

Obrigações de controlo de fornecedores externos

Resiliência

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 efeito perturbador que pode ser gerido no âmbito das operações quotidianas mediante a invocação de planos de recuperação.
"Recovery Time Objective" (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. Requisitos de resiliência de conceção de serviço	O Barclays deve estipular a categoria de resiliência dos serviços e o fornecedor deve garantir que os serviços são concebidos de forma a alcançar os "Recovery Time Objectives" (RTO - objetivos de tempo de recuperação), conforme definido abaixo.	O Barclays tem um requisito comercial (e orientado para o risco) de evitar e/ou conseguir recuperar atempadamente de significativas perturbações do processo, 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.
2. Validação de requisitos de resiliência	<p>Para efeitos da presente descrição do controlo, um "componente" de serviço inclui tudo o que facilite a prestação desse serviço, incluindo, entre outros, pessoas, equipamentos, fornecedores, aplicações de TI e infraestruturas.</p> <p>O fornecedor tem de testar e validar os componentes de serviço de 12 em 12 meses para demonstrar que os serviços preenchem os requisitos de categoria de resiliência estipulados pelo Barclays.</p> <p>Se algum componente de serviço não cumprir os requisitos de categoria de resiliência aplicáveis, o fornecedor tem de notificar</p>	É efetuado um teste e uma validação por forma a garantir ao Barclays que a conceção de serviço funciona como pretendido e permite cumprir os requisitos de resiliência estipulados pelo Barclays.

Designação do controlo	Descrição do controlo	Por que é importante
	<p>imediatamente o Barclays e de fornecer planos de correção detalhados (que incluam as ações a realizar e respetivas datas de finalização).</p>	
<p>3. Procedimento de gestão de incidentes/crises</p>	<p>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 de 12 em 12 meses, depois de o fornecedor ter efetuado, com sucesso, o teste e a validação.</p> <p>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: i) uma pessoa que aprove o procedimento, responsável por confirmar que é adequado à finalidade; e</p> <p>ii) um contacto principal e um representante (em caso de ausência do contacto principal) para cada função em contexto de crise.</p>	<p>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 entendimento sobre o processo de encaminhamento aplicável a incidentes e situações de crise.</p> <p>O fornecedor tem de efetuar testes e validações para garantir que a pessoa/equipa competente possui competências, conhecimentos e capacidade de organização suficientes para gerir incidentes e crises caso, quando e à medida que surjam.</p>
<p>4. Relato pós-incidente/crise</p>	<p>Na sequência de uma perturbação do serviço, tem de ser apresentado ao Barclays um relato pós-incidente/crise no prazo de quatro semanas de calendário a contar do restabelecimento dos níveis normais de funcionamento do serviço.</p> <p>O relatório tem de incluir, no mínimo, uma revisão de:</p> <ul style="list-style-type: none"> • eventos em torno da situação; • modo de gestão do incidente/da crise; • análise da causa originária; • se está classificado como "evento de risco" pelo fornecedor ou pelo Barclays (ou seja, se é considerado suficientemente significativo para ser notificado/encaminhado para as partes interessadas relevantes em conformidade com as políticas aplicáveis do conhecimento do fornecedor); • se representa um "risco de conduta" (p. ex., se o fornecedor está a lidar diretamente com clientes do Barclays); 	<p>O relato 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.</p>

Designação do controlo	Descrição do controlo	Por que é importante
	<ul style="list-style-type: none"> qualquer compensação do cliente do Barclays que seja do conhecimento do fornecedor; e quaisquer medidas necessárias para prevenir a repetição de incidentes/crises similares. 	

3. Tabela de sensibilidade de resiliência:

O Barclays atribui uma categoria de resiliência específica (0-3) 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 "Recovery Time Objective" (RTO - objetivo de tempo de recuperação) abaixo especificado no que respeita à categoria de resiliência estipulada pelo Barclays:

Categoria de resiliência	0	1	2	3
"Recovery Time Objective" (RTO - objetivo de tempo de recuperação)	0 s	< 4 Horas	< 12 Horas	24 Horas