MANUAL DE PROCEDIMENTOS PARA CONTRATAÇÃO DE SERVIÇOS RELEVANTES EM NUVEM

Data: 23/09/2024 – Versão: 01

Nome do Documento:	BP-SEG-PRO-0001
Versão:	01
Fase:	Vigente
Classificação:	Interna
Área Gestora:	Tecnologia e Segurança
Responsável:	Guilherme do Carmo Jose
Revisor:	Carlos Eduardo Jacinto da Silva
Aprovador:	Fabricio Anselmo da Silva
Aprovador:	Alexandre Bertoli da Costa
Áreas abrangentes:	Brinks Pay

BRINKS PAY

Sumário

1. Objetivo

O presente manual de Procedimentos de Contratação de Serviços Relevantes em Nuvem (“Manual”) foi elaborado com o objetivo de orientar as áreas relacionadas à contratação de Serviços sobre o tema e descrever procedimentos a serem praticados assim como a atenção dedicada durante a execução das atividades da Brink’s Pay Instituição de Pagamento Ltda. (“Brink’s Pay”). Esses procedimentos são voltados essencialmente a controles internos, Governança, Segurança, Infraestrutura de Tecnologia, atendendo a requisitos regulatórios e boas práticas de mercado, em que são definidos os critérios para identificação, qualificação e classificação dos fornecedores.

O presente manual foi elaborado para cumprimento das políticas da Brink’s Pay que tem como objetivo atender as disposições previstas na Resolução n° 85, de 8 de abril de 2021, que dispõe sobre a política, os procedimentos e os controles a serem adotados visando o processo de contratação de Serviços em nuvem, relevantes à operação dos negócios da Instituição, garantindo o atendimento adequado dos requisitos regulatórios que visam proteção da informação da Instituição.

2. Abrangência e Aplicação

Os princípios de ética e os valores declarados pela direção do Grupo Brinks devem reger os relacionamentos e negócios da Brink’s Pay, assegurando a correta contratação de serviços considerados “relevantes” (serviços e sistemas que atendam a processos de alta criticidade), mitigando eventuais riscos de paralisação dos serviços.

A área de Tecnologia da Informação, Segurança da Informação, Jurídico e Gestão de contratos serão responsáveis pela atualização e aprovação deste manual diante da legislação brasileira, de normativos das autoridades regulatórias e de coleta de evidências para o devido registro e guarda para eventuais solicitações dos órgãos reguladores.

O cumprimento dos procedimentos previstos neste documento é obrigatório em todos os níveis da organização. A análise cadastral, a seleção e a contratação de um novo parceiro, fornecedor ou prestador de serviço iniciando-se pelo processo denominado de RFI – *Request for Information*, onde se deve incluir os requisitos funcionais, não funcionais, regulatórios, qualificação e classificação do parceiro, fornecedor.

Após o processo de solicitação de informação (RFI), dá se sequência ao processo de RFP – *Request for Proposal*, onde apenas os fornecedores que atenderam aos requisitos solicitados farão parte do processo.

3. Definições

RFI - Request For Information: Processo inicial de contratação, ao qual todos os requisitos de negócio (funcionais), não funcionais (técnicos/ tecnológicos) e regulatórios são definidos e o parceiro/ fornecedor respondem, determinando o grau de atendimento de cada item informado.

RFP - Requesto for Proposal: Próxima etapa do processo de Contratação onde os fornecedores que atendem minimamente os requisitos necessários, informam os valores de contratação, custos de manutenção e outros requisitos comerciais.

Cloud - Nuvem de serviços tecnológicos (SaaS, IaaS, PaaS): Serviços disponibilizados em nuvem privada, pública, com garantia de disponibilidade, performance sob demanda.

SaaS - Software as a Service: Serviços contratados na Nuvem;

PaaS - Platform as a Service: Plataforma de sistemas contratados na nuvem;

IaaS - Infrastructure as a Service: Infraestrutura tecnológica como serviço;

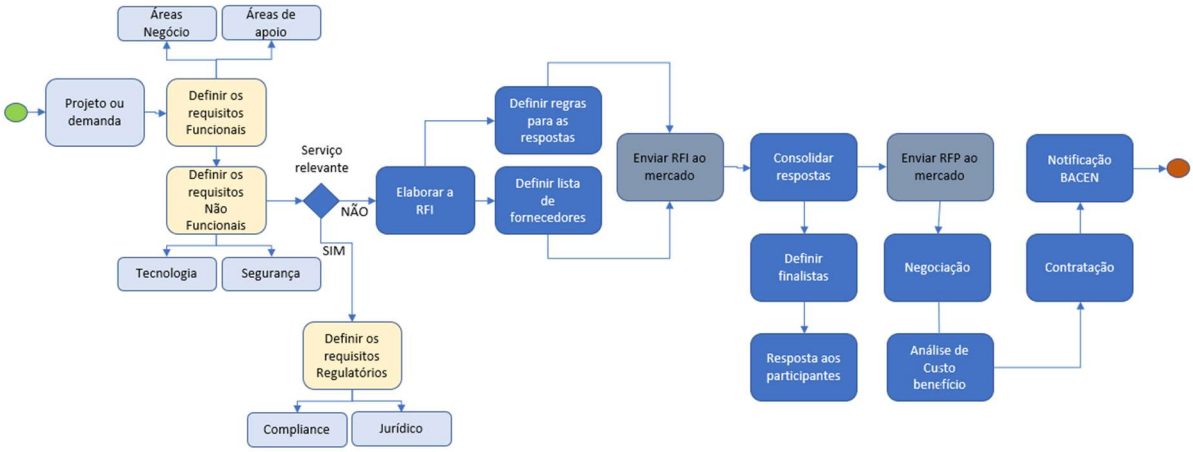
Grupo Brinks: Grupo Brinks (holding) e todas as suas Sociedades Direta e Indiretamente Controladas e Coligadas.

Serviços relevantes: Serviços que são considerados de extrema importância para o(s) processo(s) de negócio relevantes. A paralisação destes serviços causa impacto direto aos processos e consequentemente aos negócios.

Processos críticos: Processos que causam impacto relevante a Instituição em caso de paralisação. Estes processos são identificados na Análise de Impacto aos Negócios (AIN ou BIA);

AIN ou BIA: Análise de Impacto aos Negócios ou Business Impact Analysis: Avalia e identifica o grau de impacto Financeiro, Imagem, Operacional e Legal decorrente da paralisação do processo.

4. Procedimentos para Contratação



Macrofluxo de contratação

4.1. Identificação da Necessidade – Projeto ou Demanda

Considera-se que todos os projetos ou demandas causam alterações em processos e possivelmente em serviços relacionados, podendo ter a necessidade de contratação de serviços e/ou sistemas para atendimento a este projeto.

Este procedimento foi elaborado para atendimento a requisitos regulatórios específicos da resolução 85, que definem diversos pontos que devem ser observados na contratação, quando se trata de serviços relacionados a processos críticos.

4.2. Requisitos Funcionais

Para que se obtenha uma análise adequada dos fornecedores com relação a atender aos requisitos funcionais do projeto, deve se definir, baseado nos requerimentos do projeto, quais funcionalidades, funções, controles e relatórios devem ser atendidos.

Os requisitos funcionais são classificados como “obrigatórios” e “opcionais”, de acordo com as necessidades e características do projeto e são definidos e aprovados em conjunto com as áreas de Negócio e de Apoio.

Os requisitos funcionais podem variar de acordo com a especificidade do projeto.

4.3. Requisitos Não Funcionais

Os requisitos não funcionais visam atender a características técnicas (arquitetura, segurança, licenciamento) da solução a ser contratada.

Os requisitos não funcionais são classificados como “obrigatórios” e “opcionais”, de acordo com as necessidades e características do projeto e são definidos e aprovados em conjunto com as áreas de TI e Segurança da Informação.

Em todos os requisitos abaixo deve se definir as características requeridas.

Tipo de informação	Características	Observações
Arquitetura	Cloud SaaS Cloud IaaS Cloud PaaS Outros	Informar em qual provedor de CLOUD (se Cloud) Existência de redundância de Regiões (se Cloud) Existência de redundância de Zonas (se Cloud)
	Ambiente dedicado Ambiente Compartilhado	Existência de segregação física e/ou lógica
	Provisionamento de recursos computacionais	Sob demanda (automático) Manual
	Versão dos sistemas operacionais Versão de Banco de dados Uso de open source	Informar as versões de todos os sistemas operacionais, BackOffice e Open Source utilizados
Resiliência	Disaster Recovery	Existência de arquitetura de Disaster Recovery Tempo de ativação do DR (RTO); Tempo de Recovery Point Objective (RPO)
	Estrutura de alta disponibilidade	Informar RTO e RPO
Segurança	Autenticação de administradores	Controle de acessos privilegiados Uso de autenticação MFA Boas práticas de senhas Logs e trilhas de auditoria
	Gestão de acesso de usuários	Single Sign On Perfis de acesso Logs e trilhas de auditoria
	Transmissão e armazenamento de dados	Deve especificar a adoção de medidas de segurança para a transmissão e armazenamento de dados

Operação	Firewall WAF DLP HSM Cofre de senha Anti-malware	Deve se identificar quais recursos existem para proteção do ambiente aplicacional. Deve se identificar quais recursos existem para proteção do ambiente aplicacional.
	Gestão de vulnerabilidades	O fornecedor deve ter um processo de gestão de vulnerabilidades para evitar paralisações decorrentes de implementação com vulnerabilidades não identificadas; Execução de testes de vulnerabilidades para avaliar o grau de segurança da aplicação. Pentests
	Gestão de mudanças	Deve prevenir paralisações devido a implementações de novas versões Uso de boas práticas de Desenvolvimento seguro
	Monitoramento	Dados de monitoramento do ambiente deve ser disponibilizado para análise e críticas
	Manuais de operação Manual de usuário Manual do sistema	Existência de manuais
	SLA de reparo (RTO) SLA de ativação da contingência SLA de Disponibilidade (% mês e ano)	Deve informar o SLA de recuperação, ativação da contingência e o SLA de disponibilidade.
	Backup de dados Restore	Política de backup Boas práticas de backup (3-2-1) Restore preventivo

4.4. Requisitos Regulatórios

Os requisitos regulatórios se aplicam a serviços relevantes contratados na modalidade de nuvem (CLOUD).

Os requisitos a seguir devem ser considerados na avaliação do fornecedor para garantir a devida proteção da informação que podem estar armazenados em um ambiente externo e a Instituição deve garantir a Privacidade, Disponibilidade, Integridade e confidencialidade da informação sob seu domínio.

Existe a possiblidade de se exigir do fornecedor de serviços em CLOUD" não relevantes", os mesmos requisitos regulatórios, porém que podem encarecer o processo de contratação por exigir requisitos que fortalecem a proteção da informação e da disponibilidade dos serviços.

Estes requisitos devem fazer parte do processo de avaliação dos fornecedores e garantir que atendam adequadamente antes da efetiva contratação.

Tipo de informação	Características	Observações
Análise crítica do fornecedor	Solidez perante o mercado	Avaliar a capacidade do fornecedor de prover o serviço no mercado de produtos ou serviços semelhantes ao objeto; Analisar as certificações que o prestador possui para o provimento do serviço (TIER, ISO, etc)
Acesso às informações	Fornecedor deve garantir a confidencialidade integridade e disponibilidade das informações processadas e/ou armazenadas	Deve responder na RFI e constar no contrato de prestação de serviços
	acesso da instituição aos relatórios elaborado por empresa de auditoria especializada em relação aos procedimentos e aos controles utilizados para a prestação do serviço	Deve responder na RFI e constar no contrato de prestação de serviços
	Prestador deve levar em consideração a classificação quanto a sensibilidade dos dados dos clientes definidos pela instituição	Deve responder na RFI e constar no contrato de prestação de serviços
Comunicação Banco Central	Convenio para troca de informações entre o Banco Central do Brasil a as autoridades supervisoras dos países onde os serviços poderão ser prestados, caso contrário solicitar autorização do Banco Central	Garantir que as zonas disponibilizadas pelo provedor tenham convenio para troca de informações com o banco Central
	Assegurar que a legislação nos países e nas regiões onde o serviço poderá ser prestado, não restringem nem impedem o acesso da instituição contratante ou do Banco Central às informações.	Garantir que as zonas disponibilizadas pelo provedor tenham convenio para troca de informações com o banco Central
Acesso aos dados	Dados processados a armazenados	Garantia de acesso aos dados processados ou armazenados
	Transferência de dados	Garantia de transferência dos dados ao novo prestador em caso de extinção do contrato
	Exclusão de dados	Garantia de exclusão dos dados após a transferência em caso de extinção do contrato
Subcontratação	Serviços terceirizados ou quarteirizados	Cláusula que obriga a prestadora a informar se algum dos serviços relevantes prestados é subcontratada
Permissão de acesso ao BACEN	Contratos Serviços Dados Copias de segurança Códigos de acesso aos dados	Permissão de acesso do Banco Central aos contratos e acordos firmados para a prestação de serviços, aos dados, as copias de segurança bem como aos códigos de acesso aos dados e informações.
	Determinação do BACEN	Prever a adoção de medidas pela instituição contratante em decorrência de determinação do Banco Central
Sanções	Limitações de serviços	Prever a obrigação da empresa contratada de manter a instituição contratante sempre informada de limitações que possam afetar a prestação de serviços ou o cumprimento da legislação.

Comunicação e notificação	Rescisão	Prever a notificação prévia sobre a intenção de a empresa contratada interromper a prestação dos serviços com pelo menos 30 dias de antecedência, com possibilidade de prorrogação de mais 30 dias, também em casos de inadimplência da instituição contratante;

4.5. RFI - Request for Information

A RFI é considerada como a etapa preliminar do processo de contratação, onde os fornecedores respondem de que forma atendem os requerimentos funcionais, não funcionais e regulatórios (quando se tratar de serviços relevantes).

O fornecedor pode atender:

- Totalmente – Quando atende a todos os detalhes dos requisitos
- Parcialmente – Quando o fornecedor atende parte dos requisitos requeridos. Neste caso deve detalhar qual requisito existe restrição e os motivos.
- Não atende – Quando o fornecedor não atende a nenhum dos requisitos.

Uma carta deve ser encaminhada aos participantes do processo, em que basicamente deve se informar:

- Os dados da empresa
- O cronograma contendo:
    - A data de envio
    - O prazo para sanar dúvidas técnicas ou de negócio;
    - O prazo para retorno das respostas;
    - O endereço ao qual deve ser encaminhada a resposta (e-mail, físico, etc)
    - As limitações e sanções para o prorrogamento dos prazos;
    - As limitações para contato direto com áreas que não fazem parte do processo.
    - As datas para resposta aos fornecedores
        - Finalistas
        - Não finalistas

4.6. RFP – Request for Proposal

Aos fornecedores finalistas (que atenderam a maior parte dos requisitos funcionais, não funcionais e regulatórios, deve se encaminhar uma solicitação de Proposta técnico Comercial afim de identificar preliminarmente os valores e condições para operacionalização do serviço na Instituição:

Basicamente deve se observar:

- Custo de setup
- Custo de licenciamento ou serviço (mensal)
- Custo anual (se aplicável)
- Custo de manutenção e customização;
- Custo de horas adicionais para suporte
- Outros custos imediatos e a longo prazo.
- Garantia de atualização de versão

4.7. Negociação

Todas as propostas recebidas devem ser negociadas para se obter a melhor condição técnico comercial.

4.8. Análise de custo X Benefício

As áreas afins devem analisar e debater qual dos fornecedores ofertam a melhor relação custo-benefício e definir pelo melhor fornecedor.

4.9. Contratação

Solicitação das minutas contratuais para análise e ajustes.

Devem garantir que todas as cláusulas garantam o atendimento a todos os requerimentos funcionais, não funcionais e regulatórios descritos na RFI.

4.10. Notificação Banco Central

Em caso de contratação/ alteração contratual, informar até 10 dias após a contratação ao Banco Central:

- a denominação da empresa;
- os serviços relevantes contratados;
- a indicação de países e das regiões onde os serviços poderão ser prestados;
- os dados armazenados, processados e gerenciados, até 10 dias após a contratação

5. Histórico de Versionamento

Este Manual deve ser revisado anualmente quando uma adequação dos procedimentos for necessária decorrente de mudança nos normativos ou melhoria no processo de gerenciamento de riscos e de controles internos. Este manual deve ser submetido à Diretoria da Instituição e aprovado sob assinatura digital para divulgação interna.

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	20/04/2023	1.0
Guilherme do Carmo Jose	Revisão Anual	23/09/2024	1.0

6. Revisor

Área	Nome	Cargo
Segurança da Informação	Guilherme do Carmo Jose	Especialista de Segurança da Informação

7. Aprovadores

Área	Nome	Cargo
Segurança da Informação	Carlos Eduardo Jacinto da Silva	Gerente de Segurança da Informação
Tecnologia da Informação	Fabricio Anselmo da Silva	Gerente de Sistemas e Projetos
Novos Negócios	Ádrili Sato	Diretora de Desenvolvimento de Negócios
Tecnologia da Informação	Alexandre Bertoli da Costa	Diretor de TI América Latina

Autenticação da assinatura

ENVELOPE

286a0324-be8b-4b7d-8d4a-16421c25d667

Enviado em 04/10/2024 14:14:47 (UTC-3)

DOCUMENTO

401c9814-0ac0-4688-b61f-2cad7349eb3c

BrinksPay - Manual de Procedimentos Contratacao Serviços Nuvem.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: 07/10/2024 09:43:20 (UTC-3)
Métodos de autenticação: E-mail + CPF

2º ASSINANTE - Própria

Fabricio Anselmo da Silva
***.337.558-**

fab**********lmo@brinks.com.br

Assinado em: 08/10/2024 17:30:05 (UTC-3)
Métodos de autenticação: E-mail + CPF

3º ASSINANTE - Própria

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

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

Assinado em: 25/10/2024 10:03:18 (UTC-3)
Métodos de autenticação: E-mail + CPF

4º ASSINANTE - Própria

ADRILI MARIA SATO
***.473.688-**

adr*****ato@brinks.com.br

Assinado em: 29/10/2024 17:03:45 (UTC-3)
Métodos de autenticação: E-mail + CPF