Obrigações de controlo de fornecedores externos

Risco tecnológico – Controlos técnicos

Versão 12.0 Datada de outubro de 2022

Área de controlo	Designação do controlo	Descrição do controlo	Por que é importante
1. Gestão de problemas	Identificação e registo do problema	O fornecedor tem de garantir que é realizada uma investigação atempada da causa originária para todos os incidentes principais pontuais e de incidentes recorrentes em que o impacto combinado seja suficiente para causar um impacto operacional significativo.	Quando a causa principal de incidentes significativos não é identificada e resolvida atempadamente, o serviço permanece em risco de falhas repetidas e evitáveis, levando a uma interrupção dos sistemas/serviços, danos na reputação e/ou corrupção/perda de dados
	Gestão e resolução de problemas	O fornecedor deve garantir que a causa originária de incidentes significativos é resolvida atempadamente ou, quando tal não for possível, a aceitação do risco é fornecida pela Barclays e são aplicados controlos atenuantes adequados para limitar a probabilidade de recorrência.	

Área de controlo	Designação do controlo	Descrição do controlo	Por que é importante
2. Gestão da mudança	Aplicar um controlo da mudança rigoroso	O fornecedor tem de garantir que todos os componentes de TI que são utilizados na prestação de serviços ao Barclays são geridos ao abrigo de um rigoroso regime de controlo da mudança, incluindo os seguintes requisitos: 1. Não podem ser efetuadas alterações sem autorização adequada do Barclays antes da implementação. 2. Deve existir separação de funções entre o iniciador, o responsável, o aprovador e o implementador da mudança. 3. As alterações devem ser planeadas e geridas de acordo com o nível de risco associado à manutenção do nível mínimo exigido de serviço ao Barclays. 4. As mudanças devem prever adequadamente o potencial impacto no desempenho e/ou na capacidade dos componentes tecnológicos afetados. 5. As mudanças devem ser sujeitas a testes técnicos e comerciais relevantes para a mudança antes da implementação, havendo lugar à retenção de elementos de prova quando necessário. 6. As mudanças têm de ser testadas após a implementação para garantir que foram bem-sucedidas e não tiveram repercussões imprevistas.	Processos de mudança inadequados para impedir mudanças não autorizadas, mal geridas ou inadequadas podem conduzir a perturbação do serviço, corrupção de dados, perda de dados, erros de processamento ou fraude.

3. Gestão do desempenho e da capacidade	Permanecer em conformidade com as necessidades tecnológicas do Barclays	O fornecedor tem de definir, manter e documentar níveis de desempenho e capacidade adequados para todos os componentes de TI principais utilizados na prestação de serviços ao Barclays, em conformidade com todos os requisitos contratuais. Tem igualmente de garantir que estão instalados nos principais componentes alertas e limites máximos, que avisem sobre o potencial incumprimento dos limites, e que são revistos periodicamente para assegurar que a prestação do serviço está alinhada para cumprir todos os requisitos contratuais e satisfazer as necessidades do Barclays.	Medidas inadequadas para definição, documentação e monitorização do desempenho e/ou níveis de capacidade dos recursos de TI e a não manutenção das mesmas em conformidade com os requisitos atuais e futuros podem conduzir a uma redução inaceitável e/ou interrupção dos serviços tecnológicos e a uma perda de negócios.
Área de controlo	**Designação do controlo**	**Descrição do controlo**	**Por que é importante**
4. Desenvolvimento de aplicações tecnológicas	Estratégia de teste e conclusão antes do arranque técnico e/ou empresarial	O fornecedor deve compreender a qualidade de todo o software antes de vender ou fornecer esse software ao Barclays. Todos os códigos de software devem estar no(s) sistema(s) de controlo de versões e ser aprovados pelo prestador de serviços do fornecedor antes de serem fornecidos ao Barclays. As alterações à aplicação devem ser submetidas a testes de software pelo fornecedor para garantir que o software cumpre os requisitos captados. As provas de testes têm de ser guardadas.	Sistemas e serviços testados e cuja qualidade tenha sido garantida de forma inadequada podem resultar numa perda de funcionalidade crítica e imprevisível a nível dos serviços de tecnologia e processos empresariais.
	Confirmar os requisitos do sistema	Ao fornecer software de acordo com as especificações do Barclays, o fornecedor deve garantir que os requisitos empresariais são claramente definidos e acordados com o Barclays.	Requisitos empresariais inadequadamente definidos podem levar a um comportamento incorreto do sistema, resultando em riscos para os processos empresariais e operacionais.
	Aceitação empresarial antes da implementação	Ao entregar software de acordo com as especificações do Barclays, o fornecedor deve determinar e seguir um processo de qualidade/aceitação que tenha sido acordado com o Barclays.	A aceitação empresarial inadequada antes da implementação pode resultar num comportamento incorreto do sistema, bem como em riscos para os processos empresariais e operacionais.
5. Disposições de cópia de segurança para sistemas e dados	Aplicar processos de restauro e de cópia de segurança apropriados e eficazes	O fornecedor tem de garantir que todos os sistemas e serviços de TI utilizados na prestação de serviços ao Barclays dispõem de processos de restauro e de cópia de segurança adequados que funcionem de acordo com as necessidades do Barclays e cuja eficácia seja comprovada periodicamente.	A inexistência de controlo ou um fraco controlo das cópias de segurança dos dados empresariais pode resultar na perturbação dos sistemas/serviço, perda de dados ou divulgação de dados inadequada.

	Garantir suportes de cópia de segurança de dados seguros, protegidos e fiáveis	O fornecedor tem de garantir que todos os suportes de cópia de segurança associados à prestação de serviços ao Barclays, juntamente com as condições de tratamento e armazenamento desses suportes, permanecem seguros e fiáveis em todas as circunstâncias.	São necessários suportes de cópia de segurança seguros e fiáveis para evitar interrupções nos sistemas/serviços, perda de dados ou divulgação inadequada de dados.
Área de controlo	**Designação do controlo**	**Descrição do controlo**	**Por que é importante**
6. Gestão da configuração	Isolamento do ambiente de produção	O fornecedor tem de garantir que os serviços de produção disponibilizados ao Barclays não dependem de componentes não envolvidos na produção, de modo a evitar uma prestação de serviços insegura ou não fiável.	A utilização de componentes não envolvidos na produção na prestação de serviços de produção comporta riscos, na medida em que estes podem não ser construídos ou geridos de acordo com normas de produção.
	Registo e manutenção de itens de configuração	O fornecedor tem de manter registos individuais completos e rigorosos para todos os itens de configuração abrangidos e utilizados na prestação de serviços ao Barclays (incluindo a responsabilidade e as dependências/mapeamentos a montante/jusante). O fornecedor tem de dispor de controlos para garantir a manutenção contínua da precisão e integralidade dos dados.	Registos individuais inadequados ou incompletos (juntamente com dependências/mapeamentos em relação a outros itens de configuração) podem resultar em serviços e dados inseguros ou instáveis, em consequência de uma avaliação ineficaz dos incidentes e do impacto da mudança.
7. Gestão do nível de serviço	Definir e monitorizar o desempenho do serviço	O fornecedor deve garantir que o serviço está em conformidade com os níveis de serviço acordados, incluindo a monitorização e comunicação do nível de serviço.	Os níveis de serviço garantem que os serviços de TI são prestados de acordo com os compromissos de serviço de TI acordados

Definições de tecnologia:

Item de configuração	Qualquer componente que precise ser gerido para fornecer um serviço de TI. Os itens de configuração podem ser físicos (por exemplo, um computador ou router), virtuais (por exemplo, um servidor virtual) ou lógicos (por exemplo, um serviço). As alterações (adições, modificações ou cessações) devem ser realizadas sob o controlo da gestão de alterações.
Incidente	Uma interrupção não programada de um serviço de TI ou uma redução na qualidade de um serviço de TI, incluindo, sem limitação, a falha de um item de configuração que ainda não tenha afetado um serviço.
Serviço de TI	Um serviço fornecido a um ou mais clientes por um fornecedor de serviços de TI. Um serviço de TI é constituído por uma combinação de pessoas, processos e TI e é fornecido a clientes para apoiar os seus processos empresariais.

Incidente grave	Um incidente que representa um risco/impacto significativo para o Barclays e pode resultar em consequências graves, incluindo perda grave de produtividade, danos na reputação/regulamentares e impacto nos principais processos empresariais, controlos ou sistemas.
Problema	A causa desconhecida de um ou mais incidentes.