Obrigações de controlo de fornecedores externos

Risco de tecnologia

Versão 11.0 Datada de outubro de 2021

Área de controlo	Designação do controlo	Descrição do controlo	Por que é importante
1. Gerir a obsolescência	Garantir disposições de suporte contínuo	O fornecedor tem de informar imediatamente o Barclays sobre modificações conhecidas na sua capacidade para disponibilizar suporte, direta ou indiretamente, a ativos de TI utilizados na prestação de serviços ao Barclays, incluindo sempre que os produtos tenham vulnerabilidades de segurança, devendo também garantir uma atualização atempada ou a retirada de operação desses ativos de TI.	Registos e/ou procedimentos inadequados para ativos de hardware e software que deixem de receber suporte ou serviços de tecnologia que se baseiem em hardware ou software obsoleto podem resultar num desempenho inaceitável, instabilidade, vulnerabilidades de segurança, perda de negócios e custos de migração excessivos.
2. Tratamento de incidentes	Registo, classificação e resolução de incidentes	O fornecedor tem de aplicar um regime de tratamento de incidentes relativamente à operação dos sistemas e serviços de TI, regime esse que garanta que esses incidentes operacionais são adequadamente identificados, registados, priorizados, classificados e imediatamente resolvidos, seja pelo primeiro contacto, seja através de um encaminhamento oportuno e adequado. Tal deve incluir um processo sólido para tratamento imediato e efetivo de incidentes graves.	Os incidentes de tecnologia que não forem comunicados atempadamente ou com detalhe suficiente, ou quando não se adotarem as ações corretivas necessárias, podem resultar na perturbação evitável de sistemas/serviço, ou em danos ou perda de dados. Os incidentes graves implicam uma resposta reforçada e urgente, na medida em que são incidentes que constituem um risco significativo para a empresa e podem ter sérias consequências, incluindo interrupções graves, perda de reputação, impactos financeiros e impactos nos principais processos empresariais.
3. Gestão de problemas	Identificação, avaliação/análise e resolução de problemas de tecnologia	O fornecedor tem de aplicar um regime de investigação atempada dos problemas subjacentes a incidentes de tecnologia significativos, que garanta a identificação e o registo desses problemas através da análise da causa originária e a sua eficaz resolução no sentido de minimizar a probabilidade e o impacto da recorrência de incidentes. O fornecedor deve também garantir que é efetuada uma análise proativa dos incidentes recorrentes, a fim de identificar e resolver a	Quando problemas subjacentes que dão origem a incidentes com impacto na prestação de serviços de tecnologia não são identificados e resolvidos atempadamente, pode ocorrer perturbação evitável de sistemas/serviço, ou danos ou perda de dados.

		causa de incidentes comuns, com elevado número de repetições.	
4. 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, que preveja integralmente os seguintes objetivos: 1. Impossibilidade de mudança sem a devida autorização – a aprovação tem de ocorrer antes da implementação 2. Separação de funções entre o iniciador, o responsável, o aprovador e o implementador da mudança 3. Mudanças planeadas e geridas de acordo com o nível de risco associado 4. As mudanças preveem adequadamente o potencial impacto no desempenho e/ou na capacidade dos componentes tecnológicos afetados 5. As mudanças são 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 sistema, danos em dados, perda de dados, erros de processamento ou fraude.
5a. Resiliência tecnológica	Plano de recuperação do sistema (SRP)	O fornecedor tem de dispor de um ou mais Planos de recuperação do sistema (SRP) para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços Barclays com uma Categoria de resiliência 0-3, bem como os respetivos Objetivos de tempo de recuperação (RTO) e Objetivo do ponto de recuperação (RPO). A exatidão do(s) plano(s) deve ser analisada pelo menos a cada 12 meses.	A inexistência ou inadequação dos Planos de recuperação do sistema pode conduzir à perda inaceitável de serviço de tecnologia para a unidade de negócios ou para os clientes após um incidente. Manter a documentação relativa à resiliência atualizada e em prática garante que os planos de recuperação permanecem alinhados com as necessidades empresariais.

		Nota: relativamente aos sistemas/serviços tecnológicos com uma Categoria de resiliência 0-1, concebidos numa configuração ativa/passiva para as medidas de resiliência, a validação do SRP requer que o sistema permaneça no ambiente recuperado durante um período de tempo prolongado e operar como BAU a fim de confirmar que todos os elementos funcionam de forma eficiente. Na verdade, trata-se de um evento de Convergência de produção ("Production Crossover", PCO).	
5b. Resiliência tecnológica	Plano de recuperação da integridade dos dados (DIRP)	O fornecedor tem de dispor de um ou mais Planos de recuperação da integridade dos dados (DIRP) para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços Barclays com uma Categoria de resiliência 0-1. A exatidão do(s) plano(s) deve ser analisada pelo menos a cada 12 meses.	A perda de dados é uma das maiores ameaças com que nos deparamos, já que podem assumir a forma de atos dolosos ou falhas do sistema. Dispor de um plano para este cenário é crucial, pois ajuda a identificar e a compreender as fontes de dados e dependências.
5c. Resiliência tecnológica	Diversidade dos centros de dados	O fornecedor tem de garantir que cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços Barclays com uma Categoria de resiliência 0-3 é resiliente ao longo dos centros de dados e com uma distância suficiente para reduzir o risco de os centros de dados serem afetados simultaneamente pelo mesmo evento.	Os centros de dados devem dispor de fontes de alimentação, ligações de rede, etc. alternativas e estar situados a uma distância suficiente para reduzir o risco de os centros de dados serem afetados simultaneamente pelo mesmo evento.
5d. Resiliência tecnológica	Validação do SRP	O fornecedor tem de testar e validar o(s) Plano(s) de recuperação do sistema (SRP) a fim de demonstrar que os sistemas/serviços tecnológicos podem ser recuperados a fim de	Os sistemas tecnológicos providenciados pelo fornecedor podem afetar as jornadas dos clientes do Barclays. É crucial garantir que os fornecedores que apoiam as operações comerciais do Barclays dispõem de planos de resiliência adequados que são devidamente testados e que

		preencherem os requisitos de categoria de resiliência 0-3 estipulados pelo Barclays. Para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços com uma Categoria de resiliência 0-1 concebidos numa configuração ativa/passiva para as medidas de resiliência, o ambiente passivo tem de ser ativado no seguimento do SRP documentado e usado como ambiente de produção de BAU durante um período suficientemente longo para provar a capacidade e a funcionalidade de integração total (Convergência de produção ["Production Crossover", PCO]). Os requisitos respeitantes à frequência da validação têm de ser suportados pela Categoria de resiliência associada, ou seja: - Categoria de resiliência 0: a validação do SRP tem de ser realizada a cada 12 meses e a cada 3 meses para a PCO - Categoria de resiliência 1: a validação do SRP e PCO têm de ser realizadas a cada 12 meses - Categoria de resiliência 2-3: a validação do SRP tem de ser realizada a cada 24 meses Se algum teste não atingir os requisitos de recuperação mínimos para a Categoria de resiliência aplicável, o fornecedor tem de notificar imediatamente o Barclays e de fornecer planos de correção detalhados (que incluam as ações a realizar e respetivas datas de finalização). O fornecedor terá de notificar o Barclays antes de executar a PCO.	existe um mandato regulamentar para o Barclays exercer uma gestão adequada dos seus fornecedores. A Convergência de produção ("Production Crossover", PCO) consiste num método para validar se a instância passiva de um sistema configurado de forma ativa-passiva funciona conforme expectável e com a capacidade necessária para uma operação de BAU. Além disso, uma PCO também valida se qualquer dependência nos sistemas a montante e a jusante continua a funcionar conforme expectável.
5e. Resiliência tecnológica	Validação do DIRP	O fornecedor tem de testar e validar o(s) Plano(s) de recuperação da integridade dos dados (DIRP) para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços Barclays com uma	Os dados são um elemento crítico que pode ser adversamente afetado de diversas formas. O plano documentado para restituir, recuperar ou recriar dados tem de ser executado para confirmar a sua precisão e viabilidade.

		Categoria de resiliência 0-1, a fim de comprovar a integridade dos dados durante a recuperação. A validação deve ser realizada a cada 12 meses. Se algum plano não atingir os requisitos de recuperação mínimos para a Categoria de resiliência aplicável, o fornecedor tem de notificar imediatamente o Barclays e de fornecer planos de correção detalhados (que incluam as ações a realizar e respetivas datas de finalização).	
6. Gestão do desempenho e da capacidade	Permanecer em conformidade com as necessidades de tecnologia do Barclays	O fornecedor tem de definir níveis de desempenho e capacidade adequados para todos os componentes de TI principais utilizados na prestação de serviços ao Barclays, em conformidade com as necessidades empresariais definidas. 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 com as necessidades do Barclays.	Medidas inadequadas para 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 de tecnologia e a uma perda de negócios. Uma definição e/ou documentação inadequadas das necessidades da unidade de negócios/clientes podem resultar num desempenho inaceitável em termos de serviços de tecnologia e na perda de negócios.
Área de controlo	**Designação do controlo**	**Descrição do controlo**	**Por que é importante**
7. Desenvolvimento de aplicações tecnológicas	Aplicar uma garantia da qualidade consistente	O fornecedor tem de garantir que é possível demonstrar que todos os sistemas e serviços de TI utilizados na prestação de serviços ao Barclays foram sujeitos a processos de garantia de qualidade rigorosos, exaustivos e consistentes, incluindo, entre outros, testes funcionais e não funcionais, ensaios estáticos de segurança de aplicações e garantia de qualidade do código, seja através de avaliação entre pares ou de ferramentas automáticas.	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.

	Aceitação dos resultados comerciais	O fornecedor tem de concordar, numa base pontual ou contínua, com definições de resultados empresariais mutuamente aceitáveis, segundo as quais são fornecidas ao Barclays e por ele aceites versões novas ou atualizadas de sistemas e serviços de TI. O documento em que figuram estas definições tem de incluir suficientes aspetos funcionais e não funcionais dos sistemas e serviços e pode assumir qualquer formato adequado mutuamente acordado, como manuais de sistemas existentes, requisitos documentais pormenorizados mutuamente acordados, histórias de utilizadores, casos de utilização ou outro formato adequado. O fornecedor tem de colaborar com o Barclays para garantir que os resultados empresariais no seu conjunto ou uma parte mutuamente acordada dos mesmos são aceites, de modo pontual ou contínuo, com base na aprovação empresarial pelo Barclays das definições previamente acordadas.	A aprovação inadequada do comportamento funcional ou não funcional do sistema pode conduzir a um desvio face ao comportamento esperado do sistema do Barclays, colocando em risco os processos empresariais e operacionais.
8. 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.	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.

9. 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.	Registos individuais impróprios relativamente a componentes de tecnologia (hardware e software) incluindo responsabilidade definida e dependências de terceiros podem implicar serviços e dados inseguros ou não fiáveis. 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.
	Especificações de registo e manutenção da 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.
10. Gestão de ativos de hardware	Especificações de registo e manutenção de ativos de hardware	O fornecedor tem de dispor de controlos que garantam o registo e a manutenção contínuos dos dados nos ativos de hardware ao longo do ciclo de vida dos ativos. O fornecedor tem de manter registos completos e rigorosos para todos os ativos de hardware de TI utilizados na prestação de serviços ao Barclays.	Registos individuais impróprios sobre ativos de hardware tecnológicos, incluindo responsabilidade definida e dependências de terceiros, podem implicar serviços e dados inseguros ou não fiáveis. O não apagamento e a não eliminação seguros de ativos de hardware podem resultar em prejuízos financeiros, regulamentares e para a reputação.
	Eliminação de ativos	Todos os dados do Barclays constantes de ativos eliminados têm de ser totalmente apagados, devendo estes ativos ser eliminados de acordo com um processo de eliminação oficial consentâneo com os requisitos de todas as normas de segurança pertinentes do Barclays.	É essencial o fornecedor obter e registar uma confirmação formal de que os ativos foram corretamente eliminados (incluindo a destruição, em segurança, dos dados bancários). O não apagamento e a não eliminação seguros de ativos de hardware podem resultar em prejuízos financeiros, regulamentares e para a reputação.

	Ativos em falta	Todas as situações que envolvam ativos "perdidos ou furtados" têm de ser devidamente investigadas e reportadas ao Barclays para aprovação do risco caso não sejam encontrados.	É essencial que o fornecedor disponha de controlos que garantam que os ativos perdidos são devidamente investigados e - caso não sejam encontrados - são reportados ao Barclays para posterior aprovação do risco. A perda e consequente não apagamento e não eliminação seguros de ativos de hardware podem resultar em prejuízos financeiros, regulamentares e para a reputação.
Área de controlo	**Designação do controlo**	**Descrição do controlo**	**Por que é importante**
11. Gestão de ativos de software	Especificações de registo e manutenção de ativos de software/instalações. Licenciamento de ativos de software	O fornecedor tem de manter registos individuais completos e rigorosos para todos os ativos de software e instalações dos mesmos abrangidos e utilizados na prestação de serviços ao Barclays (incluindo a responsabilidade). O fornecedor tem de manter o rigor e a integralidade dos dados desde a sua recolha à eliminação (e instalação e desinstalação). O fornecedor tem igualmente de garantir que a utilização de software permanece consentânea com os termos da licença específica.	Registos individuais impróprios relativamente a ativos de software tecnológico, incluindo à responsabilidade definida, podem implicar serviços e dados inseguros ou não fiáveis. A gestão de software não autorizada pode resultar em prejuízos financeiros, regulamentares e para a reputação.

Resiliência tecnológica - Definições:

"Recovery Time Objective" (RTO - objetivo de tempo de recuperação)	"RTO" é o período entre uma falha ou interrupção inesperada dos serviços e o restabelecimento das operações.
"Recovery Point Objective" (RPO - objetivo de ponto de recuperação)	"RPO" é a situação almejada em termos de disponibilidade de dados no início do processo de recuperação. Trata-se da medida da perda de dados máxima que é tolerável numa situação de recuperação.
"Production Crossover" (PCO - Convergência de produção)	"PCO" é o ato de ativar a instância alternativa (DR) para os sistemas concebidos numa configuração ativa/passiva e utilizar a mesma como instância de produção durante um período de tempo prolongado a fim de validar a sua total funcionalidade e capacidade.
Plano de recuperação do sistema (SRP)	É um documento que define os elementos técnicos e detalhes sobre como recuperar um sistema ou qualquer componente em situação de falha, repondo o seu estado operacional.
Plano de recuperação da integridade dos dados (DIRP)	É um documento que define as medidas a tomar para recuperar os dados perdidos devido a uma falha do sistema ou intenção malévola. O plano deve abordar cenários com opções relevantes (por ex., reprodução de dados a partir de outros sistemas, restauro de dados a partir de arquivos ou recriação de dados).

Requisitos do Barclays em matéria de resiliência por matriz de categoria de resiliência

Categoria de resiliência	0	1	2	3
"Recovery Time Objective" (RTO - objetivo de tempo de recuperação)	Até 5 minutos	Até 4 horas	Até 12 horas	Até 24 horas
"Recovery Point Objective" (RPO - objetivo de ponto de recuperação)	Até 5 minutos	Até 15 min	Até 30 min	Até 24 horas