POLÍTICA DE SEGURANÇA CIBERNÉTICA

INDICE

1. OBJETIVO

Estabelecer as diretrizes e os princípios de Segurança Cibernética e Segurança da Informação aplicáveis à Placarpay S.A. – Sociedade de Crédito, Financiamento e Investimento ("Instituição" e "Placar Pay"), visando proteger seus ativos de informação, sistemas, ambientes tecnológicos e dados internos e de clientes contra ameaças cibernéticas, acessos não autorizados, indisponibilidades, vazamentos, perdas, alterações indevidas ou qualquer comprometimento da confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações.

A presente Política também tem como objetivo estabelecer diretrizes para:

a) gestão de riscos cibernéticos;
b) prevenção, detecção e resposta a incidentes;
c) gestão de acessos e identidades;
d) contratação de serviços relevantes de tecnologia e computação em nuvem;
e) continuidade de negócios;
f) proteção de dados pessoais;
g) conscientização e cultura de segurança;
h) atendimento às exigências regulatórias, legais e contratuais aplicáveis.

2. REGRAS GERAIS

2.1. PRINCÍPIOS

O processo de Segurança Cibernética e Segurança da Informação da Instituição, cujo objetivo é proteger as informações do negócio e clientes, é pautado pelos princípios fundamentais de: Confidencialidade, Disponibilidade e Integridade.

- **Confidencialidade:** Garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário.
- **Disponibilidade:** Garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário.
- **Integridade:** Garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.
- **Autenticidade**: Garantir a legitimidade, origem e validade das informações, comunicações, acessos e transações realizadas nos ambientes tecnológicos da Instituição.

Neste contexto a Instituição determina como diretrizes gerais os pontos abaixo elencados:

a) Garantir a privacidade, integridade, disponibilidade e confidencialidade das informações dos seus clientes e da própria Instituição, protegendo os dados e os sistemas de informação contra acessos indevidos e modificações não autorizadas;

b) Promover a aderência às leis e regulamentações aplicáveis à privacidade de dados e de proteção financeira de seus clientes, sendo este compromisso transmitido aos seus colaboradores, contratados e prestadores de serviço;

c) Assegurar que somente pessoas autorizadas tenham acesso às instalações da Placar Pay, às informações e aos sistemas de informação;

d) Garantir e proteger os processos críticos de negócio contra falhas ou desastres significativos;

e) Atender aos requisitos regulamentares, legais e contratuais pertinentes à sua atividade;

f) Assegurar a conscientização contínua sobre os procedimentos de segurança da informação;

g) Garantir que os recursos tecnológicos disponibilizados pela Instituição aos colaboradores estejam devidamente protegidos por controles eficazes contra ataques cibernéticos, infecções por malware e vazamento de dados;

h) Restringir o acesso às informações sensíveis de acordo com a necessidade de conhecimento para o negócio;

i) Identificar, avaliar, monitorar e tratar periodicamente os riscos cibernéticos e de segurança da informação aos quais a Instituição esteja exposta;

j) Registrar, investigar, tratar e monitorar os incidentes de segurança cibernéticos relevantes, bem como analisar as suas causas e os impactos deles decorrentes;

k) Criar e manter procedimentos para gerenciar os acessos de terceiros às informações sensíveis;

l) Classificar todas as informações de acordo com a Classificação da Informação;

m) Garantir que os colaboradores, prestadores de serviços, terceiros, fornecedores e parceiros observem obrigações de confidencialidade, segurança da informação, proteção de dados e uso adequado dos ativos tecnológicos, mediante formalização contratual apropriada.

2.2. DEFINIÇÕES

2.2.1. Segurança Cibernética

Conjunto de processos, controles e práticas que visam proteger a confidencialidade e integridade das redes, computadores e sistema de dados de ataques cibernéticos ou acesso não autorizado a informações da instituição e dos clientes.

2.2.2. Incidentes

São considerados Incidentes de Segurança Cibernética quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco.

2.2.3. Informação Confidencial

As informações que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa.

2.2.4. Informação Restrita

Informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores.

2.2.5. Informação de Uso Interno

Informações que não podem ser divulgadas para pessoas de fora da organização e com restrição de uso apenas para uso interno na empresa.

2.2.6. Informação Pública

Dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

2.2.7. Proprietário da Informação

Pessoa ou área responsável pela classificação, autorização de acesso, revisão periódica e adequada utilização das informações sob sua responsabilidade.

2.2.8. Ativo de Informação

Qualquer dado, sistema, ambiente, infraestrutura, aplicação, dispositivo, serviço tecnológico ou informação que possua valor para a Instituição e que necessite de proteção adequada.

2.3. GESTÃO DE SEGURANÇA CIBERNÉTICA

2.3.1 Controle de Acesso Lógico

O acesso às informações e aos ambientes tecnológicos da Instituição deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

a) A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);

b) A remoção de autorizações dadas a usuários afastados ou desligados, ou ainda que tenham mudado de função;

c) A revisão periódica das autorizações concedidas;

d) Utilização de mecanismos adicionais de autenticação para acessos privilegiados, acessos remotos e sistemas críticos, sempre que aplicável;

e) Revisão periódica dos acessos privilegiados e das contas administrativas; e

f) Segregação lógica entre ambientes de desenvolvimento, homologação e produção.

Os procedimentos relativos ao controle de acesso lógico estão devidamente detalhados e descritos no procedimento específico.

2.3.2 Contratação de Serviços

Os contratos celebrados entre a Placar Pay e as empresas prestadoras de serviços com acesso às suas informações e/ou ao seu ambiente tecnológico devem conter cláusulas com o objetivo de preservar a confidencialidade entre as partes e assegurar, no mínimo, que os profissionais sob sua responsabilidade:

a) Observem e cumpram com os requisitos estabelecidos, bem como as demais leis, regulamentos e normas aplicáveis (ex.: que tratem de aspectos atinentes a propriedade intelectual e preservação do sigilo bancário);

b) Assegurem que as informações, os sistemas e o ambiente tecnológico à sua disposição sejam utilizados apenas para as finalidades autorizadas pela Instituição;

c) Comuniquem imediatamente à área de Segurança da Informação sobre qualquer descumprimento ou violação a esta Política;

d) Permitam à Instituição realizar avaliações, diligências ou auditorias relacionadas à segurança da informação e proteção de dados, diretamente ou por terceiros autorizados;

e) Estabeleçam obrigações de comunicação tempestiva sobre incidentes de segurança cibernética; e

f) Prevejam controles mínimos relacionados à continuidade de negócios, proteção de dados, gestão de acessos e subcontratação de serviços críticos.

2.3.3 Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem

A Placar Pay deve realizar, antes da contratação, uma análise do prestador de serviços, com o objetivo de avaliar a sua capacidade de aderência à requisitos mínimos da Resolução CMN 4.893/21, conforme procedimentos internos, e classificar o serviço como grau de relevância alta, média e baixa.

a) Alta Relevância

- Manipulação de dados confidenciais ou;
- A interrupção do serviço impacta diretamente o funcionamento das atividades da instituição ou fornecimento de serviços a clientes.

b) Média Relevância

- Manipulação de dados restritos e/ou de uso interno ou;
- A interrupção do serviço impacta indiretamente o funcionamento das atividades da instituição ou fornecimento de serviços a clientes.

c) Baixa Relevância

- Manipulação de dados de uso interno e/ou públicos e;
- A interrupção do serviço não impacta o funcionamento das atividades da instituição ou fornecimento de serviços a clientes.

Para a classificação do serviço, deve ser analisado respectivamente na ordem de Alta Relevância, Média Relevância e Baixa Relevância. Para enquadrar nos dois primeiros níveis o serviço precisa atender apenas 1 (um) dos itens listados na categoria, porém para atendimento ao terceiro nível, o serviço precisa atender simultaneamente os 2 (dois) itens listados.

2.3.4 Comunicação ao Banco Central do Brasil

A área de Tecnologia da Informação deve comunicar ao Banco Central, os serviços classificados como Alta Relevância até 10 (dez) dias após a contratação.

A contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem deverá observar os requisitos regulatórios aplicáveis, incluindo eventual necessidade de comunicação ao Banco Central do Brasil, nos termos da regulamentação vigente.

2.4. GESTÃO DE INCIDENTES

Todos os incidentes relacionados à segurança cibernética devem ser reportados a área de Tecnologia da Informação - Segurança de Informação para identificação e elaboração de Plano de Ação para sua resolução.

Os incidentes classificados com alta relevância serão reportados mensalmente para a Diretoria e para a área de Gestão de Riscos, bem como sua efetiva resolução.

A classificação da relevância dos incidentes deve seguir a diretrizes abaixo:

a) Alta Relevância

- Incidente relacionado a segurança dos dados dos clientes ou da instituição, que possa acarretar vazamento e exposição do dado, infringindo os requisitos regulamentares, legais e contratuais;
- Incidente relacionado ao ambiente cibernético que possa acarretar interrupção atividades da instituição ou fornecimento de serviços a clientes.

b) Média Relevância

- Incidentes que, embora não comprometam diretamente a continuidade operacional ou dados sensíveis, possam gerar impactos operacionais, financeiros, regulatórios ou reputacionais moderados.

c) Baixa Relevância

- Demais incidentes relacionados à segurança de sistemas, rede ou informação.

2.4.1. Plano de Ação e de Resposta a Incidentes

O Plano de Ação e de Resposta a Incidentes tem o objetivo de formalizar o plano de ação da instituição para aderência a Resolução CMN nº 4.893/21 e adequação as diretrizes desta política, bem como formalizar o conjunto de rotinas, procedimentos, controles e as tecnologias a serem utilizadas na prevenção e resposta aos incidentes ocorridos.

A área de Tecnologia da Informação deve elaborar adicionalmente, o relatório anual de implantação do plano de ação e de resposta a incidentes contendo as principais ações para atendimento a Resolução CMN nº 4.893/21 e os resultados na implantação de rotinas e procedimentos utilizados na prevenção e resposta a incidentes.

O Plano de Resposta a Incidentes deverá contemplar, minimamente, procedimentos de identificação, contenção, análise, erradicação, recuperação, comunicação, registro de evidências e lições aprendidas decorrentes dos incidentes cibernéticos identificados.

2.5. CONTROLES

Visando reduzir a vulnerabilidade na estrutura tecnológica, a Instituição adota procedimentos e controles que busquem minimizar o risco de falhas e assegurar a administração segura de redes de comunicações.

a) Autenticação

O acesso às informações e aos ambientes tecnológicos deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

b) Criptografia

Toda solução de criptografia utilizada deve seguir as regras de Segurança da Informação e os padrões de segurança dos órgãos reguladores.

c) Prevenção de vazamento de informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

d) Testes e varreduras

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

e) Proteção contra softwares maliciosos

Todos os ativos (computadores, servidores etc.) que estejam conectados à rede corporativa ou façam uso de informações da Instituição, devem, sempre que compatível, ser protegidos com uma solução *anti-malware* determinada pela área de Tecnologia da Informação.

f) Rastreabilidade

As trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os eventos de autenticação de usuários; acesso a informações; ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

g) Cópias de Segurança

O processo de execução de *backups* é realizado periodicamente nos ativos de informação, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

h) Teste de Vulnerabilidade

Os testes de vulnerabilidade serão aplicados para todas as soluções contratadas pela Placar Pay.

As novas contratações sistemas que são classificados como alta relevância são testados antes da implantação do sistema no ambiente de produção.

Semestralmente, todas as soluções contratadas pela Instituição devem ser testadas.

As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

i) Gestão de Vulnerabilidades e Correções

A Instituição deverá manter processo periódico de identificação, avaliação, priorização e tratamento de vulnerabilidades de segurança, incluindo aplicação de correções, atualizações e *hardening* dos ambientes tecnológicos, observando criticidade, risco e exposição dos ativos envolvidos.

2.6. CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade de Negócios da instituição abrange o tratamento de incidentes relacionados ao ambiente cibernético e os procedimentos a serem seguidos no caso de interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados.

As responsabilidades, estratégias e procedimentos relativos à continuidade de negócios, bem como a elaboração de cenários de testes para incidentes relacionados ao ambiente cibernético, estão devidamente detalhados e descritos na Política de Continuidade de Negócios.

2.7. TREINAMENTO

A Instituição deverá promover programa contínuo de conscientização e treinamento em Segurança Cibernética e Segurança da Informação, aplicável a colaboradores, terceiros e prestadores de serviços, contemplando ações periódicas de capacitação, reciclagem e disseminação de boas práticas, de forma compatível com as funções exercidas e com os riscos identificados.

Os treinamentos deverão abordar, minimamente:

a) proteção de dados e sigilo das informações;
b) prevenção a ataques cibernéticos;
c) *phishing* e engenharia social;
d) uso seguro dos recursos tecnológicos;
e) gestão de senhas e acessos;
f) reporte de incidentes;
g) responsabilidades previstas nesta Política.

3. RESPONSABILIDADES

3.1. DIRETORIA

a) Aprovar a política de Segurança da Cibernética e o Plano de Ação e de Resposta a Incidentes;
b) Acompanhar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes;
c) Nomear o diretor responsável pela estrutura de segurança cibernética;
d) Assegurar que a estrutura remuneratória adotada não incentive comportamentos incompatíveis com um nível de risco considerado prudente e definido nas políticas e estratégias de longo prazo adotadas;
e) Assegurar a aderência da instituição às políticas e às estratégias de segurança cibernética;
f) Assegurar a correção tempestiva das deficiências da estrutura de segurança cibernética;
g) Disseminar a cultura de segurança cibernética por toda a organização para que o tema seja difundido de forma ampla e completa entre todos;
h) Adotar medidas cabíveis para garantir a confidencialidade, integridade e disponibilidade das informações;
i) Assegurar a disponibilização de recursos humanos, tecnológicos e financeiros adequados para implementação e manutenção da estrutura de segurança cibernética e segurança da informação.

3.2. TECNOLOGIA DA INFORMAÇÃO - TI

a) Operacionalizar as normas e procedimentos relacionados a esta Política, por meio dos recursos de TI, que visam garantir a segurança cibernética;
b) Conduzir a gestão da Segurança da Informação;
c) Criar e revisar os procedimentos de Segurança da Informação;

d) Definir, selecionar, garantir a implementação e revisar os controles e/ou soluções técnicas aderentes aos requisitos de segurança da informação;

e) Registro, controle e acompanhamento das não-conformidades relacionadas à segurança cibernética;

f) Desenvolver, acompanhar a implantação e manter planos de continuidade relacionados a TI;

g) Identificar, avaliar, monitorar e tratar os riscos cibernéticos e de segurança da informação relacionados aos ativos e ambientes tecnológicos da Instituição;

h) Providenciar meios eletronicamente seguros para a transmissão e arquivamento das informações classificadas como confidenciais;

i) Promover ampla divulgação, orientação e treinamento desta política para todos os usuários;

j) Coordenar a gestão de identidades, incluindo os processos de concessão, manutenção, revisão e suspensão de acesso dos usuários aos sistemas de informação e recursos computacionais;

k) Preservar a Segurança da Informação em ambientes compartilhados com outras instituições, através de acordos, cooperações técnicas, parcerias, e demais situações de interesse da instituição;

l) Manter os logs e trilhas de auditoria de ativos de infraestrutura de TI, a fim de garantir o processo de rastreabilidade observando critérios de retenção, integridade, disponibilidade e rastreabilidade aplicáveis;

m) Elaborar e manter atualizada a Política, Procedimentos e Manuais pertinentes a Segurança da Informação;

n) Atuar na identificação, análise técnica, contenção, tratamento e recuperação de incidentes cibernéticos, em conjunto com as áreas competentes, quando aplicável;

o) Elaborar o Relatório Anual sobre a implementação do plano de ação e de resposta a incidentes;

p) Reportar para a Diretoria relatórios periódicos sobre o tema segurança cibernética;

q) Apoiar os processos de avaliação regulatória e eventual comunicação ao Banco Central do Brasil relacionados à contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, quando aplicável .

3.3. INFRAESTRUTURA DE TI

a) Manter todos os sistemas de informação em níveis aceitáveis de Segurança da Informação;

b) Monitorar a infraestrutura tecnológica para garantir o cumprimento desta Política;

c) Gerenciar antivírus e varredura periódica da infraestrutura tecnológica, bem como processos de atualização, correção de vulnerabilidades e *hardening* dos ativos tecnológicos;

d) Gerenciar solução tecnológica para Prevenção ao Vazamento de Informações e controle de dispositivos removíveis e garantir que todos os computadores estejam preparados para seguir as regras estipuladas nesta Política e instrumentos normativos;

e) Homologar e especificar os programas de computador autorizados a serem utilizados pelos usuários;

3.4. JURÍDICO

O Jurídico deverá apoiar a adequação contratual dos instrumentos celebrados com terceiros, fornecedores, parceiros e prestadores de serviços, observando os requisitos legais, regulatórios e contratuais relacionados à segurança da informação, proteção de dados, confidencialidade, continuidade de negócios e segurança cibernética.

3.5. GESTÃO DE RISCOS

Avaliar, monitorar e acompanhar os riscos relacionados aos processos e ambientes tecnológicos da Instituição, apoiando a identificação, mensuração e tratamento dos riscos cibernéticos e de segurança da informação.

3.6. RECURSOS HUMANOS - RH

a) Assegurar que todo novo colaborador esteja ciente das diretrizes e/ou das normas e procedimentos de Segurança da Informação, por meio da participação do treinamento de integração;

b) Colher assinatura dos usuários no Termo de Uso dos Sistemas de Informação e Recursos Computacionais;

c) Guardar os Termos de Uso dos Sistemas de Informação e Recursos Computacionais assinados pelos usuários;

d) Comunicar tempestivamente a área de Tecnologia da Informação a ausência, desligamento ou afastamento de usuário para bloqueio ou revogação de credenciais de acesso físico e a recursos computacionais;

e) Garantir que os ativos de informação confiados aos usuários sejam devolvidos quando ocorrer desligamento ou afastamento.

3.7. COMPLIANCE

a) Avaliar se os normativos internos (Políticas, Procedimentos e Manuais) estão de acordo com a regulamentação vigente e melhores práticas;

b) Realizar o processo de publicação e divulgação dos documentos internos (políticas, procedimentos etc.) nas bases e sistemas apropriados de acesso dos colaboradores;

c) Realizar o controle de todos os documentos emitidos e garantir que o processo de revisão e atualização junto aos responsáveis ocorra periodicamente;

d) Garantir que o processo de aprovação de todos os documentos ocorra conforme as regras e alçadas estabelecidas.

3.8. GESTORES

a) Gerenciar as informações geradas ou confiadas à área de negócio sob sua responsabilidade, durante todo o seu ciclo de vida;

b) Transmitir aos usuários sob sua responsabilidade as regras desta Política;

c) Controlar as informações geradas em sua área de negócio e atuação;

d) Identificar e classificar as informações conforme critérios e procedimentos adotados pela Instituição;

e) Comunicar à Tecnologia da Informação – Segurança da Informação a ausência ou o desligamento de usuários especiais como terceiros e consultores para bloqueio ou revogação de credenciais de acesso aos recursos computacionais;

f) Revisar periodicamente a classificação das informações;

g) Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

h) Comunicar tempestivamente incidentes, desvios ou fragilidades relacionadas à segurança das informações sob sua responsabilidade

3.9. USUÁRIOS DA INFRAESTRUTURA TI

a) Assegurar que os recursos tecnológicos sejam utilizados apenas para as finalidades autorizadas pela Instituição;

b) Adotar medidas cabíveis de segurança que estejam ao seu alcance, visando sempre proteger as informações da Instituição;

c) Utilizar as informações da Instituição exclusivamente para os objetivos do negócio e jamais para fins pessoais;

d) Não compartilhar ou divulgar senhas de usuário, uma vez que a senha é individual, intransferível e de responsabilidade do usuário;

e) Manter informações e documentos confidenciais, em papel ou em mídias eletrônicas, protegidos e armazenados em gavetas, armários ou cofre, especialmente quando se ausentar de sua mesa de trabalho;

f) Manter sigilo sobre todas as informações que venha a tomar conhecimento em virtude das suas atividades profissionais junto a Instituição, o que permanecerá em vigor e vinculará legalmente o usuário enquanto vigorar o regime jurídico a que estiver submetido, vigorando, ainda, após a eventual rescisão, a qualquer título, por qualquer das partes, de maneira permanente, sob pena do direito da Instituição pleitear o ressarcimento das perdas e danos decorrentes da violação do sigilo pelo usuário, sem prejuízo das sanções legais;

g) Notificar a área de Tecnologia da informação de qualquer incidente relacionado ao ambiente cibernético.

4. DOCUMENTOS INTERNOS RELACIONADOS

- Política de Segurança da Informação;
- Política de Continuidade de Negócios.

5. REGULAMENTAÇÃO EXTERNA

- **Resolução CMN nº 4.893/2021** – Que 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 a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil;
- Resolução BCB nº 85/2021 – Dispõe sobre a política de segurança cibernética e requisitos para processamento e armazenamento de dados e computação em nuvem aplicáveis às instituições de pagamento;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- ABNT NBR ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2022 – Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2013

6. GLOSSÁRIO

- ***Anti-malware:*** É um software antivírus desenvolvido para detectar uma ampla variedade de malwares (software malicioso criado para danificar, espalhar ou fornecer acesso indesejado a um computador, dispositivo ou rede).
- **Ataques cibernéticos:** É uma ação praticada por hackers que consiste na transmissão de vírus (arquivos maliciosos) que infectam, danificam e roubam informações de computadores e demais bancos de dados online.
- **Backup:** É o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) para sistemas de armazenamento secundários, buscando a preservação dos dados em caso de qualquer problema.

- **Criptografia:** É a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de criptografia específica.

* * * * *

REGISTRO DAS ALTERAÇÕES

Versão	Data Publicação	Resumo da Alteração	Motivo	Área Responsável	Data Vencimento
01	30/04/2020	Revisão geral	Atualização do documento	Tecnologia da Informação	30/04/2021
02	10/09/2021	Revisão geral	Atualização do documento	Tecnologia da Informação	10/09/2022
03	08/09/2022	Revisão geral	Atualização do documento	Tecnologia da Informação	08/09/2023
04	14/05/2024	Revisão geral	Atualização do documento	Tecnologia da Informação	14/05/2025
05	15/06/2026	Revisão geral	Atualização do documento	Tecnologia da Informação	15/06/2027

Este documento deve ser revisado conforme exigência regulatória e sempre que desatualizado, no mínimo a cada 2 anos.

Em caso de dúvidas sobre o conteúdo deste documento, contate a área responsável.

Qualquer outro assunto em relação à publicação deste documento, fale com a área de Compliance.