External Supplier Control Obligations

Planeamento de recuperação

Versão 11.0 datada de outubro de 2021

1. Definições:

"Crise"	Significa um evento perturbador ou com impacto na reputação que exige uma resposta que ultrapassa a estrutura e/ou os recursos rotineiros (BAU) normais, bem como uma intervenção executiva, para efeitos de tomada de decisão e de coordenação.
"Incidente"	Significa um evento perturbador que pode ser gerido no âmbito das operações quotidianas mediante a invocação de planos de recuperação.
"Planeamento de recuperação"	O processo ou planeamento para a recuperação de serviços de negócios, processo de negócios e dependências subjacentes
"Evento de perturbação"	Um registro dos impactos do incidente, agnóstico em relação à causa, que os fornecedores escolheram mitigar através da implementação do planeamento e capacidades de recuperação e resiliência
"Objetivo de tempo de recuperação"	Significa o período entre uma falha ou interrupção inesperada dos serviços e o restabelecimento das operações.

2. Controlos:

Designação do controlo	Descrição do controlo	Por que é importante
1. Eventos de perturbação para requisitos de Planeamento de recuperação	O Barclays estipulará a Categoria de resiliência para os serviços contratados. O fornecedor tem de definir os eventos de perturbação no âmbito do planeamento e o nível de planeamento necessário para garantir que os serviços podem ser prestados dentro dos níveis de serviço acordados e dos respetivos Objetivos de tempo de recuperação. As categorias de Evento de perturbação devem considerar como um mínimo: ▪ Perda de edifício(s) em vários locais que não suportam operações de negócio; ▪ Cenário de perda de dados, incluindo eventos cibernéticos e o potencial impacto na prestação de serviços ao Barclays. Perda de recursos de colegas que possam afetar a prestação de níveis de serviço acordados; ▪ Indisponibilidade de serviços para ao Barclays devido a potenciais eventos cibernéticos/não cibernéticos e potencial impacto na prestação de serviços ao Barclays; ▪ Recuperação única e simultânea de serviços de tecnologia (ou seja, perda de centro de dados)	O Barclays tem um requisito comercial (e orientado para o risco) para evitar e/ou conseguir recuperar atempadamente de Eventos de perturbação significativos, ou seja, ser adequadamente resiliente. O Barclays tem de receber garantias e de poder garantir às partes interessadas que o serviço está concebido de forma a minimizar o impacto (no cliente, financeiro e/ou na reputação) de eventuais perturbações.

Designação do controlo	Descrição do controlo	Por que é importante
	Os eventos de perturbação devem ser revistos anualmente e de forma contínua, para informar o planeamento e testar e demonstrar como esta evolução ocorre ao longo do tempo. O fornecedor deve ser capaz de demonstrar que vários fatores de gravidade foram considerados, testados e validados.	
2. Requisitos de Mapeamento de dependências para inclusão no Planeamento de recuperação	O fornecedor tem de definir e documentar as dependências que são críticas para a prestação do serviço ao Barclays, de forma a garantir que estas são igualmente resilientes para o fornecedor. Essas dependências devem ser mantidas e revistas a cada 12 meses. As dependências a considerar incluem: ▪ Perda de toda a tecnologia e dados ▪ Indisponibilidade de serviços do(s) subcontratante(s) de material (aqueles que são críticos para a prestação do serviço ao Barclays) ▪ Perda da força de trabalho (perda de edifícios ou/e perda de pessoas; não considerar nenhuma estratégia de recuperação da área de trabalho ou a capacidade de trabalhar a partir de casa) Estes devem ser testados e validados através do Plano de recuperação de negócios, para demonstrar que os serviços cumprem o requisito de Categoria de resiliência estipulado pelo Barclays para garantir que estes são igualmente resistentes e cumprem os níveis de serviço necessários.	Os fornecedores de serviços têm de compreender as dependências para prestar o seu serviço ao Barclays. Quaisquer dependências farão parte do seu Plano de recuperação de negócios para garantir que são consideradas para mitigar o impacto dos incidentes e evitar a indisponibilidade do serviço para o Barclays.
3. Validação dos requisitos de Planeamento de recuperação	O fornecedor tem de manter Planos de recuperação de negócios para os seus Eventos de perturbação acordados. Os Planos de recuperação de negócios devem documentar os passos detalhados de recuperação e a resposta do fornecedor que é possível para mitigar o impacto e/ou adiar a indisponibilidade do serviço prestado ao Barclays.	São levados a cabo testes e validações para garantir ao Barclays que o design de serviço e o plano decorrem conforme pretendido e para demonstrar que os níveis de serviços acordados podem ser prestados e que os serviços

Designação do controlo	Descrição do controlo	Por que é importante
	No mínimo, devem considerar-se: ▪ Possíveis soluções ▪ Protocolos de decisão ▪ Comunicação e estabelecimento de prioridades de negócios para retomar/manter um serviço mínimo viável ▪ Dependências Os Planos de recuperação devem ser testados e validados a cada 12 meses para demonstrar que os níveis de serviço acordados podem ser prestados e que os serviços cumprem os requisitos da Categoria de resiliência estipulados pelo Barclays. Se algum plano não atingir os níveis de serviço acordados ou não cumprir os requisitos da 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 as respetivas datas de finalização).	cumprem os requisitos de resiliência estipulados pelo Barclays.
4. Teste integrado	O fornecedor, mediante solicitação do Barclays, terá de participar num teste integrado a fim de validar a resiliência/continuidade do fornecedor e do Barclays. O Barclays não fará este pedido mais do que uma vez a cada 2 anos, exceto se os testes integrados anteriores tiverem sinalizado falhas materiais ou a aplicação de alterações materiais aos serviços.	Os exercícios conjuntos ajudam a garantir a aplicação de protocolos de Planeamento de recuperação adequados, com a adoção de estratégias de comunicação eficazes, e que tanto o fornecedor quanto o Barclays estão a implementar uma resposta coordenada na gestão da perturbação da atividade e a minimizar o impacto nos clientes Barclays e no sistema financeiro mais vasto.
5. Procedimento de gestão de incidentes/crises	O fornecedor tem de dispor de um procedimento de gestão de incidentes e crises documentado que inclua o processo de encaminhamento de incidentes/crises para o Barclays. Os procedimentos de gestão de incidentes e crises têm de ser aprovados a cada 12 meses, depois de o fornecedor ter efetuado, com sucesso, o teste e a validação. O procedimento tem de definir as atividades e os resultados mínimos exigidos para gerir e lidar com o incidente/a crise ao longo do seu ciclo de vida, do início ao fim. O fornecedor deve nomear:	O fornecedor tem de ser inequívoco quanto aos seus procedimentos para lidar e gerir os serviços em caso de incidente ou crise. O fornecedor e o Barclays têm de chegar a um entendimento sobre o processo de encaminhamento aplicável a incidentes e situações de crise. Os testes e validações têm de ser executados para garantir que a pessoa/equipa em questão possui competências, conhecimentos e capacidade de organização suficientes

Designação do controlo	Descrição do controlo	Por que é importante
	(i) uma pessoa que aprove o procedimento, responsável por confirmar que é adequado à finalidade; (ii) um contacto principal e um representante (em caso de ausência do contacto principal) para cada função em contexto de crise;	para gerir incidentes e crises caso e à medida que estes surjam.
6. Relato pós-incidente/crise	Na sequência de uma perturbação do serviço, tem de ser apresentado ao Barclays um relatório pós-incidente/crise no prazo de quatro semanas de calendário a contar do restabelecimento dos níveis normais de funcionamento do serviço. O relatório tem de incluir, no mínimo, uma revisão de: ▪ a causa principal do incidente ou crise ▪ etapas de correção concluídas e quaisquer ações de melhoria contínua para evitar nova ocorrência ▪ qualquer impacto para os clientes do Barclays conhecido pelo fornecedor	O relatório pós-incidente/crise é necessário para garantir ao Barclays que os problemas são identificados/remediados e que são retiradas as devidas ilações em tempo útil.
7. Planos de recuperação do sistema	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 do 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. Observação: 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 opere 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 (PCO).	A inexistência ou inadequação dos Planos de recuperação do sistema pode conduzir à perda inaceitável do serviço de tecnologia para o Barclays ou para os respetivos 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.
8. Planos de recuperação da integridade dos dados	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 do 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, podendo esta ser originada por atos dolosos ou falhas do sistema. Dispor de um plano para este cenário é crucial e ajuda a identificar e a compreender as fontes de dados e dependências.

Designação do controlo	Descrição do controlo	Por que é importante
9. Diversidade dos centros de dados	O fornecedor tem de garantir que cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços do 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.
10. 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 preencherem os requisitos da 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 [PCO]). Os requisitos relativos à frequência da validação têm de ser suportados pela Categoria de resiliência associada, ou seja: - Categoria de resiliência 0: A validação do SRP deve ser realizada, no mínimo, quatro vezes por ano através da PCO. - Categoria de resiliência 1: A validação do SRP e da PCO deve ser realizada, no mínimo, duas vezes por ano através da PCO - Categoria de resiliência 2: A validação do SRP deve ser realizada, no mínimo, a cada 12 meses; - Categoria de resiliência 3: A validação do SRP deve ser realizada, no mínimo, 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 fornecer planos de correção detalhados (que incluam as ações a realizar e as respetivas datas de finalização). O fornecedor terá de notificar o Barclays antes de executar a PCO.	Os sistemas tecnológicos providenciados por terceiros podem afetar os percursos 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 existe um mandato regulamentar para o Barclays exercer uma governança adequada na gestão dos seus fornecedores. A Convergência de produção (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.

Designação do controlo	Descrição do controlo	Por que é importante
11. 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 do Barclays com uma Categoria de resiliência 0-1, a fim de comprovar a integridade dos dados durante a recuperação. A validação deve ser realizada, pelo menos, 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 as respetivas datas de finalização).	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.
12. Planos de reconstrução/reparação de plataforma e aplicação	Para apoiar a recuperação de eventos de perturbação, tais como uma exploração cibernética, o fornecedor deve ter um Plano de reconstrução/reparação de plataforma e aplicação para cada serviço/sistema tecnológico necessário para apoiar a prestação de serviços do Barclays com uma Categoria de resiliência 0-1 e estar sujeito a revisão, aprovação e teste pelo menos uma vez 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 as respetivas datas de finalização).	Os serviços de tecnologia e os acordos de suporte têm planos de recuperação adequados para um evento de integridade de dados/cibernético.

3. Tabela de níveis críticos de resiliência:

O Barclays atribui uma Categoria de resiliência específica (0-4) aos serviços do fornecedor. Uma Categoria de resiliência mais elevada (ou seja, um número mais baixo) exigirá um padrão de resiliência ou recuperação mais elevado proporcional à importância do serviço. O fornecedor deve assegurar que os seus serviços cumprem o Objetivo de tempo de recuperação (RTO) abaixo especificado para a Categoria de resiliência aplicável estipulada pelo Barclays:

		ERMF - Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		Resilience Category	0	1	2	3	4
		Resilience Type	Continuous	Highly Resilient	Resilient	Recover	Suspend / Backup Only
Disruption Event	Application	RTO for Application Recovery (non-data events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery