# Política de Segurança da Informação e Cibernética

**Versão impressa deste Procedimento, sem autorização prévia do Sistema de Gestão da Qualidade, será considerada como Cópia não Controlada.**

## Sumário


01. Objetivo 4
02. Abrangência 4
03. Responsabilidades 4
04. Normas Aplicáveis 6
05. Definições 6
06. Princípios 7
08. Processo de Segurança da Informação e Cibernética 10
- 8.1. Gestão de Ativos ..... 10
- 8.2. Autenticação ..... 10
- 8.3. Autorização ..... 10
- 8.4. Segmentação de rede ..... 10
- 8.5. Classificação da Informação ..... 11
- 8.6. Controle de acesso ..... 11
- 8.7. Gestão de riscos ..... 12
- 8.8. Gestão de fornecedores ..... 12
- 8.9. Segurança física do ambiente ..... 13
- 8.10. Backup e gravação de LOG ..... 13
- 8.11. Proteção contra vírus, arquivos e softwares maliciosos ..... 13
- 8.12. Testes de varredura para detecção de vulnerabilidade ..... 14
- 8.13. Criptografia ..... 14

09. Plano de continuidade 14
10. Incidentes de segurança 15
- 10.1 Classificação de relevância dos incidentes ..... 15
- 10.2 Gestão de incidentes ..... 15
- 10.3 Plano de compartilhamento de incidentes ..... 15
- 10.4 Plano de ação e resposta a incidentes ..... 16
- 10.5 Relatório anual de incidentes ..... 16

11. Mecanismos de rastreabilidade 17
12. Registro de impacto 17
13. Treinamentos e conscientização 17
14. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem 18
15. Execução de aplicativos pela internet 19
16. Serviços de computação em nuvem 19
- 16.1 Contratação de serviços de computação em nuvem no exterior ..... 20

17. Contrato de prestação de serviços 21
18. Comunicação ao Bacen 23

19. Continuidade dos serviços de pagamento 23
20. Arquivamento de informações 24
21. Declaração de Responsabilidade 25
22. Histórico de Alterações | Modificações 26

## 01. Objetivo

Estabelecer diretrizes que permitam à **PROTEGE CASH** preservar e proteger suas informações, bem como a de seus clientes, funcionários, prestadores de serviços e partes interessadas contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da instituição quanto a incidentes. Esta Política também define requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pela **PROTEGE CASH** enquanto instituição de pagamento.

Esta Política será formulada e implementada 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. Esta Política é compatível com:

- O porte, o perfil de risco e o modelo de negócio da **PROTEGE CASH**;
- A natureza das atividades da **PROTEGE CASH** e a complexidade dos produtos e serviços oferecidos;
- A sensibilidade dos dados e das informações sob responsabilidade da **PROTEGE CASH.**

A **PROTEGE CASH** designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes. O diretor designado poderá desempenhar outras funções na instituição, desde que não haja conflito de interesses.

## 02. Abrangência

A Política se aplica a todos os colaboradores, incluindo a Alta Administração (diretores e administradores), Colaboradores e empresas prestadoras de serviço, que são responsáveis pelo estabelecimento de um ambiente permanente de controle, e no qual seja possível monitorar e atuar em todas as operações atinentes a esta Política.

## 03. Responsabilidades

São deveres e responsabilidades de implementação, execução e manutenção desta Política:

- **Área de Compliance:**

Responsável, em conjunto com o diretor responsável pela elaboração, manutenção e atualização anual ou a qualquer momento para contemplar quaisquer alterações regulatórias e outras obrigações legais, desta Política;

- **Diretor responsável pela execução e manutenção da Política:**

Responsável pela implementação, execução e manutenção desta política e pela execução do plano de ação e de resposta a incidentes, assim como, pela convocação das reuniões periódicas do comitê de segurança da informação e segurança cibernética;

- **Alta Administração:**

Responsável pela aprovação da Política e suas versões atualizadas;

- **Comitê de Segurança da Informação e Segurança Cibernética:**

Comitê formado pelo Diretor responsável por esta Política, e por Colaboradores indicados pelas áreas de **PROTEGE CASH** e aprovadas pela Alta administração, com o objetivo de deliberar a respeito de assuntos relacionados à Segurança da Informação e Cibernética, e a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;

- **Colaboradores:**

Alta Administração e Colaboradores da **PROTEGE CASH**, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da **PROTEGE CASH**, e que devem, no que couber:

Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política;

Informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivos, serviços ou processos relacionados à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva;

Utilizar as informações relacionadas à esta Política, como patrimônio da **PROTEGE CASH,** e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

## 04. Normas Aplicáveis

**Lei nº 12.865/2013:** dispõe sobre os Arranjos de Pagamento e as Instituições de Pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).

**Resolução BCB n° 1 de 12/8/2020:** Institui o arranjo de pagamentos Pix e aprova o seu Regulamento.

**Resolução BCB n° 80/2021**: estabelece os requisitos e os procedimentos para constituição e funcionamento, e de pedido de autorização de funcionamento das Instituições de Pagamento, e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Bacen.

**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.

## 05. Definições

**Ativos**: todas as formas de tratamento de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.

**Alta Administração**: Formado pelos sócios e administradores da PROTEGE CASH.

**Bacen:** Banco Central do Brasil.

**Gestão de Ativos:** são as boas práticas utilizadas pela **PROTEGE CASH** 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.

**Instituição de Pagamento:** para fins desta Política, é a **PROTEGE CASH** como emissora de moeda eletrônica, cuja atividade consiste em gerenciar a Conta de Pagamento de Usuários, utilizada para o pagamento de transações pré-pagas.

**Log:** registro de eventos de um sistema.
**Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da **PROTEGE CASH**.

**Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da **PROTEGE CASH** contra danos, ataques, ameaças ou acesso não autorizado.

**PROTEGE CASH:** Protege Cash Instituição de Pagamento S.A.

## 06. Princípios

A **PROTEGE CASH** tem o compromisso garantir a segurança e o tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

- **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.

## 07. Diretrizes Gerais

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

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 **PROTEGE CASH.**

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 **PROTEGE CASH** adotará mecanismos que visam a assegurar a utilização segura de senhas.

Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela **PROTEGE CASH.**

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.

Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.

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.

Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis.

Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da **PROTEGE CASH**, como Instituição de Pagamento.

Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

Definir os 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 **PROTEGE CASH**;

Classificar os dados e as informações quanto à relevância;

Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;

Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:

- A implementação de programas de capacitação e de avaliação periódica de pessoal;
- 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 Bacen.

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.
Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela **PROTEGE CASH** e por esta Política.

## 08. 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 **PROTEGE CASH** adotará políticas e procedimentos para os processos elencados a seguir.

### 8.1. 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 **PROTEGE CASH** 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.

### 8.2. Autenticação

A **PROTEGE CASH** adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados.

### 8.3. Autorização

Prever processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

### 8.4. Segmentação de rede

A **PROTEGE CASH** 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.

### 8.5. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a **PROTEGE CASH** deve adotar a seguinte classificação:

**Informação Pública**: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;

**Informação Interna**: aquela que pode ser acessada somente por Colaboradores da **PROTEGE CASH** São exemplos de Informação Interna: normas, procedimentos e formulários da **PROTEGE CASH.**

**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 **PROTEGE CASH.**

**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.

### 8.6. Controle de acesso

A **PROTEGE CASH** 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 **PROTEGE CASH** 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.

### 8.7. Gestão de riscos

A **PROTEGE CASH** 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 **PROTEGE CASH**, 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 **PROTEGE CASH**, com o objetivo da preparação para essas situações.

Neste processo, será levado em conta: o levantamento dos impactos organizacionais; a priorização das ações de mudanças no ambiente de tecnologia da **PROTEGE CASH**; o planejamento; os testes; a mobilização; a comunicação; e 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 **PROTEGE CASH.**

### 8.8. Gestão de fornecedores

A **PROTEGE CASH** 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 **PROTEGE CASH**, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A **PROTEGE CASH** deve disponibilizar um canal para que seus prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da **PROTEGE CASH.**

### 8.9. Segurança física do ambiente

A **PROTEGE CASH** deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros 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.

### 8.10. Backup e gravação de LOG

A **PROTEGE CASH** deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.
A **PROTEGE CASH** também deve realizar 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.

### 8.11. Proteção contra vírus, arquivos e softwares maliciosos

A **PROTEGE CASH** deve adotar 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 **PROTEGE CASH** a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, devem estar instalados e atualizados em toda a rede interna da **PROTEGE CASH.**

### 8.12. Testes de varredura para detecção de vulnerabilidade

A **PROTEGE CASH** 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 **PROTEGE CASH** 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 **PROTEGE CASH.**

### 8.13. Criptografia

Os Ativos de informação da **PROTEGE CASH** 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.

## 09. Plano de continuidade

A **PROTEGE CASH** 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 da **PROTEGE CASH** sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a **PROTEGE CASH** 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 **PROTEGE CASH** certifique a conformidade dos planos desenvolvidos com os objetivos da Instituição de Pagamento e requisitos legais.

## 10. Incidentes de segurança

### 10.1 Classificação de relevância dos incidentes

A **PROTEGE CASH** classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios da instituição.

### 10.2 Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável e ao Diretor responsável por esta Política, no que couber.

A comunicação deverá ser feita por meio dos canais indicados pela **PROTEGE CASH** através do e-mail segurança.informacao@protege.com.br
Os incidentes reportados serão classificados segundo o risco que representam para a **PROTEGE CASH** e respectivo impacto na continuidade dos negócios da Instituição de Pagamento. Além disso, devem ser devidamente registrados, tratados e comunicados.

A **PROTEGE CASH** 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.

### 10.3 Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a **PROTEGE CASH** deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com outras Instituições de

Pagamento 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 **PROTEGE CASH** 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.

### 10.4 Plano de ação e resposta a incidentes

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

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

### 10.5 Relatório anual de incidentes

A **PROTEGE CASH** deve 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 efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
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;

Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

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 à Alta Administração da **PROTEGE CASH** até 31 de março do ano seguinte ao da data-base.

## 11. Mecanismos de rastreabilidade

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

## 12. Registro de impacto

A **PROTEGE CASH** deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da **PROTEGE CASH**, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

## 13. Treinamentos e conscientização

A **PROTEGE CASH** preza por uma cultura 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 toda a Alta Administração e todos os seus Colaboradores.

A **PROTEGE CASH** promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, no que couber, 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, a Alta Administração da **PROTEGE CASH** deverá 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.

## 14. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

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

O cumprimento da legislação e da regulamentação em vigor;

O acesso da **PROTEGE CASH** aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

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

A aderência do prestador de serviço a certificações exigidas pela **PROTEGE CASH** para a prestação do serviço a ser contratado;

O acesso da **PROTEGE CASH** 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;

O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

A identificação e a segregação dos dados dos usuários finais da **PROTEGE CASH** por meio de controles físicos ou lógicos;
A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da **PROTEGE CASH.**

Na avaliação da relevância do serviço a ser contratado, a **PROTEGE CASH** 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 **PROTEGE CASH** 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.

## 15. Execução de aplicativos pela internet

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

## 16. Serviços de computação em nuvem

Os serviços de computação em nuvem, Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à **PROTEGE CASH** implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela **PROTEGE CASH** ou por ela adquiridos;

Implantação ou execução de aplicativos desenvolvidos pela **PROTEGE CASH**, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;

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

A **PROTEGE CASH** é responsável, em conjunto com o prestador de serviços, 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 **PROTEGE CASH** ao Bacen.

### 16.1 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 **PROTEGE CASH** deverá observar os seguintes requisitos:
Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;

Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;

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;

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 **PROTEGE CASH** 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 **PROTEGE CASH** deverá solicitar autorização 60 dias antes da alteração contratual.

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

## 17. Contrato de prestação de serviços

A **PROTEGE CASH** deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:
A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados.

A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais.

Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à **PROTEGE CASH**, 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.

O acesso da **PROTEGE CASH** 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;

A obrigação da empresa contratada notificar a **PROTEGE CASH** sobre a subcontratação de serviços relevantes para a **PROTEGE CASH**; 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.

A adoção de medidas pela **PROTEGE CASH,** em decorrência de determinação do Bacen;
A obrigação de a empresa contratada manter a **PROTEGE CASH** 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 **PROTEGE CASH** pelo Bacen, o contrato de prestação de serviços deve prever:

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;

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:

- 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;

- A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da **PROTEGE CASH**.

## 18. 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:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- 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 prevista no item 18 “d”.

## 19. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a **PROTEGE CASH** deve assegurar:
O tratamento dos incidentes relevantes relacionados com o ambiente cibernético.

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 **PROTEGE CASH**.
Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.

O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados.

O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos.

A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela **PROTEGE CASH**, bem como das providências para o reinício das suas atividades.
Estabelecer e documentar os critérios que configurem a situação de crise.

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

- O documento relativo à política de Segurança Cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- O relatório anual sobre a implementação do plano de ação de resposta a incidentes, com data-base em 31 de dezembro.

A documentação sobre os procedimentos que contemplem a verificação da capacidade do potencial prestador de serviço de assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso 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 a certificações exigidas para a prestação do serviço a ser contratado, o acesso aos relatórios elaborados por empresa de auditoria especializada independente;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais por meio de controles físicos ou lógicos; e a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados;
- A documentação com os critérios que configurem a situação de crise, bem como das providências para o reinício das suas atividades.

## 21. Declaração de Responsabilidade

Os Colaboradores da **PROTEGE CASH** devem aderir formalmente e se comprometerem a agir de acordo com esta Política.

Os contratos celebrados com terceiros pela **PROTEGE CASH** e que tratem de Ativos de informação referentes a esta Política devem possuir cláusula que assegure a segurança das informações.

## 22. Histórico de Alterações | Modificações

| REVISÃO | MODIFICAÇÃO | DATA | RESPONSÁVEL |
|---|---|---|---|
| 00 | Primeira versão | 24/04/22 | Departamento da Segurança da Informação |
| 01 | Revisão | 09/11/22 | Carolina de Almeida Ventura |
| 02 | Revisão | 15/05/23 | Fernanda Pirani |
| 03 | Revisão anual, atualização do padrão, ajuste na nomenclatura e alteração do código da política. | 16/08/24 | Fernanda Pirani |
| 04 | Revisão para a alteração da denominação social da empresa. | 10/02/2025 | Fernanda Pirani |
| 05 | Atualização da Logomarca. | 27/03/2025 | Fernanda Pirani e Nathália Julia – Segurança da Informação |

# Política de Segurança da Informação e Segurança Cibernética V5 pdf

Código do documento e839176c-1670-4b32-a872-73a152e7885c

## Assinaturas

Fernanda Pirani Correia da Silva
fernanda.silva@protege.com.br
Assinou




Ivan Burti Genaro de Castro
ivan.castro@protege.com.br
Assinou

flavio baptista de oliveira
flavio.baptista@protege.com.br
Assinou


## Eventos do documento

**02 Apr 2025, 17:00:51**
Documento e839176c-1670-4b32-a872-73a152e7885c **criado** por DANIELA GARCIA ONHA MANUGUERRA (3ee01b9e-053e-4e1e-a6f5-9bfd7bd09718). Email:Daniela.Garcia@protege.com.br. - DATE_ATOM: 2025-04-02T17:00:51-03:00

**02 Apr 2025, 17:03:02**
Assinaturas **iniciadas** por DANIELA GARCIA ONHA MANUGUERRA (3ee01b9e-053e-4e1e-a6f5-9bfd7bd09718). Email: Daniela.Garcia@protege.com.br. - DATE_ATOM: 2025-04-02T17:03:02-03:00

**02 Apr 2025, 17:44:29**
IVAN BURTI GENARO DE CASTRO **Assinou** (ded871fd-cdcd-435d-ba0c-dd7d8858d36a) - Email: ivan.castro@protege.com.br - IP: 201.64.101.226 (201.64.101.226 porta: 22850) - Geolocalização: -23.549794343749397 -46.65068893790201 - Documento de identificação informado: 339.160.328-36 - DATE_ATOM: 2025-04-02T17:44:29-03:00

**02 Apr 2025, 19:17:59**
FLAVIO BAPTISTA DE OLIVEIRA **Assinou** (27bfc69d-cf59-42cd-9eae-32bb6296a927) - Email: Flavio.Baptista@protege.com.br - IP: 201.64.101.226 (201.64.101.226 porta: 7652) - Geolocalização: -23.5405312 -46.6419712 - Documento de identificação informado: 588.223.216-34 - **Assinado com EMBED** - Token validado por **email** - DATE_ATOM: 2025-04-02T19:17:59-03:00

**07 Apr 2025, 10:48:03**
FERNANDA PIRANI CORREIA DA SILVA **Assinou** (42a4696f-fd13-4f3e-8496-a3670d6f5548) - Email:

28 páginas - Datas e horários baseados em Brasília, Brasil
**Sincronizado com o NTP.br e Observatório Nacional (ON)**
Certificado de assinaturas gerado em 07 de April de 2025, 10:48:58

fernanda.silva@protege.com.br - IP: 201.64.101.226 (201.64.101.226 porta: 20298) - Documento de identificação informado: 332.912.528-45 - DATE_ATOM: 2025-04-07T10:48:03-03:00

Hash do documento original

(SHA256):a1be7e5e741f6028c317f00135b675a43f10d8ed385b213fe20f3ddc88f2423c
(SHA512):516837dc377364a360b78edf1c85368ed92b9d9e944b474a1d8e31abcfbd96a2a6e0355eab7130d5bcae944e323cecabbc9854d687f263b4b753da22e525a98b

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

**Esse documento está assinado e certificado pela D4Sign**
**Integridade certificada no padrão ICP-BRASIL**
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.