; e,
d) **Integridade**: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

C. DIRETRIZES GERAIS

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

a) Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na Inovanti;
b) Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A Inovanti adotará mecanismos que visam a assegurar a utilização segura de senhas;
c) Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela Inovanti;
d) Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar ou, ao menos, registrar acessos indevidos, modificações, destruições ou divulgações não autorizadas;
e) Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização;
f) Assegurar o cumprimento dos procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;
g) Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis;
h) Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Inovanti;
i) Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados pela instituição;

j) Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos Fornecedores que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Inovanti;
k) Classificar os dados e as informações quanto à relevância;
l) Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
m) Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen;
n) Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros;
o) Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela Inovanti e por esta Política;
p) Divulgar ao público resumo contendo as linhas gerais desta Política;
q) Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo (i) a implementação de programas de capacitação e de avaliação periódica de pessoal; e, (ii) a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.

D. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a Inovanti adotará políticas e procedimentos para os processos elencados a seguir.

1. Gestão de Ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com armazenagem de documentos físicos deve ser restrito e limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A Inovanti deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir

que os princípios da autenticidade, confidencialidade, disponibilidade e integridade sejam cumpridos integralmente.

2. Autenticação

A Inovanti adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, para de forma consequente prever os respectivos processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3. Segmentação de rede

A Inovanti deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

Caso o Colaborador queira criar, alterar ou excluir regras nos *firewalls* e Ativos de rede, deverá enviar uma requisição ao departamento de tecnologia da informação, que fará análise e aprovação.

4. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus Clientes. Portanto, a Inovanti adota a seguinte classificação:

a) **Informação Pública**: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;
b) **Informação Interna**: aquela que pode ser acessada somente por Colaboradores da Inovanti. São exemplos de Informação Interna: normas, procedimentos e formulários da instituição;
c) **Informação Restrita**: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos e documentos estratégicos da Inovanti; e,
d) **Informação Confidencial**: aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um

propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

5. Controle de acesso

A Inovanti deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados, aos sistemas internos e as informações que não sejam de livre acesso e sem permissão prévia. Desta forma, a Inovanti deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções, rastreabilidade de acesso e aprovação de acesso, quando aplicável, de forma a garantir procedimentos internos adequados e consistentes.

6. Gestão de riscos e falhas de segurança

A instituição possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

Os processos de gestão de riscos englobam os controles de mudanças no ambiente de tecnologia da Inovanti, que são estruturados e aplicados através de um conjunto de processos que vão atuar em todas as áreas potencialmente impactadas, bem como a capacitação e o engajamento dos Colaboradores diretamente envolvidos nas ações mitigatórias dentro da instituição, com o objetivo da preparação para essas situações.

Neste processo, será levado em conta: (i) o levantamento dos impactos organizacionais; (ii) a priorização das ações de mudanças no ambiente de tecnologia da Inovanti; (iii) o planejamento; (iv) os testes; (v) a mobilização; (vi) a comunicação; e (vii) os treinamentos contínuos para a devida capacitação das pessoas diretamente envolvidas no processo de gestão de riscos e controle dos respectivos ambientes de tecnologia da Inovanti, da seguinte forma:

a) O levantamento dos impactos organizacionais irá detalhar quais áreas da instituição podem vir a ser impactadas direta e/ou indiretamente;
b) A priorização das ações de mudanças no ambiente de tecnologia irá avaliar e elencar todas as mudanças que precisam ser implementadas, definindo quais demandas serão tratadas com prioridade e quais poderão ser mitigadas;

c) O planejamento irá definir os planos de implementação, impactos e correções, visando maximizar a segurança e integridade dos ambientes de tecnologia, e minimizar ao máximo riscos de ações ineficientes e ineficazes;

d) Os testes irão monitorar todo o processo e se certificar que tudo está acontecendo conforme o planejamento realizado. Através dos testes serão elaborados relatórios, os quais serão revisados pelo Diretor responsável pela execução e manutenção desta Política, que descreverá os resultados, funcionalidades e correções;

e) A mobilização irá, através do Diretor de Segurança Cibernética, em conjunto com o Comitê de Segurança da Informação e Segurança Cibernética e a Área de Compliance, direcionar a Inovanti e todos os Colaboradores ao encontro do objetivo deste processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da instituição;

f) A comunicação irá informar e detalhar os objetivos da mudança através dos canais de comunicação e do desenvolvimento do plano de comunicação, para que todos os Colaboradores tenham conhecimento da relevância e da necessidade do engajamento para o alcance de todas as medidas adequadas e mitigatórias, para neutralizar ou minimizar os eventuais ou potenciais danos;

g) O treinamento contínuo irá garantir a transferência e o nivelamento de conhecimentos relacionados ao trabalho desenvolvido no processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da Inovanti.

7. Gestão de Fornecedores

A Inovanti verifica o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da Inovanti, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A instituição disponibiliza um canal de comunicação para que seus Parceiros e Fornecedores comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da Inovanti, e diretrizes desta Política.

8. Segurança física do ambiente

A Inovanti deve implementar sistema para controle de acesso dos Colaboradores, Parceiros e Fornecedores aos locais restritos.

Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

9. Backup e gravação de LOG

A Inovanti adota uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades. Bem como, realizará a gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acesos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

10. Proteção contra vírus, arquivos e softwares maliciosos

A Inovanti adotará mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a instituição a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, devem estar instalados e atualizados em toda a rede interna.

11. Testes de varredura para detecção de vulnerabilidade

A Inovanti se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

A Inovanti adota processo de atualização periódica de segurança no parque tecnológico, de forma a prevenir vulnerabilidades que possam ocasionar brechas de segurança para ataque de vírus e outros tipos de software, que se propaguem nos computadores, sistemas e servidores da instituição.

12. Criptografia

Os Ativos de informação da Inovanti devem possuir criptografia adequada, conforme a classificação da informação, em todo tráfego que ocorrer em rede pública, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

13. Plano de continuidade

A Inovanti realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a Inovanti realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.

Devem ser aplicados testes de continuidade de serviços de pagamento e realização testes periódicos para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a Inovanti certifique a conformidade dos planos desenvolvidos com os objetivos da instituição, requisitos regulatórios e requisitos legais.

Além disso, haverá uma a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados Fornecedores da Inovanti, que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição. Bem como a classificação dos dados e das informações quanto à relevância; e a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes.

14. Incidentes de segurança

a. Classificação de relevância dos incidentes

A Inovanti classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios, que serão detalhados em manuais específicos da instituição.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, Parceiro ou Fornecedor, devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por através do e-mail ouvidoria@inovanti.com.br.

Os incidentes reportados serão classificados segundo o risco que representam para a instituição e o respectivo impacto na continuidade dos negócios. Além disso, devem ser devidamente registrados, tratados e comunicados.

A Inovanti adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

c. Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a Inovanti irá adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Bacen, por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a Inovanti comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas, informando o prazo para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, estabelecendo e documentando os critérios que configuraram a situação de crise.

d. Plano de ação e resposta a incidentes

A Inovanti deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

a) As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política; e,
b) As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

e. Relatório anual de incidentes

A Inovanti deverá elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

a) A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
b) 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, em conformidade com as diretrizes desta Política;
c) Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e,
d) Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado aos Administradores da Inovanti até 31 de março do ano seguinte ao da data-base.

Este relatório será revisado anualmente.

15. Mecanismos de rastreabilidade

A Inovanti deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

Para as operações em dispositivos autorizados a realizar transações na plataforma da Inovanti, o controle e a gestão das informações sensíveis terão tratamento específico para

assegurar a segurança e integridade das informações de identidade do dispositivo, preservando-se as diretrizes da Lei 13.709/2018, no que se aplicar.

16. Registro de impacto

A Inovanti deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, que devem abranger inclusive informações recebidas de Fornecedores.

17. Treinamentos e conscientização

A Inovanti preza por uma cultura integra de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para todos os Administradores e Colaboradores.

A instituição promoverá a ampla divulgação desta Política a todos os seus Fornecedores e Parceiros, bem como ao público em geral, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, os Administradores irão difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

18. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

a. Seleção de terceiros

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a

Inovanti deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

a) O cumprimento da legislação e da regulamentação em vigor;
b) O acesso da Inovanti 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 aderência do prestador de serviço a certificações exigidas pela Inovanti para a prestação do serviço a ser contratado;
e) O acesso da Inovanti 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 usuários finais da Inovanti por meio de controles físicos ou lógicos; e,
h) A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição.

Na avaliação da relevância do serviço a ser contratado, a Inovanti também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a Inovanti deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, a Inovanti deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

c. Serviços de computação em nuvem

Os serviços de computação em nuvem disponibilizados à Inovanti, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

a) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Inovanti ou por ela adquiridos;
b) Implantação ou execução de aplicativos desenvolvidos pela Inovanti, ou por ela adquiridos, utilizando recursos computacionais do Fornecedor;
c) Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio Fornecedor.

A Inovanti é responsável, em conjunto com o Fornecedor contratado, 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.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela Inovanti ao Bacen.

d. Contratação de serviços de computação em nuvem no exterior

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a instituição deverá observar os seguintes requisitos:

a) Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
b) Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
c) Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços; e,

d) Previsão de alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a Inovanti solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a Inovanti deverá solicitar autorização 60 dias antes da alteração contratual.

A instituição deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da Inovanti e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

e. Contrato de prestação de serviços

A Inovanti deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

a) A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
b) A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
c) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
d) Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à Inovanti, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
e) O acesso da Inovanti às informações fornecidas pela empresa contratada, bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
f) A obrigação da empresa contratada notificar a Inovanti sobre a subcontratação de serviços relevantes para a instituição;

g) A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
h) A adoção de medidas pela Inovanti, em decorrência de determinação do Bacen; e,
i) A obrigação de a empresa contratada manter a Inovanti permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da Inovanti pelo Bacen, o contrato de prestação de serviços deve prever:

a) A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;
b) A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços. A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que: (i) a empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e, (ii) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da Inovanti.

f. Comunicação ao Bacen

A comunicação ao Bacen, referente a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deve conter as seguintes informações:

a) O nome da empresa a ser contratada;
b) Os serviços relevantes a serem contratados; e,
c) No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese da contratação de serviços de computação em nuvem no exterior, que possui prazo específico.

19. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a Inovanti deve assegurar:

a) O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
b) Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da Inovanti;
c) Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.
d) O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
e) O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
f) A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela instituição, bem como das providências para o reinício das suas atividades;
g) Estabelecer e documentar os critérios que configurem a situação de crise.

A Inovanti deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

20. Arquivamento de informações

A Inovanti deve armazenar em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

a) O documento relativo à política de Segurança Cibernética;
b) A ata de reunião da Diretoria da Inovanti aprovando a Política e o plano de ação de resposta a incidentes;
c) O documento relativo ao plano de ação e de resposta a incidentes;
d) O relatório anual sobre a implementação do plano de ação e de resposta a incidentes;
e) A documentação sobre os procedimentos desta Política referentes à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
f) A documentação no caso de serviços prestados no exterior;
g) Os contratos de prestação de serviços;
h) Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados.

E. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores da Inovanti, devem aderir formalmente por meio de um termo em que se comprometem a agir de acordo com esta Política.

Os contratos celebrados com Fornecedores pela Inovanti e que tratem de Ativos de informação referentes a esta Política devem possuir cláusula que assegure a segurança das informações.

F. DISPOSIÇÕES GERAIS

Esta Política está acompanhada de um **Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética** e **Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética**, que deverão ser assinados por todos os Colaboradores, Fornecedores e Parceiros, no que couber, conforme textos aprovados em seus Anexos I e II.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site www.inovanti.com.br.

Ainda, esta Política será divulgada publicamente em uma versão resumida contendo as linhas gerais da Política de Segurança Cibernética, conforme texto aprovado em seu Anexo II.

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, **[NOME DO COLABORADOR]**, inscrito no CPF sob o nº **[número do CPF]**, declaro ter conhecimento desta Política Segurança da Informação e Segurança Cibernética, publicada internamente sob o código **PI_PSISC_001**, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da Inovanti.

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do e-mail contido nesta Política.

Este documento será assinado eletronicamente.

[LOCAL], [DIA] de [MÊS] de [ANO].

_____

Nome: **[NOME DO COLABORADOR]**

E-mail: **[E-MAIL DO COLABORADOR]**

ANEXO II - TERMO DE ADESÃO ÀS ALTERAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, **[NOME DO COLABORADOR]**, inscrito no CPF sob o nº **[número do CPF]**, declaro ter conhecimento das alterações à Política Segurança da Informação e Segurança Cibernética, publicada internamente sob o código **PI_PSISC_002**, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da Inovanti.

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do e-mail contido nesta Política.

Este documento será assinado eletronicamente.

[LOCAL], [DIA] de [MÊS] de [ANO].

_____

Nome: **[NOME DO COLABORADOR]**

E-mail: **[E-MAIL DO COLABORADOR]**

ANEXO III - DIVULGAÇÃO DAS LINHAS GERAIS DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DA INOVANTI INSTITUIÇÃO DE PAGAMENTO S.A.

INTRODUÇÃO

Na Inovanti, oferecemos soluções de pagamento para nossos Clientes, na abertura de contas de pagamento, gestão das contas e dos recursos financeiros, e pagamentos recorrentes.

E como nosso negócio é pautado em tecnologia, temos o objetivo de implementar e manter a nossa Política de Segurança da Cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados. Bem como a privacidade dos dados de nossos clientes, colaboradores, fornecedores e prestadores de serviços.

Aqui nós divulgamos as linhas gerais da Política de Segurança Cibernética da instituição, que definem os critérios e diretrizes para preservar e proteger as informações contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade a incidentes, e dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

ASPECTOS GERAIS

Nós da Inovanti temos o compromisso de garantir a segurança e o tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos princípios de segurança da informação, de:

- ✓ Autenticidade: garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação;

- ✓ Confidencialidade: garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
- ✓ Disponibilidade: garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário;
- ✓ Integridade: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

PROCEDIMENTOS E CONTROLES ADOTADOS

Através dessa Política, adotamos procedimentos e controles que buscam reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, partindo sempre do comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, tais como:

- ✓ Autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;
- ✓ Procedimentos e controles que são adotados pela Inovanti, serão aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição;
- ✓ Controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis;
- ✓ Plano de ação e de resposta a incidentes, bem como o registro, a análise da causa e o impacto, e o controle dos efeitos de incidentes relevantes para as atividades da Inovanti;
- ✓ Diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

- ✓ Definição de procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Inovanti;
- ✓ Classificação dos dados e as informações quanto à relevância;
- ✓ Definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- ✓ Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo: (i) a implementação de programas de capacitação e de avaliação periódica de pessoal; e, a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos;
- ✓ Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;
- ✓ Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros; e,
- ✓ Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela Inovanti.

A Política de Segurança Cibernética e o Plano de Ação e de Resposta a Incidentes serão revisados minimamente uma vez por ano.

PROCEDIMENTOS PARA CONTRATAÇÃO DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

A Inovanti, procura assegurar que todas as diretrizes, estratégias e estruturas quanto a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior, estejam alinhadas com sua Política e procedimentos.

Para isso, adotamos procedimentos que contemplam:

- ✓ As boas práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado, no País ou no exterior, e respectivos riscos a que estejamos expostos;
- ✓ Validamos a capacidade de nossos prestadores de serviços de assegurar: o cumprimento da legislação e da regulamentação em vigor; o acesso da Inovanti aos dados e às informações a serem processados ou armazenados; a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados; a aderência de nossos prestadores quanto a certificações exigidas para a prestação do serviço a ser contratado; o acesso aos relatórios elaborados relativos aos procedimentos e aos controles utilizados na prestação dos serviços; a identificação e a segregação dos dados dos clientes da Inovanti por meio de controles físicos ou lógicos; e a qualidade dos controles de acesso voltados à proteção dos dados e das informações de nossos Clientes.