BRINKS PAY

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

BRINKS PAY

Data: 17/06/2024 Versão: 01

Nome do Documento:	BP-SEG-POL-0001
Versão:	01
Fase:	Vigente
Classificação:	Interna
Área Gestora:	Tecnologia e Segurança da Informação
Responsável:	Guilherme do Carmo Jose
Revisor:	Carlos Eduardo Jacinto da Silva
Aprovador:	Carlos Eduardo Jacinto da Silva
Aprovador:	Leandro Barreira Nascimento
Aprovador:	Alexandre Bertoli da Costa
Áreas abrangentes:	Brink’s Pay

BRINKS PAY

Sumário

A. Escopo Dessa Política 5
1. Objetivo 5
2. Abrangência 5
3. Responsabilidades 5
4. Normas Aplicáveis 6
5. Aprovação e Revisão 6
6. Definições 6
B. Princípios 7
C. Diretrizes Gerais 7
D. Processo de Segurança da Informação e Cibernética 8
1. Gestão de Ativos 8
2. Autenticação 9
3. Segmentação de rede 9
4. Classificação da Informação 9
5. Controle de acesso 9
6. Gestão de riscos 10
7. Gestão de fornecedores 10
8. Segurança física do ambiente 10
9. Backup e gravação de Log 10
10. Proteção contra vírus, arquivos e softwares maliciosos 10
11. Testes de varredura para detecção de vulnerabilidade 10
12. Criptografia 11
13. Evasão de Dados 11
14. Plano de continuidade 11
15. Incidentes de segurança 12
a. Classificação de relevância dos incidentes 12
b. Gestão de incidentes 12
c. Plano de compartilhamento de incidentes 12
d. Plano de ação e resposta a incidentes 13
e. Relatório anual de incidentes 13
16. Mecanismos de rastreabilidade 13

17. Registro de impacto 13
18. Treinamentos e conscientização 14
19. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem 14
a. Seleção de terceiros 14
b. Execução de aplicativos pela internet 15
c. Serviços de computação em nuvem 15
d. Contratação de serviços de computação em nuvem no exterior 16
e. Contrato de prestação de serviços 16
f. Comunicação ao Bacen 17
20. Continuidade dos serviços de pagamento 18
21. Arquivamento de informações 18
22. Auditorias 19
E. Declaração de Responsabilidade 19
F. Disposições Gerais 19
1. Histórico de Versionamento 19
2. Revisores 20
3. Aprovadores 20
ANEXO I 21
ANEXO II 22

A. Escopo Dessa Política

1. Objetivo

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem à BRINK'S PAY preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria BRINK'S PAY contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da BRINK'S PAY a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A BRINK'S PAY 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.

Esta Política será compatível com:

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

A BRINK'S PAY possui um diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes.

2. Abrangência

A Política se aplica a todos os administradores (Conselho de Administração, Diretoria-Executiva, Superintendentes Executivos, Diretores e demais órgão diretivos da BRINK'S PAY, coletivamente "Alta Administração"), funcionários e prestadores de serviço[1] da BRINK'S PAY (coletivamente, "Colaboradores").

3. Responsabilidades

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

a. Área de Compliance: responsável, em conjunto com o Diretor responsável pela execução e manutenção desta Política, pela aprovação e atualização periódica da Política;
b. Diretor responsável pela execução e manutenção desta Política: responsável pela implementação, execução e manutenção da política, assim como, pela convocação das reuniões periódicas do comitê;
c. Comitê de Segurança da Informação e Segurança Cibernética: comitê formado por Colaboradores indicados pelas áreas da BRINK'S PAY e aprovadas pela Alta Administração, com o objetivo de deliberar a respeito de assuntos relacionados à esta Política;
d. Usuários: Alta Administração e Colaboradores da BRINK'S PAY, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou informações da BRINK'S PAY, e que devem, no que couber: (i) cumprir as normas e procedimentos relacionados ao uso de

1 Quaisquer terceiros que atuem em nome da BRINK'S PAY, tais como Auditoria Externa, Assessoria Jurídica, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

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 BRINK'S PAY, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

4. Normas Aplicáveis

Circular Bacen nº 3.909/2018: 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.

5. Aprovação e Revisão

Esta Política foi aprovada e revisada pela Alta Administração e será revisada com a periodicidade mínima de um ano. A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

6. Definições

Ativos: Todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis, etc.

Alta Administração: Conselho de Administração ou, se inexistente, Diretoria da BRINK'S PAY.

Bacen: Banco Central do Brasil.

Gestão de Ativos: São as boas práticas utilizadas pela BRINK'S PAY 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.

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

Instituição de Pagamento: Para fins desta Política, é a BRINK'S PAY.

Log: Registro de eventos de um sistema.

Segurança da Informação: Conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da BRINK'S PAY.

Segurança Cibernética: Conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da BRINK'S PAY contra, ataques, danos, ameaças ou acesso não autorizado.

B. Princípios

A BRINK'S PAY 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.

C. Diretrizes Gerais

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

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador é pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na BRINK'S PAY.
- Cada Colaborador, quando aplicável, recebe 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 BRINK'S PAY adota mecanismos que asseguram a complexidade, troca periódica e guarda de histórico de senhas.
- Qualquer risco à informação deve ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela BRINK'S PAY.
- Assegurar que todas as informações são tratadas de maneira ética e sigilosa e que são adotadas medidas capazes de evitar acessos indevidos, modificações, destruições ou divulgações não autorizadas.
- Assegurar que as informações são 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 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 BRINK'S PAY, 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 são adotados pelos prestadores de serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da BRINK'S PAY;
- Classificar os dados e as informações quanto à relevância;
- Definir os parâmetros 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.
- Assegurar as iniciativas para compartilhamento de informações sobre os incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen.
- Assegurar 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 BRINK'S PAY e por esta Política.

D. Processo de Segurança da Informação e Cibernética

A fim de assegurar que todas as diretrizes acima são cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética são devidamente seguidos, a BRINK'S PAY adota políticas e procedimentos para os processos elencados a seguir.

1. Gestão de Ativos

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

Os Ativos são utilizados tão somente para a finalidade devidamente autorizada. A BRINK'S PAY assegura 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 BRINK'S PAY adota mecanismos para garantir que o acesso às informações e ambientes tecnológicos é permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3. Segmentação de rede

A BRINK'S PAY adota mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determina 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 são classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a BRINK'S PAY adota 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 BRINK'S PAY. São exemplos de Informação Interna: normas, procedimentos e formulários da BRINK'S PAY;

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 BRINK'S PAY.

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 BRINK'S PAY adota controles de acesso em toda infraestrutura computacional 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 BRINK'S PAY implementa 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

A BRINK'S PAY 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.

7. Gestão de fornecedores

A BRINK'S PAY 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 BRINK'S PAY, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A BRINK'S PAY disponibiliza 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 BRINK'S PAY.

8. Segurança física do ambiente

A BRINK'S PAY implementa 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 são 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 BRINK'S PAY adota uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A BRINK'S PAY também realiza gravação de logs de dados permitindo a rastreabilidade do acesso e a identificação do criador, data, meios de acessos e informações acessadas. As informações dos logs são protegidas contra alterações e acessos não autorizados.

10. Proteção contra vírus, arquivos e softwares maliciosos

A BRINK'S PAY adota mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.x: phishing, spam, etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a BRINK'S PAY a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, são instalados e atualizados em toda a rede interna da BRINK'S PAY.

11. Testes de varredura para detecção de vulnerabilidade

A BRINK'S PAY 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, promove monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

A BRINK'S PAY 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 BRINK'S PAY.

12. Criptografia

Os Ativos de informação da BRINK'S PAY possuem criptografia adequada, conforme classificação da informação, 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. Evasão de Dados

A BRINK'S PAY adota mecanismos e estratégias para prevenir e tratar evasão de dados. Um incidente envolvendo vazamento de dados ameaça a confidencialidade, integridade e disponibilidade das informações causando impacto negativo aos negócios da empresa e afetando clientes e fornecedores. Definimos papeis e responsabilidades para cada membro responsável pela resposta aos incidentes envolvendo vazamento de dados, categorizamos a criticidade dos incidentes e definimos um fluxo de atuação.

a. Definição

Evasão de dados: quando os dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros sem autorização.

Dados Privados: qualquer informação sob a gestão da BRINK'S PAY que não seja considerada pública incluindo:

Informações de Identificação Pessoal: dados que direta ou indiretamente se vinculam a um indivíduo e possam ser usados para identificar alguém. Exemplos: Nome, RG, CPF, endereço de e-mail, número de telefone, número da conta bancária entre outros.

Dados de Clientes: qualquer informação não pública de clientes, fornecedores e parceiros utilizada pela BRINK'S PAY que são necessárias para execução dos serviços prestados.

14. Plano de continuidade

A BRINK'S PAY 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

BRINK'S PAY sejam devidamente identificados e preservados após a ocorrência de um evento que cause a indisponibilidade do serviço.

Para tanto, a BRINK'S PAY realiza o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.

São aplicados testes de continuidade de serviços de pagamento e realização de testes periódicos para garantir a eficácia e segurança dos processos. Os testes são conduzidos em um ambiente controlado permitindo a BRINK'S PAY certificar a conformidade dos planos desenvolvidos com os objetivos da BRINK'S PAY e requisitos legais.

15. Incidentes de segurança

a. Classificação de relevância dos incidentes

A BRINK'S PAY classifica os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro são imediatamente comunicados à área responsável. A comunicação é feita por meio dos canais indicados pela BRINK'S PAY através do e-mail segurancadainformacao@brinkspay.com.br.

Os incidentes reportados são classificados segundo o risco que representam para a BRINK'S PAY e o impacto na continuidade dos negócios. Além disso, são devidamente registrados, tratados e comunicados.

A BRINK'S PAY adota 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.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a BRINK'S PAY deve comunicar o Bacen e adotar medidas necessárias para que as suas atividades sejam reiniciadas.

c. Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a BRINK'S PAY adota 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.

d. Plano de ação e resposta a incidentes

A BRINK'S PAY estabelece 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.

e. Relatório anual de incidentes

A BRINK'S PAY elabora relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório aborda:

- 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 utilizadas 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 é apresentado ao Conselho de Administração ou, na sua inexistência, à Diretoria da BRINK'S PAY até 31 de março do ano seguinte ao da data-base.

16. Mecanismos de rastreabilidade

A BRINK'S PAY adota 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 BRINK'S PAY, o controle e a gestão das informações sensíveis terão tratamento específico para assegurar a segurança e integridade das informações de identidade do dispositivo. Caso um dispositivo diferente daquele autorizado a realizar transações na plataforma vier a tentar acessar os sistemas da BRINK'S PAY, será enviado por e-mail ou outro meio, um token para verificação de segurança, validando que as informações sensíveis estão sendo preservadas e protegidas.

17. Registro de impacto

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

18. Treinamentos e conscientização

A BRINK'S PAY preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, são adotadas políticas e procedimentos para difusão dos princípios e diretrizes integrantes desta Política, além dos treinamentos sobre Segurança da Informação disponibilizados na plataforma de *e-learning* (educação a distância) da Companhia, garantindo assim a capacitação e conscientização para toda Alta Administração e seus Colaboradores.

A BRINK'S PAY promove a ampla divulgação desta Política em seu portal ou através de boletins internos a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, 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. Também divulgamos um resumo contendo as linhas gerais da política de Segurança cibernética.

Além disto, a Alta Administração da BRINK'S PAY difunde 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.

19. 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 é realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros é 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 BRINK'S PAY adota 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 BRINK'S PAY 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 BRINK'S PAY para a prestação do serviço a ser contratado;
- O acesso da BRINK'S PAY 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 BRINK'S PAY 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 BRINK'S PAY.

Na avaliação da relevância do serviço a ser contratado, a BRINK'S PAY também considera a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos são documentados.

Ademais, a BRINK'S PAY adota 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 BRINK'S PAY assegura 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 BRINK'S PAY, sob demanda e de maneira virtual, incluem um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à BRINK'S PAY implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela BRINK'S PAY ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela BRINK'S PAY, 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 BRINK'S PAY 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 BRINK'S PAY 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 BRINK'S PAY observa os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços são prestados;
- Verificação de que a prestação dos serviços não causa prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços são prestados e os dados armazenados, processados e gerenciados. Essa definição ocorre 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 são prestados, a BRINK'S PAY deve solicitar 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 BRINK'S PAY deve solicitar autorização 60 dias antes da alteração contratual.

A BRINK'S PAY assegura que a legislação e a regulamentação nos países em que os serviços são prestados não restrinjam ou impeçam o acesso da BRINK'S PAY e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deve ser documentados.

e. Contrato de prestação de serviços

A BRINK'S PAY assegura 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 são 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 BRINK'S PAY, 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 BRINK'S PAY 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 BRINK'S PAY sobre a subcontratação de serviços relevantes para a BRINK'S PAY;
- 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 BRINK'S PAY, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter a BRINK'S PAY 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 BRINK'S PAY pelo Bacen, o contrato de prestação de serviços prevê:

- A obrigação da 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 deve 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 deve ocorrer também na situação em que a interrupção for motivada por inadimplência da BRINK'S PAY.

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:

- 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

deve ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 19 “d”.

20. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a BRINK’S PAY deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- Os procedimentos 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 BRINK’S PAY;
- 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 BRINK’S PAY, bem como das providências para o reinício das suas atividades.

A BRINK’S PAY institui 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 incluem 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.

21. Arquivamento de informações

A BRINK’S PAY armazena em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- A ata de reunião do Conselho de Administração ou, na sua inexistência, da Diretoria da BRINK’S PAY;
- O documento relativo ao plano de ação e de resposta a incidentes;
- O relatório anual;
- A documentação sobre os procedimentos desta Política;
- A documentação no caso de serviços prestados no exterior;

- Os contratos de prestação de serviços;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados.

22. Auditorias

A BRINK'S PAY se reserva no direito de conduzir auditorias para validar se os seus processos, operações, atividades e procedimentos estão em conformidade com as diretrizes definidas pela Companhia. Os trabalhos de auditoria podem ocorrer através de auditorias internas, consultorias terceirizadas ou auditorias externas independentes e são realizadas no mínimo uma vez ao ano ou sempre que a Companhia julgar necessário.

E. Declaração de Responsabilidade

Os Colaboradores e prestadores de serviço da BRINK'S PAY aderem formalmente a um termo em que se comprometem a agir de acordo com esta Política. Ademais, todos os contratos da BRINK'S PAY possui cláusula que assegure a confidencialidade 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 são assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política foi aprovada e revisada pela Alta Administração e será revisada com a periodicidade mínima de um ano e poderá ser alterada a qualquer momento para contemplar quaisquer alterações regulatórias e outras obrigações legais. A Política está disponível em local acessível a todos Colaboradores.

1. Histórico de Versionamento

Autor	Motivo Principal	Data	Versão
Carlos Eduardo Jacinto da Silva	Versão inicial	13/06/2022	1.0
Helio Holsback Serejo	Versão inicial	13/06/2022	1.0
Aloysio Regis Gouveia Filho	Revisão Anual	19/04/2023	1.0
Guilherme do Carmo Jose	Revisão Anual	17/06/2024	1.0

2. Revisores

Área	Nome	Cargo
Segurança da Informação	Carlos Eduardo Jacinto da Silva	DPO - Gerente de Segurança da Informação

3. Aprovadores

Área	Nome	Cargo
Segurança da Informação	Carlos Eduardo Jacinto da Silva	DPO - Gerente de Segurança da Informação
Novos Negócios	Leandro Barreira Nascimento	Gerente Nacional Instituições Financeiras
Tecnologia da Informação	Alexandre Bertoli da Costa	Diretor de TI América Latina

ANEXO I

Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento desta Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da BRINK'S PAY.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la na Intranet da empresa.

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.

_____ /_____ /_____

Data

_____

Assinatura

ANEXO II

Termo de Adesão ás alterações da Política de Segurança da Informação e Segurança Cibernética

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento das alterações da Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da BRINK'S PAY.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la na intranet da empresa.

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.

_____ /_____ /_____

Data

_____

Assinatura

Autenticação da assinatura

ENVELOPE

0ef60d96-cb66-4677-aa84-ac6c99825f75

Enviado em 01/07/2024 13:49:21 (UTC-3)

DOCUMENTO

38f97f55-31b6-47dc-a69b-a9934dae3384

BRINKS PAY - Política de Segurança da Informação e Segurança Cibernética.pdf.pdf

unico idtech

DOCUMENTO CERTIFICADO

Fotografe o QR Code para validar a autenticidade desse documento

Remetente do documento

BRINKS Segurança e Transporte de Valores LTDA.

60.860.087/0012-51

1º ASSINANTE - Própria

Carlos Eduardo Jacinto da Silva
***.775.698-**

car********rdo@brinks.com.br

Assinado em: 01/07/2024 13:54:22 (UTC-3)
Métodos de autenticação: E-mail + CPF

2º ASSINANTE - Própria

Leandro Barreira Nascimento
***.560.035-**

lea***********nto@brinks.com.br

Assinado em: 04/07/2024 11:58:39 (UTC-3)
Métodos de autenticação: E-mail + CPF

3º ASSINANTE - Própria

Alexandre Bertoli da Costa
***.775.818-**

ale**********oli@brinks.com.br

Assinado em: 16/07/2024 17:14:58 (UTC-3)
Métodos de autenticação: E-mail + CPF