Obrigações de controlo de fornecedores externos

Planeamento de recuperação

Versão 13.0 Setembro de 2023

1. Definições:

"Evento de perturbação"	Um registo 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.
"Incidente"	Significa um evento perturbador que pode ser gerido no âmbito das operações quotidianas mediante a invocação de planos de recuperação.
"Plano de recuperação"	Planos de recuperação são documentos que detalham as etapas e ações a serem tomadas para restaurar um serviço de volta ao estado operacional. Podem ser designados por Plano de continuidade empresarial ou termos semelhantes.
"Planeamento de recuperação"	O processo ou planeamento para a recuperação de serviços de negócios, processo de negócios e dependências subjacentes.
"Objetivo de tempo de recuperação"	Significa o período entre uma falha ou interrupção inesperada dos serviços e o restabelecimento das operações.
"Categoria de resiliência"	Categoria de resiliência é uma classificação utilizada pelo Barclays para aplicar requisitos de resiliência a um serviço. A categoria de resiliência impulsiona o objetivo de tempo de recuperação ("Recovery Time Objective - RTO"), o objetivo de ponto de recuperação ("Recovery Point Objective - RPO") e o requisito de frequência de validação.

2. Tabela de níveis críticos de resiliência:

Os serviços do fornecedor são atribuídos a uma categoria de resiliência específica (0 - 4) pelo Barclays, que reflete o possível impacto no Barclays devido a uma perturbação do serviço. 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) e o objetivo de ponto de recuperação (RPO) abaixo especificados para a categoria de resiliência aplicável estipulada pelo Barclays para os serviços contratados. A tabela seguinte especifica quais os controlos de fornecedor aplicáveis com base na categoria de resiliência definida e os detalhes desses controlos são indicados na secção 3 (*Controlo*) abaixo.

Avaliação de impacto de risco	Impacto excecional	Impacto elevado	Impacto moderado	Impacto reduzido	Impacto insignificante
Categoria de resiliência	0	1	2	3	4
RTO pretendido	Até 1 hora	Até 4 horas	Até 12 horas	Até 24 horas	Sem recuperação planeada
RPO pretendido	Até 5 minutos	Até 15 min	Até 30 min	Até 24 horas	Sem recuperação planeada

Frequência de teste de tecnologia	Categoria de resiliência 0	Categoria de resiliência 1	Categoria de resiliência 2	Categoria de resiliência 3	Categoria de resiliência 4
Validação do plano de recuperação do sistema	Mín. duas vezes por ano	Mín. duas vezes por ano	Mín. a cada 12 meses	Mín. a cada 24 meses	Sem recuperação planeada
Validação do plano de recuperação de dados	Validação anual do plano em ambiente de produção	Validação anual através de instruções no ambiente de trabalho	Opcional	Opcional	Sem recuperação planeada
Validação do plano de reconstrução de plataforma e aplicação	Validação anual através de instruções no ambiente de trabalho	Validação anual através de instruções no ambiente de trabalho	Opcional	Opcional	Sem recuperação planeada

Aplicabilidade dos controlos do fornecedor	Categoria de resiliência 0	Categoria de resiliência 1	Categoria de resiliência 2	Categoria de resiliência 3	Categoria de resiliência 4
1. Requisito de mapeamento de dependências para inclusão no planeamento de recuperação	✓	✓	✓	✓	O
2. Eventos de perturbação para requisito de planeamento de recuperação	✓	✓	✓	✓	O
3. Requisito de validação e planeamento de recuperação	✓	✓	✓	✓	O
4. Requisito de teste integrado	✓	✓	O	O	O
5. Requisito de validação e planos de recuperação do sistema	✓	✓	✓	✓	O
6. Requisitos de validação e planos de recuperação de dados	✓	✓	O	O	O
7. Requisitos do fornecedor de serviços na nuvem e diversidade dos centros de dados	✓	✓	✓	✓	O
8. Requisito de planos de reconstrução da plataforma e aplicação	✓	✓	O	O	O

✓ = Obrigatório	O = Opcional

Se forem identificados quaisquer problemas durante a análise ou um incumprimento dos requisitos durante o teste de controlos, o fornecedor tem de notificar o Barclays de imediato (normalmente no período de 10 dias) e corrigir os problemas até uma data acordada.

3. Controlos:

O fornecedor deve ter uma abordagem estruturada à resiliência (continuidade de negócios e recuperação de desastres) que seja suportada por um documento de políticas e normas que regulem os requisitos de resiliência operacional e técnica de acordo com as melhores práticas do setor e os requisitos regulamentares, conforme aplicável. A abordagem estruturada à resiliência deve ser supervisionada pela direção e analisada e testada anualmente quanto à eficácia.

Designação do controlo	Descrição do controlo	Por que é importante
1. Requisito 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. Essas dependências devem ser mantidas e revistas a cada 12 meses ou quando ocorrer uma mudança substancial. As dependências a considerar incluem: ▪ Tecnologia e dados (fornecidos por pessoal interno e subcontratados). ▪ Subcontratante(s) importante(s) (que poderia(m) ter um impacto relevante no desempenho e fornecimento do serviço ao Barclays). ▪ Força de trabalho (perda de pessoas; não considerar nenhuma estratégia de recuperação da área de trabalho ou a capacidade de trabalhar a partir de casa).	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.
2. Eventos de perturbação para requisito de planeamento de recuperação	O fornecedor tem de definir os eventos de perturbação no âmbito do planeamento de recuperação 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. O fornecedor tem de garantir que esses eventos de perturbação continuam a refletir o cenário atual de risco/ameaça, são avaliados quanto à gravidade e plausibilidade e são suportadas por perceções da indústria e de informações. No mínimo, o fornecedor tem de incluir os seguintes eventos de perturbação no âmbito do seu planeamento. ▪ Perda de edifícios em várias localizações que afetem a prestação de serviços ao Barclays. (Edifícios e infraestruturas associadas não estão disponíveis). ▪ Cenário de perda de dados, incluindo eventos cibernéticos e o potencial impacto na prestação de serviços ao Barclays.	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 tem de ser capaz de garantir às partes interessadas que, no caso de ocorrência de perturbação, o serviço está concebido de forma a minimizar o impacto (seja do cliente, financeiro e/ou na reputação).

Designação do controlo	Descrição do controlo	Por que é importante
	▪ Perda de recursos da força de trabalho que afetaria o fornecimento dos níveis de serviço acordados (ou seja, evento pandémico, evento geopolítico, falha crítica da infraestrutura nacional, etc.). ▪ Perda de serviços de tecnologia (ou seja, perda de centros de dados ou região do fornecedor de serviços na nuvem). ▪ Perda de um subcontratante importante (serviços ou materiais). 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.	
3. Requisito de validação e planeamento de recuperação	O fornecedor tem de manter planos de recuperação para os seus eventos de perturbação acordados. Os planos de recuperação devem documentar os passos detalhados de recuperação e a resposta do fornecedor que é possível para mitigar o impacto e/ou adiar a indisponibilidade dos serviços prestados ao Barclays. 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 ou quando ocorre uma mudança substancial 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 (normalmente no período de 10 dias) e fornecer planos de correção detalhados (que incluam as ações a realizar e as respetivas datas de finalização).	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 cumprem os requisitos de resiliência estipulados pelo Barclays.

Designação do controlo	Descrição do controlo	Por que é importante
4. Requisito de teste integrado	Para garantir que as interdependências entre o Barclays e os serviços do fornecedor são compreendidas em relação à recuperação de serviços, o fornecedor, a pedido do Barclays e numa data mutuamente acordada, tem de participar num teste integrado para validar a resiliência/continuidade coletiva 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 se tiver ocorrido um incidente que tenha provocado a perturbação dos 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. Requisito de validação e planos de recuperação do sistema	O fornecedor deve ter um plano de recuperação do sistema que detalhe as ações necessárias para repor os sistemas no estado operacional após uma interrupção. Os planos têm de ser testados e validados para demonstrar (com provas) que o sistema pode ser recuperado dentro do objetivo de tempo de recuperação e do objetivo de ponto de recuperação definidos, conforme exigido pela categoria de resiliência definida. Para sistemas concebidos numa configuração ativa/passiva, deve ser ativado o ambiente passivo e utilizado como ambiente de produção de BAU durante um período de tempo suficientemente longo para provar a capacidade e a funcionalidade de integração total. Para serviços concebidos como ativo/ativo, a validação deve comprovar a continuação do funcionamento sob a perda de um nó, instância ou zona de disponibilidade (para alojamento na Nuvem) do sistema (mínimo de 60 minutos). Os requisitos de frequência de validação são definidos pela categoria de resiliência do sistema. Consulte a tabela de níveis críticos de resiliência acima	A inexistência ou inadequação de 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.
6. Requisitos de validação e planos de recuperação de dados	O fornecedor deve ter planos de recuperação de dados para cada sistema tecnológico necessário para apoiar a prestação de serviços ao Barclays. Os planos devem ser revistos quanto à precisão pelo menos uma vez a cada 12 meses ou quando ocorrer uma mudança substancial e devem considerar, no mínimo, o seguinte: ▪ Fontes e fluxo de dados (a montante e a jusante) ▪ Fontes de cópia de segurança e replicação ▪ Requisitos de sincronização de dados após a restauração	A perda de dados é uma das maiores ameaças com que o Barclays se depara, 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
	O fornecedor deve testar e validar os planos de recuperação de dados para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços ao Barclays e comprovar (com provas) que o processo de recuperação pode recuperar dados para o estado operacional esperado e dentro do objetivo do ponto de recuperação.	
7. Requisitos do fornecedor de serviços na nuvem e diversidade dos centros de dados	O fornecedor tem de garantir que cada sistema tecnológico necessário para apoiar a prestação de serviços ao Barclays é resiliente ao longo nos centros de dados e com uma distância geograficamente suficiente para reduzir o risco de os centros de dados serem afetados simultaneamente pelo mesmo evento. Nos casos em que o sistema tecnológico está alojado num fornecedor de serviços na nuvem, o sistema deve estar disponível em diferentes zonas de disponibilidade para mitigar uma interrupção na zona de disponibilidade. São necessários sistemas críticos para demonstrar a capacidade de recuperar de uma falha de região do fornecedor de serviços na nuvem.	Os sistemas tecnológicos devem ser implantados em vários centros de dados para proteger contra uma paragem do centro de dados. Isto aplica-se a sistemas alojados em fornecedor de serviço de nuvem - Falha na região.
8. Requisito de planos de reconstrução da plataforma e aplicação	O fornecedor deve manter um plano de reconstituição de plataforma e aplicação para cada sistema tecnológico necessário para apoiar a prestação de serviços ao Barclays e estar sujeito a análise, aprovação e teste pelo menos uma vez a cada 12 meses, ou quando ocorre uma mudança substancial. Estes planos destinam-se a situações em que as opções tradicionais de recuperação/restauração não podem ser utilizadas e é necessária uma restauração "bare-metal" do sistema. Os planos devem considerar: ▪ Sistema operativo/software de infraestrutura ▪ Implementação e configuração de aplicações ▪ Controlos/configuração de segurança ▪ Dependências e reintegração do ecossistema do sistema ▪ Requisitos de dados (plano de recuperação de dados) ▪ Dependências de ferramentas para executar planos de recuperação	É fundamental que os serviços tecnológicos e os acordos de assistência tenham planos de recuperação adequados para um evento de integridade de dados/cibernético.

Designação do controlo	Descrição do controlo	Por que é importante